

## Calendar No. 28

114TH CONGRESS }  
*1st Session* }

SENATE

{ REPORT  
114-32

---

---

### CYBERSECURITY INFORMATION SHARING ACT OF 2015

---

APRIL 15, 2015.—Ordered to be printed

---

Mr. BURR, from the Select Committee on Intelligence,  
submitted the following

#### R E P O R T

together with

#### ADDITIONAL VIEWS

[To accompany S. 754]

The Select Committee on Intelligence, having considered an original bill (S. 754) to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes, reports favorably thereon and recommends that the bill do pass.

#### BACKGROUND AND NEED FOR LEGISLATION

Over the last several years, the Committee has listened with increasing alarm to the testimony of senior intelligence officials and private sector experts about the growing cybersecurity threats to our nation.

The Committee has already seen the impact these threats are having on the nation's security and its economy as losses to consumers, businesses, and the government from cyber attacks, penetrations, and disruptions already total billions of dollars. Beyond direct monetary losses, the continuing efforts of foreign actors to steal intellectual property will have far reaching impacts on the innovation upon which a robust economy and strong military relies. The Committee has seen widespread theft through cyberspace increasingly evolve into disruptive and destructive attacks. American financial institutions have been subjected to denial of service attacks by foreign actors that blocked consumers' access to banking services. Critical infrastructure companies abroad and businesses

in the United States have seen their vital business systems rendered useless by hostile actors operating in other countries. The reported destructive cyberattacks on the Las Vegas Sands Corporation and Sony Pictures Entertainment represent further escalation of this disturbing trend, including unprecedented efforts to destroy data of U.S. companies. Our nation is growing more vulnerable to cyber threats. Every aspect of society is growing more dependent on computers which are all linked to networks, opening this country up to many known vulnerabilities and many yet to be discovered.

The Committee and its staff have also engaged in hundreds of conversations with senior government and private sector officials that have demonstrated the need for a legislative effort to allow for the increased sharing of information about these cyber threats. There are many stakeholders who are engaged on these issues and the Committee is convinced that legislation is needed to assist them in finding better ways to work together to address our nation's shared cybersecurity challenges. This legislation is designed to create a *voluntary* cybersecurity information sharing process that will encourage public and private sector entities to share cyber threat information, removing legal barriers and the threat of unnecessary litigation. This in turn allows for greater cooperation and collaboration in the face of growing cybersecurity threats to national and economic security. Additionally, the Committee believes that such increased sharing will drive public and private sector cybersecurity efforts to develop key new technologies and processes, such as an improved ability to share technical threat information through an automated process in "real time" to counter cyber threats at machine speed.

Through the Committee's oversight of the Intelligence Community, it has long recognized the need to better use the government's knowledge and expertise about cyber threats for defensive purposes. This legislation includes requirements for the government to share more information, including classified information under appropriate safeguards, with relevant private sector entities to further cybersecurity. Often as a result of overclassification and parochialism, some cybersecurity information that could enable the businesses facing these threats to better protect themselves remains exclusively in the government. Although sensitive sources and methods must be protected, the government does not presently share adequate information about cyber threats. This bill encourages the government to expand this sharing and to create the appropriate processes to do so.

This legislation also includes positive legal authorities for private companies to: (1) monitor their networks, or those of their customers upon authorization and written consent, for cybersecurity purposes; (2) take defensive measures to stop cyber attacks and (3) share cyber threat information with each other and with the government to further collective cybersecurity. Through extensive hearings, briefings, and discussions, the Committee has identified the need to provide carefully tailored cybersecurity authorities to address these current gaps. The Committee also recognizes the careful balance that must be struck in providing increased authorities to ensure they are used appropriately. This legislation creates a completely voluntary information-sharing framework that in-

cludes several layers of privacy protections to prevent abuse and ensure that the government cannot inappropriately acquire or use sensitive information other than for limited cybersecurity and public safety purposes.

In addition to concerns about legal authorities, the specter of litigation for monitoring a company's own networks or sharing cyber threat indicators or defensive measures for cybersecurity purposes has disincentivized private sector cybersecurity efforts. Entities appropriately monitoring their systems for cybersecurity threats and sharing information necessary to protect against those threats should not be exposed to costly legal uncertainty for doing so. Moreover, it is these same companies who are the victims of malicious cyber activity, and their appropriate efforts to protect themselves and other future victims from cyber threats should not only be authorized but protected from unnecessary litigation. This legislation creates narrowly tailored liability protection to incentivize companies' efforts to identify cybersecurity threats and share information about them. However, this liability protection does not extend to defensive measures, nor does it protect unauthorized monitoring or sharing, including gross negligence or willful misconduct, that risks sensitive data rather than safeguarding it.

The Committee believes that the increased information sharing enabled by this bill is critical step forward for improving cybersecurity in America.

#### SECTION-BY-SECTION ANALYSIS AND EXPLANATION

The following is a section-by-section analysis and explanation of the Cybersecurity Information Sharing Act of 2015 that is being reported by the Committee.

##### *Section 1. Short title*

Section 1 states that this Act may be cited as the "Cybersecurity Information Sharing Act of 2015."

##### *Section 2. Definitions*

Section 2 provides 18 definitions for this Act, to include the following key terms: "cybersecurity purpose," "cybersecurity threat," "cyber threat indicator," "defensive measure," and "monitor."

The term "cybersecurity purpose" means the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability. This definition ensures that the authorities of private entities to monitor and operate defensive measures must be exercised for the purpose of protecting their own networks and those of their customers when authorized by the written consent of such customers. The definition of "cybersecurity purpose" is also one of the main limitations on the ability of private and governmental entities to use cyber threat indicators and defensive measures.

The term "cybersecurity threat" is defined as an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system that is stored on, processed by, or transiting an information system. The term

does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement. Many terms of service agreements prohibit activities that would also meet the “cybersecurity threat” definition; such activities would still be considered a “cybersecurity threat” because they were not “solely” violations of consumer agreements. The Committee intends this definition to include activities that may have unauthorized and negative results, but to exclude authorized activities, such as extensive use of bandwidth that may incidentally cause adverse effects. However, this definition clearly does not permit hackers to cloak their criminal actions like theft of information or destruction of property under the ambit of First Amendment protected activities.

The term “cyber threat indicator” is one of the most important definitions in this Act. It is defined as information that is necessary to describe or identify: (1) malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability; (2) a method of defeating a security control or exploitation of a security vulnerability; (3) a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability; (4) 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 to unwittingly enable the defeat of a security control or exploitation of a security vulnerability; (5) malicious cyber command and control; (6) the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat; (7) any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or (8) any combination thereof. This narrow definition is a key privacy protection in the Act because it creates an exhaustive list of the types of cyber threat information that can be shared among private and governmental entities, and only when they are necessary to describe or identify threats to information and information systems. Essentially, this definition limits the information that can be shared under this Act to the techniques and “malware” used by malicious actors to compromise the computer networks of their victims, not sensitive personal and business information contained in such networks.

The term “defensive measure” is defined as an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability. However, a defensive measure does not include a measure that destroys, renders unusable, or substantially harms an information system or data on an information system not belonging to the private entity operating such measure or another entity or Federal entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure. Recognizing the inherent right of self-defense that entities have to protect their networks and data, the Committee intends for this definition to provide a positive legal authority allowing private entities to take measures to take appropriate steps to defend their own in-

formation networks and systems, or those of their customers when authorized by the written consent of such customers, against malicious cybersecurity threats. For example, a defensive measure could be something as simple as a security device that protects or limits access to a private entity's computer infrastructure or as complex as using sophisticated software tools to detect and protect against anomalous and unauthorized activities on a private entity's information system. Regardless, this definition does not authorize the use of measures that are generally to be considered "offensive" in nature, such as unauthorized access of or executing computer code on another entity's information systems or taking an action that would substantially harm another private entity's information systems. The Committee is aware that defensive measures on one entity's network could have effects on other networks. It is the Committee's intent that the authorization in this Act extends to defensive measures on an entity's information systems that do not cause substantial harm to another entity's information systems or data on such systems, regardless of whether such non-substantial harm was intended or foreseen by the implementing entity.

The term "monitor" means to acquire, identify, or scan, or to possess, information that is stored on, processed by, or transiting an information system. This definition, as used in this Act, is not intended to equate to the meaning of the term "monitor" used in the context of the interception of communications under the Federal criminal wiretap statutes or electronic surveillance under the Foreign Intelligence Surveillance Act. Specifically, private entities are only authorized to monitor *their own information systems* or those of another private entity upon the authorization and written consent of such other entity. Moreover, such monitoring is limited to cybersecurity purposes. Essentially, these important limitations ensure that private entities are only authorized to monitor their information systems to protect against cybersecurity threats and vulnerabilities. Any other monitoring would require lawful authority other than that provided in this Act.

### *Section 3. Sharing of Information by the Federal Government*

Section 3 requires the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General to develop and promulgate procedures that facilitate and promote the timely sharing of: (1) classified cyber threat indicators with cleared representatives of relevant entities; (2) declassified cyber threat indicators with relevant entities; (3) unclassified cyber threat indicators with relevant entities or the public; and (4) information in the possession of the Federal Government about cybersecurity threats to such entities to prevent or mitigate adverse effects from such cybersecurity threats. These procedures must ensure that the Federal government has and maintains the capability to share cyber threat indicators in real time consistent with the protection of classified information and incorporate to the greatest extent practicable existing processes and existing roles and responsibilities.

The procedures required by this section must also include a process for notifying entities that have received a cyber threat indicator from a Federal entity that is known or determined to be in error or in contravention of Federal law or policy. Federal entities receiv-

ing cyber threat indicators will also be required to implement and use security controls to protect against unauthorized access to or acquisition of such indicators. Moreover, the procedures require that a Federal entity, prior to sharing a cyber threat indicator, review and remove any information that the Federal entity knows at the time of the sharing to be personal information of or identifying a specific person not directly related to a cybersecurity threat or implement and use a technical capability configured to remove personal information of or identifying a specific person not directly related to a cybersecurity threat. In developing these procedures, the responsible officials must coordinate with other appropriate Federal entities, including the National Laboratories due to their technical expertise, so that effective protocols are implemented to facilitate and promote sharing in a timely manner. Within 60 days of the enactment of this Act, the Director of National Intelligence in consultation with the heads of the appropriate Federal entities shall submit these procedures to the Congress.

*Section 4. Authorizations for Preventing, Detecting, Analyzing, and Mitigating Cybersecurity Threats*

Subsection (a) of Section 4 provides a private entity with the authority to monitor, for cybersecurity purposes: (1) its own information systems; (2) an information system of another entity, upon the authorization and written consent of such other entity; (3) an information system of a Federal entity, upon the authorization and written consent of an authorized representative of the Federal entity; and (4) information that is stored on, processed by, or transiting an information system monitored by the private entity. Nothing in subsection (a) shall be construed to authorize the monitoring of information systems, or the use of any information obtained through such monitoring of such information systems, other than as provided in this Act.

Subsection (b) provides private entities with the authority to operate defensive measures, for cybersecurity purposes, that are applied to its information systems to protect the rights and property of such private entities, those of another entity upon written consent of such entity for operation of such defensive measures to protect the rights and property of that entity, or those of a Federal entity upon written consent of an authorized representative of such Federal entity for operation of such defensive measures to protect the rights or property of the Federal Government. This subsection does not authorize the use of defensive measures other than for cybersecurity purposes.

Under subsection (c), an entity is authorized to share with or receive from any other entity or the Federal Government cyber threat indicators and defensive measures for the purposes permitted under this Act, consistent with the protection of classified information when applicable. An entity receiving cyber threat indicators and defensive measures from another entity or Federal entity must comply with otherwise lawful restrictions placed on the sharing or use of such cyber threat indicators or defensive measures by the sharing entity or Federal entity, such as a limitation of future sharing of the indicators or measures.

An entity monitoring information systems, operating defensive measures or providing or receiving defensive measures under Sec-

tion 4 must implement and utilize security controls to protect against unauthorized access to or acquisition of such cyber threat indicators or defensive measures.

Prior to sharing a cyber threat indicator pursuant to this Act, an entity shall review such cyber threat indicator to assess whether such indicator contains any information that the entity knows at the time of sharing to be personal information of or identifying a specific person not directly related to a cybersecurity threat and remove such information or implement and utilize a technical capability configured to remove any information contained with such indicator that the entity knows at the time of the sharing to be personal information of or identifying a specific person not directly related to a cybersecurity threat. During the Committee's drafting of the legislation, industry groups and trade associations noted that the requirement to remove personal information may preclude some companies, especially smaller ones, from participating in the information sharing process endorsed by the bill. As a private entity must ensure that any information shared meets the definition for "cyber threat indicator" or "defensive measure" to comply with the Act, the requirement to remove any known unnecessary privacy information strikes the appropriate balance between narrowly tailoring what information can be shared and providing a practicable standard. Further, the Committee hopes that the Attorney General guidance required in section 5 and common practices and guidelines will assist smaller and middle-sized companies implement this requirement.

Section 4 authorizes an entity to use cyber threat indicators and defensive measures, for cybersecurity purposes, to monitor or operate defensive measures on its information systems or those of another entity or Federal entity upon written consent.

A cyber threat indicator shared by an entity with a State, tribal, or local department or agency may, with the prior written consent of such entity, be used for the purpose of preventing, investigating, or prosecuting any of the offenses described in Section 5(d)(5)(A)(vi). These offenses involve imminent threats of death, serious bodily harm, or serious economic harm, including a terrorist act or a use of a weapon of mass destruction. They also include serious violent felonies and offenses related to fraud and identity theft, and protection of trade secrets. If the need for immediate use prevents a State, tribal, or local department or agency from obtaining written consent before such use, consent may be provided orally with subsequent documentation of consent. The entity providing consent for this use must have the authorization to possess and share such a cyber threat indicator under this Act and must conduct such sharing consistent with the conditions set out.

Cyber threat indicators shared with a State, tribal, or local department or agency under Section 4 are deemed voluntarily shared information and exempt from disclosure under any State, tribal, or local law requiring disclosure of information or records.

In general, cyber threat indicators shared with a State, tribal, or local government under this Act shall not be directly used by any State, tribal, or local government to regulate, which includes bringing an enforcement action, the lawful activity of any entity, including an activity relating to monitoring, operating a defensive measure, or sharing of a cyber threat indicator. However, a cyber threat

indicator or defensive measure may, consistent with a State, tribal, or local government regulatory authority specifically relating to the prevention or mitigation of cybersecurity threats to information systems, inform the development or implementation of a regulation relating to such information systems. The Committee views this as a narrow exception to ensure that government agencies with regulatory authority understand the current landscape of cyber threats and those facing the particular regulatory sector over which they have cognizance.

Under subsection (e), two or more private entities are not to be considered in violation of any provision of antitrust law when exchanging or providing a cyber threat indicator, or assistance relating to the prevention, investigation, or mitigation of a cybersecurity threat, for cybersecurity purposes under this Act. This provision should be read in conjunction with the rule of construction in Section 8(e) that nothing in the Act shall be construed 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. The bill allows for the sharing of cybersecurity-related information for cybersecurity purposes, acknowledging that doing so might otherwise be a potential violation of anti-trust laws that seek to limit sharing of information for other purposes. The bill does not intend to protect companies from engaging in anti-competitive behavior under the guise of cybersecurity.

Further, this subsection only applies to information that is exchanged or assistance provided to the communication or disclosure of cyber threat indicators for the facilitation of the prevention, investigation, or mitigation of cybersecurity threats to an information system or information that is stored on, processed by, or transiting an information system.

Section 4 also clarifies that the sharing of cyber threat indicators under this Act shall not create a right or benefit to similar information by such entity or another entity.

*Section 5. Sharing of Cyber Threat Indicators and Defensive Measures with the Federal Government*

Section 5 directs the Attorney General, in coordination with the heads of appropriate Federal entities, to develop and submit to Congress not later than 60 days after the enactment of this Act interim policies and procedures relating to the receipt of cyber threat indicators and defensive measures by the Federal Government. Not later than 180 days after the enactment of this Act, the Attorney General, in coordination with the heads of appropriate Federal entities, is required to promulgate a final version of such policies and procedures.

The policies and procedures developed under Section 5 must meet several requirements in addition to being consistent with the Attorney General's privacy and civil liberties guidelines required by subsection (b). They must ensure that cyber threat indicators shared with the Federal Government through the real time process described in subsection (c)—the capability and process within the DHS—are shared in an automated manner with all appropriate Federal entities, are not subject to any delay or interference, and may be provided to other Federal entities. The Committee intends

that these policies and procedures both enable the delivery of real time information about cybersecurity threats to appropriate Federal entities and provide sufficient technical controls to protect privacy information.

For cyber threat indicators shared in a manner other than the real-time process described in subsection (c), the policies and procedures shall ensure that cyber threat indicators are shared as quickly as operationally practicable with all appropriate Federal entities, are not subject to unnecessary delay, interference, or any other action that could impede receipt by all of the appropriate Federal entities, and may be provided to other Federal entities. As cyber threat indicators received outside of the real-time process in subsection (c) may be received by the Federal Government in a format less conducive to “as quickly as operationally practicable” sharing, the Committee intends that this sharing requirement will vest when such information is in a format that can feasibly be shared. Once a cyber threat indicator can feasibly be shared with appropriate Federal entities, the Federal entity possessing such indicator must proceed to share it consistent with the policies and procedures and without unnecessary delay. The Attorney General’s policies and procedures should include how such cyber threat indicators will be put into a shareable format and the proper sharing procedures within the Federal Government. Further, the policies and procedures shall govern the retention, use, and dissemination of cyber threat indicators shared with the Federal Government, consistent with this Act, otherwise applicable law, and consistent with the applicable sections of the commonly accepted fair information practice principles. To ensure compliance, an audit capability and appropriate sanctions for officers, employees, or agents of a Federal entity who knowingly and willfully conduct unauthorized activities are required to be included in the policies and procedures.

In an effort to assist the public and promote sharing of cyber threat indicators, Section 5 requires the Attorney General to develop and make publicly available guidance that: (1) identifies the types of information that would qualify as a cyber threat indicator under this Act that would be unlikely to include personal information of or identifying a specific person not directly related to a cyber security threat; (2) identifies the types of information that are protected under otherwise applicable privacy laws that are unlikely to be directly related to a cybersecurity threat; and (3) contains such other matters as the Attorney General considers appropriate for entities sharing cyber threat indicators with Federal entities under this Act.

Section 5 also directs the Attorney General, not later than 60 days after the date of enactment, in coordination with heads of the appropriate Federal entities and in consultation with privacy and civil liberties officers of such entities, to develop, submit to Congress, and make available to the public interim guidelines relating to privacy and civil liberties that will govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity obtained in connection with activities authorized under this Act. Not later than 180 days after the date of enactment, the Attorney General shall, in coordination with the heads of the appropriate Federal entities and in consultation with privacy and civil liberties officers of such entities and such private entities with industry ex-

pertise as the Attorney General considers relevant, promulgate final privacy guidelines that shall govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity obtained in connection with activities authorized in this Act. The Attorney General is also required to periodically review these privacy guidelines, again in coordination with the heads of the appropriate Federal entities and in consultation with privacy and civil liberties officers and industry experts. Consistent with the need to protect information from cybersecurity threats and mitigate those threats, the guidelines are required to limit the impact on privacy and civil liberties from activities by the Federal Government under this Act. These guidelines shall also limit the receipt, retention, use, and dissemination of cyber threat indicators containing personal information of or identifying specific persons. As part of these limitations, the guidelines will establish a process for the timely destruction of information that is known not to be directly related to uses authorized under this Act and specific limitations on the length of time a cyber threat indicator may be retained by the Federal Government.

The guidelines will include requirements to safeguard cyber threat indicators containing personal information of or identifying specific persons from unauthorized access or acquisition, including appropriate sanctions for activities by officers, employees, or agents of the Federal Government in contravention of such guidelines. If a Federal entity determines or knows that it has received information that does not constitute a cyber threat indicator, the guidelines shall include a procedure to notify entities and Federal entities. The privacy and civil liberties guidelines will protect the confidentiality of cyber threat indicators containing personal information of or identifying specific persons to the greatest extent practicable, and they will require recipients to be informed that such indicators may only be used for purposes authorized under this Act. They must also include steps that may be needed so that dissemination of cyber threat indicators is consistent with the protection of classified and other sensitive national security information.

Subsection (c) requires the Secretary of Homeland Security, not later than 90 days after the date of the enactment of this Act and in coordination with the heads of the appropriate Federal entities, to develop and implement a capability and process (commonly referred to as a “portal”) within the DHS that accepts cyber threat indicators and defensive measures from any entity in real time. The Committee intends that this DHS capability should build upon current Federal Government efforts to both more efficiently receive cyber threat indicators from outside the Federal Government and to more efficiently share such indicators within the Federal Government.

Upon certification by the Secretary of Homeland Security, this capability shall be the process by which the Federal Government receives cyber threat indicators and defensive measures shared by a private entity through electronic mail or media, an interactive form on an Internet website, or a real time, automated process between information systems. There are only two exceptions to this requirement: (1) communications between a Federal entity and a private entity regarding a previously shared cyber threat indicator; and (2) communications by a regulated entity with such entity’s

Federal regulatory authority regarding a cybersecurity threat. The sharing of cyber threat indicators and defensive measures in other formats where there is less privacy risk, such as a telephone call, letter, or in-person meeting, receives liability protection regardless of whether it is first sent through the DHS portal.

When cyber threat indicators and defensive measures are shared through the DHS capability, the Secretary of Homeland Security will ensure that all of the appropriate Federal entities, as defined, receive them consistent with applicable policies, procedures, and guidelines in Section 5.

The DHS capability and process does not limit or prohibit otherwise lawful disclosures of communications, records, or other information, including: (1) reporting of known or suspected criminal activity, by an entity to any other entity or a Federal entity; (2) voluntary or legally compelled participation in a Federal investigation; or (3) providing cyber threat indicators or defensive measures as part of a statutory or authorized contractual requirement.

Not later than 60 days after the date of enactment, the Secretary of Homeland Security shall submit to Congress a report on the development and implementation of the capability and process required by this section.

Subsection (d) includes a number of protections for information shared with or provided to the Federal Government. The provision of cyber threat indicators and defensive measures to the Federal Government under this Act does not constitute the waiver of any applicable privilege or protection provided by law, including trade secret protection. A cyber threat indicator or defensive measure provided by an entity to the Federal Government under this Act shall be considered the commercial, financial, and proprietary information of such entity when so designated by the originating entity. Consistent with this Act and all privileges, protections, and any claims of propriety on such cyber threat indicators or defensive measures, the Committee expects that the Federal Government will further share and use such information for cybersecurity purposes. This sharing and use will be governed by the policies, procedures, and guidelines required by Section 5. Cyber threat indicators and defensive measures provided to the Federal Government under this Act will also be deemed voluntary shared information and exempt from disclosure under section 5 U.S.C. 552 and any State, tribal, or local law requiring disclosure of information or records. Additionally, such cyber threat indicators and defensive measures shall be withheld without discretion from the public under 5 U.S.C. 552(b)(3)(B) and any State, tribal, or local law requiring disclosure of information or records. The provision of cyber threat indicators and defensive measures under this Act shall not be subject to the rules of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decision-making official.

Cyber threat indicators and defensive measures provided to the Federal Government under this Act may be disclosed to, retained by, and used by, consistent with otherwise applicable Federal law, any Federal agency or department, component, officer, employee, or agent of the Federal Government solely for the purposes identified by Section 5, and consistent with the procedures developed by the Attorney General. These purposes are: (1) a cybersecurity purpose;

(2) the purpose of identifying a cybersecurity threat, including the source of such cybersecurity threat, or a security vulnerability; (3) the purpose of identifying a cybersecurity threat involving the use of an information system by a foreign adversary or terrorist; (4) the purpose of responding to, or otherwise preventing or mitigating, an imminent threat of death, serious bodily harm, or serious economic harm, including a terrorist act or a use of a weapon of mass destruction; (5) the purpose of responding to, or otherwise preventing or mitigating, a serious threat to a minor, including sexual exploitation and threats to physical safety; or (6) the purpose of preventing, investigating, disrupting, or prosecuting an offense arising out of a previously described imminent threat or any of the offenses listed in Section 5(d)(5)(vi), including offenses related to serious violent felonies, fraud and identity theft, espionage and censorship, and protection of trade secrets. The word “imminent” in paragraph 5(d)(5)(A)(iv) is intended to modify all the threats listed in that paragraph, to include the threat of a terrorist act or use of a weapon of mass destruction.

Use of cyber threat indicators and defensive measures by the Federal Government will be conducted in accordance with the policies, procedures, and guidelines required in Section 5, and will be done in a manner that protects from unauthorized use or disclosure any cyber threat indicators that may contain personal information of or identifying specific persons and protects the confidentiality of such information.

Additionally, such cyber threat indicators and defensive measures shared with the Federal Government under this Act shall not be directly used by any Federal, State, tribal, or local government to regulate, including an enforcement action, the lawful activities of any entity, including an activity relating to monitoring, operating a defensive measure, or sharing of a cyber threat indicator. However, a cyber threat indicator or defensive measure may, consistent with Federal or State regulatory authority specifically relating to the prevention or mitigation of cybersecurity threats to information systems, inform the development or implementation of a regulation relating to such information systems. As previously described, the Committee intends for this exception to be narrowly constrained to improving the government’s understanding of cybersecurity threats. The procedures developed and implemented under this Act are not to be considered regulations within the meaning of this section.

#### *Section 6. Protection from Liability*

Subsection (a) of Section 6 provides that no cause of action shall lie or be maintained in any court against any private entity, and such action shall be promptly dismissed, for the monitoring of information systems and information under Section 4 that is conducted in accordance with this Act. The Committee intends that monitoring for cybersecurity purposes as authorized by this Act should be protected from liability to encourage private entities’ efforts to identify cybersecurity threats.

Subsection (b) provides that no cause of action shall lie or be maintained in any court against any entity, and such action shall be promptly dismissed, for the sharing or receipt of cyber threat indicators or defensive measures under Section 4 when conducted in

accordance with this Act, including cases in which such information is shared with the Federal Government in a manner consistent with subsection (c)(1)(B) of Section 5. Liability protection for the sharing or receipt of cyber threat indicators or defensive measures under Section 4 conducted in accordance with this Act, and in a manner consistent with subsection (c)(1)(B) of Section 5, does not go into effect until the earlier of the date on which the interim policies required under Section 5(a)(1) are submitted to Congress or the date that is 60 days after this Act's date of enactment. In all other cases where the sharing or receipt of cyber threat indicators or defensive measures is conducted in accordance with the Act, liability protection is effective immediately upon enactment of this Act. The Committee intends that the sharing between entities of cyber threat indicators and defensive measures for cybersecurity purposes in accordance with this Act, including the removal of sensitive personal information not directly related to a cybersecurity threat, should be protected from claims. Activities conducted in contravention of this Act's provisions are not entitled to such liability protection, but this Act does not create any cause of action for such non-compliance. When private entities share cyber threat indicators or defensive measures with the Federal Government in a manner consistent with subsection (c)(1)(B) of Section 5, such entities should also not be subject to burdensome litigation. The Committee intends that entities sharing such information with the Federal Government should do so consistently with required procedures to qualify for such protection.

Subsection (c) clarifies that nothing in this section shall be construed to require dismissal of a cause of action against an entity that has engaged in gross negligence or willful misconduct in the course of conducting activities authorized by this Act. Also, nothing in this section shall be construed to undermine or limit the availability of otherwise applicable common law or statutory defenses. The Committee intends to protect the responsible behavior of entities furthering cybersecurity under the authorizations and procedures of this Act, but it does not seek to protect willful or reckless activities that violate the letter and spirit of its provisions. Entities should not use Section 6 as an excuse to engage in wanton or dangerous activities, nor should they consider it to indemnify them for purposes other than the purposes authorized by this Act.

This section does not provide protections from liability arising out of a private entity's use of defensive measures, because it is the Committee's intent to maintain the status quo with respect to the use of cybersecurity defensive measures. While section 4 authorizes the use of defensive measures by an entity on its information networks or the networks of a consenting entity, the Committee notes that the use of defensive measures may have significant impact on those networks or in physical space. The lack of liability protection for the use of defensive measures should not be interpreted as the Committee taking any view on whether and how defensive measures should or should not be implemented.

#### *Section 7. Oversight of Government Activities*

Section 7 mandates reports on implementation and privacy impacts by agency heads, Inspectors General, and the Privacy Civil Liberties Oversight Board to ensure that cyber threat information

is properly received, handled, and shared by the federal government.

*Section 8. Construction and Preemption*

Section 8 contains 19 construction provisions for this Act. Nothing in this Act shall be construed to: (1) limit or prohibit otherwise lawful disclosures of communications, records, or other information; (2) preempt any employee from exercising whistleblower rights currently provided under any law, rule, or regulation; (3) create any immunity against, or otherwise affecting, any action brought by the Federal Government to enforce any law, executive order, or procedure governing the appropriate handling, disclosure, or use of classified information; (4) affect the conduct of authorized law enforcement or intelligence activities; (5) modify the authority of the Federal Government to protect classified information and sources and methods and the national security of the United States; (6) affect any requirement under any other provision of law for an entity to provide information to the Federal Government; (7) 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; (8) limit or modify an existing information sharing relationship; (9) prohibit a new information sharing relationship; (10) require a new information relationship between any entity and the Federal Government; (11) require the use of the DHS capability in Section 5(c); (12) amend, repeal, or supersede any current or future contractual relationship between any entities, or between any entity and the Federal Government; (13) abrogate trade secret or intellectual property rights of any entity or Federal entity; (14) permit the Federal government to require an entity to provide information to the Federal Government; (15) permit the Federal Government to condition the sharing of cyber threat indicators with an entity on such entity's provision of cyber threat indicators to the Federal Government; (16) permit the Federal Government to condition the award of any Federal grant, contract, or purchase on the provision of a cyber threat indicator to a Federal entity; (17) subject any entity to liability for choosing not to engage in the voluntary activities authorized in this Act; (18) authorize, or to modify any existing authority of, a department or agency of the Federal Government to retain or use any information shared under this Act for any use other than permitted in this Act; or (19) limit the authority of the Secretary of Defense to develop, prepare, coordinate, or, when authorized by the President to do so, conduct a military cyber operation in response to a malicious cyber activity carried out against the United States or a United States person by a foreign government or an organization sponsored by a foreign government or a terrorist organization.

This bill supersedes any statute or other law of a State or political subdivision of a State that restricts or otherwise expressly regulates an activity authorized under this bill. However, this bill shall not be construed to supersede any statute or other law of a State or political subdivision of a State concerning the use of authorized law enforcement practices and procedures.

Nothing in this bill shall be construed to authorized the promulgation of any regulations not specifically authorized by this bill, es-

establish any regulatory authority not specifically established under this bill, or to authorize regulatory actions that would duplicate or conflict with regulatory requirements, mandatory standards, or related processes under Federal law.

*Section 9. Report on Cybersecurity Threats*

Section 9 requires the Director of National Intelligence to submit a one-time report to the congressional intelligence committees on cybersecurity threats, including cyber attacks, theft, and data breaches.

*Section 10. Conforming Amendments*

Section 10 makes a technical amendment to 5 U.S.C. 552(b).

Section 10 also makes a conforming amendment to Section 941 of the National Defense Authorization Act for Fiscal Year 2013 (Public Law 112–239) to allow the Secretary of Defense to share information received under that section consistent with this bill.

COMMITTEE ACTION

On March 12, 2015, a quorum being present, the Committee met to consider the bill and amendments. The Committee took the following actions:

*Votes on amendments to committee bill*

By a voice vote, the Committee made the Chairman and Vice Chairman’s bill the base text for purposes of amendment. The Committee also authorized the staff to make technical and conforming changes in the bill following the completion of the markup.

The Committee moved to consideration of the managers’ amendment by the Chairman, which was developed jointly by the Chairman and the Vice Chairman, and adopted the managers’ amendment by a voice vote.

By a vote of 7 ayes to 8 noes, the Committee rejected an amendment by Senator Collins to require entities that own or control information systems that are deemed essential to the operation of designated critical infrastructure to report successful intrusions of those under certain circumstances. According to the amendment, such reporting would only be required with respect to systems where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security. The votes in person or by proxy were as follows: Chairman Burr—no; Senator Risch—no; Senator Coats—aye; Senator Rubio—no; Senator Collins—aye; Senator Blunt—no; Senator Lankford—no; Senator Cotton—no; Vice Chairman Feinstein—no; Senator Wyden—no; Senator Mikulski—aye; Senator Warner—aye; Senator Heinrich—aye; Senator King—aye; Senator Hirono—aye.

By a vote of 3 ayes to 12 noes, the Committee rejected an amendment by Senator Wyden to prohibit the federal government from mandating that private companies deliberately introduce security weaknesses into their products. The votes in person or by proxy were as follows: Chairman Burr—no; Senator Coats—no; Senator Rubio—no; Senator Collins—no; Senator Blunt—no; Senator Lankford—no; Senator Cotton—no; Vice Chairman Feinstein—no;

Senator Wyden—aye; Senator Mikulski— no; Senator Warner— no; Senator Heinrich—aye; Senator King— no; Senator Hirono—aye.

By a voice vote, the Committee adopted an amendment by Senator Heinrich to require the Attorney General develop and make publicly available guidance to assist entities on the types of information that would qualify as cyber threat indicators under the bill and identify types of information that are protected under otherwise applicable privacy laws.

By a voice vote, the Committee adopted an amendment by Senator Hirono and Senator Rubio to place the Attorney General privacy guidelines on the same timeline as the bill requires for the Attorney General policies and procedures for the receipt of cyber threat indicators and defensive measures by the government. The amendment also requires the Attorney General to consult with private entities with industry expertise that are considered relevant before the promulgation of the final privacy guidelines.

*Vote to report the committee bill*

The Committee voted to report the bill as amended, by a vote of 14 ayes to 1 no. Chairman Burr—aye; Senator Risch—aye; Senator Coats—aye; Senator Rubio—aye; Senator Collins—aye; Senator Blunt—aye; Senator Lankford—aye; Senator Cotton—aye; Vice Chairman Feinstein—aye; Senator Wyden—no; Senator Mikulski—aye; Senator Warner—aye; Senator Heinrich—aye; Senator King—aye; Senator Hirono—aye.

COMPLIANCE WITH RULE XLIV

Rule XLIV of the Standing Rules of the Senate requires publication of a list of any “congressionally directed spending item, limited tax benefit, and limited tariff benefit” that is included in the bill or the committee report accompanying the bill. Consistent with the determination of the Committee not to create any congressionally directed spending items or earmarks, none have been included in the bill or this report. The bill and report also contain no limited tax benefits or limited tariff benefits.

ESTIMATE OF COSTS

Pursuant to paragraph 11(a)(1) of rule XXVI of the Standing Rules of the Senate, the Committee estimates that implementing the bill would have a discretionary cost of about \$20 million over the 2015–2019 period, assuming appropriation of the necessary amounts. Enacting S. 754 would not affect direct spending or revenues; therefore pay-as-you-go procedures do not apply. On March 17, 2015, the Committee transmitted this bill to the Congressional Budget Office and requested it to conduct an estimate of the costs incurred in carrying out S. 754.

EVALUATION OF REGULATORY IMPACT

In accordance with paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee finds that no substantial regulatory impact will be incurred by implementing the provisions of this legislation.

## ADDITIONAL VIEWS OF SEN. HEINRICH AND SEN. HIRONO

The rising incidences of cyber attacks on our private and public networks increasingly threaten our economic and national security. Although the enactment of the Cybersecurity Information Sharing Act, or CISA, would not necessarily prevent such attacks, there is a general consensus that facilitating cybersecurity information sharing between the private sector and federal government would promote a common understanding of the threats we face and allow the private sector to more effectively defend its networks.

We supported the Cybersecurity Information Sharing Act during its consideration in the Senate Intelligence Committee because we support the broad aims of this bill. In particular, we agree that individuals, companies, and government institutions can best protect themselves from cyber-attacks when they are aware of the presence and nature of cyber threats. But the only way to ensure the broadest dissemination of threat information is to develop a framework in which that information can be shared and disseminated with appropriate restraints, guidance, and oversight.

The bill as passed out of the Committee provides more restraints, guidance, and oversight than did the earlier draft version of the legislation, including a narrowing of the definition and authorized use of defensive measures, fewer exceptions for liability protections for information shared outside of the DHS portal, and more limits on how cyber threat information is used.

In addition, we are pleased that the Committee adopted amendments we offered during the bill's markup. Senator Heinrich's amendment requires the Attorney General to develop guidance to help private sector companies understand the types of information typically considered to be cyber threat indicators, and the types of personal information generally considered unrelated to such a threat. Senator Hirono's amendment—offered with Senator Rubio—requires the privacy guidelines called for in the bill to be developed and promulgated in a timely and thorough manner, alongside the policies and procedures to be developed for the cyber threat information sharing program.

But we continue to harbor concerns about some of the bill's provisions. Vice Chairman Feinstein noted that the goal of the bill is for companies and the government to voluntarily share information about cybersecurity threats—not about personal information. Our concern is that, however well intended, the bill's provisions do not adequately direct companies to remove personally identifiable information when sharing cyber threat indicators with the government. The bill also lacks a directive that the Department of Homeland Security scrub cyber threat indicators for unnecessary personally identifiable information before sharing that information with other areas of the federal government. Further, the bill confers broad liability protections on companies before requiring them to

abide by privacy guidelines. We believe that the privacy guidelines required in the bill should be treated as a serious component of the new cyber threat sharing regime—not as an afterthought—and thus should be promulgated before the liability protections in this legislation take effect.

Finally, we are unconvinced that it is necessary to create an entirely new exemption to the Freedom of Information Act, or FOIA. Government transparency is critical in order for citizens to hold their elected officials and bureaucrats accountable; however, the bill's inclusion of a new FOIA exemption is overbroad and unnecessary as the types of information shared with the government through this bill would already be exempt from unnecessary public release under current FOIA exemptions. And to the extent FOIA exemptions need to be updated, those changes should only be made following open hearings in which all stakeholders have an opportunity to have their voices heard.

We are committed to addressing some of these issues through amendments on the Senate floor, and believe there should be an open amendment process as this bill moves forward. A number of our colleagues on the Committee offered important amendments during the markup that we hope will be offered again for full Senate consideration—in particular, a number of those offered by Senator Wyden, and one by Sen. Collins to require mandatory reporting of cybersecurity intrusions for the most critical infrastructure owners and operators.

As with other countries around the world, the United States is still just beginning to find ways to confront and mitigate the very real dangers our country faces from cyber threats. Thus far, we have seen no perfect answers. But this bill is not intended to confront every threat. We support it as a way for the government and private sector to begin to address the shared threat that cyber attacks represent, and we will look forward to a robust debate on the floor.

## ADDITIONAL VIEWS OF SENATOR COLLINS

The Cybersecurity Information Sharing Act of 2015 eliminates some of the legal and economic disincentives impeding voluntary two-way information sharing between private industry and government and is a first step in improving our nation's dangerously inadequate defenses against cyber attacks. This bill is insufficient, however, to protect the critical infrastructure of the American people who rely upon this infrastructure for their safety, health, and economic well-being. Simply put, the current threat posed by cyber actors is too great and the vulnerability of existing information systems operating critical infrastructure too widespread to depend solely upon voluntary measures to protect the most essential of these systems upon which our country and citizens depend.

Without information about intrusions into our most critical infrastructure, our government's ability to defend the country against advanced persistent threats will suffer in a domain where speed is critical. This threat is not theoretical. Admiral Mike Rogers, the director of the National Security Agency, has publicly discussed the cyber threat posed against critical infrastructure. In addition to stating his belief that U.S. Cyber Command will be tasked to help defend critical infrastructure, he has said that "We have . . . observed intrusions into industrial control systems . . . what concerns us is that . . . capability can be used by nation-states, groups or individuals to take down the capability of the control systems."

A tiered system of information sharing is part of the solution to address this significant vulnerability. The first tier of reporting should be voluntarily, rely upon the procedures established in this legislation, and be utilized by 99 percent of businesses. The second tier of reporting should be mandatory, and it should apply only to a subset of critical infrastructure where a cybersecurity incident could reasonably be expected to result in *catastrophic* regional or national effects on public health or safety, economic security, or national security.

For this reason, I offered an amendment during the Committee's consideration of the bill to implement this tiered system by requiring the small number of the owners and operators of the country's most critical infrastructure at greatest risk to report to the federal government intrusions of information systems essential to the operation of critical infrastructure.

Had my amendment been adopted, 99.99 percent of businesses and 96 percent of critical infrastructure would still decide for themselves whether or not to share information with the government. The four percent of critical infrastructure at greatest risk of a devastating cyber attack would be mandated to report successful cyber intrusions so the government can develop and deploy countermeasures to protect its networks and the information systems of other critical infrastructure.

The Department of Homeland Security has already identified 63 critical infrastructure entities where damage caused by a single cyber incident could reasonably result in \$50 billion in economic damage or \$25 billion in damage that occurs in conjunction with 2,500 immediate deaths or the severe degradation of our national security or defense. Public reporting by Mandiant in 2013 and repeated testimony of the Intelligence Community leave no doubt that U.S. critical infrastructure already faces advanced persistent cyber threats posed by nation-states and other actors.

The critical infrastructure of the United States remains woefully unprepared to confront this clear and present threat. One former agency head told the 9/11 Commission during its 10th anniversary review that, “We are at September 10th levels in terms of cyber preparedness.” We cannot afford to wait for a “cyber 9/11” before taking legislative action to protect our critical infrastructure. By rejecting my amendment, the Committee is electing to take just such a risk.

SUSAN M. COLLINS.

## ADDITIONAL VIEWS OF SENATOR RON WYDEN

Cyber-attacks and hacking against U.S. companies and networks are a serious and growing problem, with very real consequences for American companies and American consumers, and pose a significant challenge for national security. I share my colleagues' view that Congress should do what it can to help address this problem. The most effective way to protect cybersecurity is to ensure that network owners take responsibility for security and effectively implement good security practices. And it is important to ensure that government agencies do not deliberately weaken security standards.

It also makes sense to encourage private companies to share information about cybersecurity threats. However, this information-sharing must include strong protections for the privacy rights of law-abiding American citizens. Any information-sharing legislation that lacks adequate privacy protections is not simply a cybersecurity bill, but a surveillance bill by another name.

I opposed this bill because I believe its insufficient privacy protections will lead to large amounts of personal information being shared with the government even when that information is not needed for cybersecurity. This could include email content, financial records, and a wide variety of other personal information. While corporations will have a choice about whether or not to participate in this sharing, they could do so without the knowledge or consent of their customers, and will be granted immunity from liability if they do so. Additionally, this bill trumps federal privacy laws and permits government agencies to use the collected information for a wide variety of purposes, rather than only to protect cybersecurity. The bill also creates a problematic double standard, in that personal information about individual consumers can be used for a variety of non-cybersecurity purposes, including law enforcement actions against those consumers, but information about the companies supplying the information generally may not be used to regulate those companies. A corporation's privacy is not more important than an individual's privacy.

This excessively broad collection may not be the intent of this bill, but the language is clearly drafted broadly enough to permit it. Most notably, the bill defines a cybersecurity threat as anything that "may result" in harm to a network. This broad definition will incentivize the sharing of information even when it is *unlikely* to pertain to an actual cybersecurity threat. A more tailored definition, limited to actions that are *reasonably likely* to harm or interfere with a network, would ensure that information-sharing is more narrowly focused on actual threats.

A more tailored approach would also specify that companies should only provide the government with individuals' personal information if it is necessary to describe a cybersecurity threat. This

would discourage companies from unnecessarily sharing large amounts of their customers' private information. This bill unfortunately takes the opposite approach, and only requires private companies to withhold information that is *known* at the time of sharing to be personal information unrelated to cybersecurity. This approach will disincentivize companies from carefully reviewing the information that they share and lead to a much greater amount of personal information being transferred unnecessarily to law enforcement and intelligence agencies.

I am also concerned that this legislation does not provide individuals with an adequate mechanism for redress in cases where the government violates the rules established by this act. Similar bills have included provisions permitting individuals harmed by such violations to recover damages from the government, and such a provision is needed in this bill as well.

I am disappointed that the committee did not adopt stronger privacy protections in this legislation, and I am also disappointed that my amendment to prohibit government agencies from requiring U.S. hardware and software companies to build weaknesses into their products was not adopted. I have introduced this amendment as stand-alone legislation and will continue to pursue this goal.

This bill is likely to significantly increase government collection of individuals' personal information, while unfortunately doing relatively little to secure American networks. I hope to work with colleagues to address this bill's shortcomings, and if these flaws are not fixed I will continue to oppose it.

Finally, I remain very concerned that a secret Justice Department opinion that is of clear relevance to this debate continues to be withheld from the public. This opinion, which interprets common commercial service agreements, is inconsistent with the public's understanding of the law, and I believe it will be difficult for Congress to have a fully informed debate on cybersecurity legislation if it does not understand how these agreements have been interpreted by the Executive Branch.

I have repeatedly asked the Department of Justice to withdraw this opinion, and to release it to the public so that anyone who is a party to one of these agreements can consider whether their agreement should be revised. The deputy head of the Justice Department's Office of Legal Counsel testified to the Intelligence Committee that she would not rely on this opinion today, but I remain concerned that other government officials may be tempted to rely on it in the future. I will continue to press the Justice Department to release this opinion, so that Congress and the public can debate this bill with a full understanding of the facts. And I look forward to working with my colleagues to revise this legislation to ensure that Americans' privacy rights and American cybersecurity are both adequately protected.

CHANGES IN EXISTING LAWS

In the opinion of the Committee, it is necessary to dispense with the requirements of paragraph 12 of rule XXVI of the Standing Rules of the Senate in order to expedite the business of the Senate.



## Calendar No. 28

114TH CONGRESS  
1ST SESSION**S. 754**

To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes.

---

IN THE SENATE OF THE UNITED STATES

MARCH 17, 2015

Mr. BURR, from the Select Committee on Intelligence, reported the following original bill; which was read twice and placed on the calendar

---

**A BILL**

To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*  
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE; TABLE OF CONTENTS.**

4 (a) **SHORT TITLE.**—This Act may be cited as the  
5 “Cybersecurity Information Sharing Act of 2015”.

6 (b) **TABLE OF CONTENTS.**—The table of contents of  
7 this Act is as follows:

Sec. 1. Short title; table of contents.  
Sec. 2. Definitions.

Sec. 3. Sharing of information by the Federal Government.

Sec. 4. Authorizations for preventing, detecting, analyzing, and mitigating cybersecurity threats.

Sec. 5. Sharing of cyber threat indicators and defensive measures with the Federal Government.

Sec. 6. Protection from liability.

Sec. 7. Oversight of Government activities.

Sec. 8. Construction and preemption.

Sec. 9. Report on cybersecurity threats.

Sec. 10. Conforming amendments.

1 **SEC. 2. DEFINITIONS.**

2 In this Act:

3 (1) AGENCY.—The term “agency” has the  
4 meaning given the term in section 3502 of title 44,  
5 United States Code.

6 (2) ANTITRUST LAWS.—The term “antitrust  
7 laws”—

8 (A) has the meaning given the term in sec-  
9 tion 1 of the Clayton Act (15 U.S.C. 12);

10 (B) includes section 5 of the Federal  
11 Trade Commission Act (15 U.S.C. 45) to the  
12 extent that section 5 of that Act applies to un-  
13 fair methods of competition; and

14 (C) includes any State law that has the  
15 same intent and effect as the laws under sub-  
16 paragraphs (A) and (B).

17 (3) APPROPRIATE FEDERAL ENTITIES.—The  
18 term “appropriate Federal entities” means the fol-  
19 lowing:

20 (A) The Department of Commerce.

1 (B) The Department of Defense.

2 (C) The Department of Energy.

3 (D) The Department of Homeland Security.  
4

5 (E) The Department of Justice.

6 (F) The Department of the Treasury.

7 (G) The Office of the Director of National  
8 Intelligence.

9 (4) CYBERSECURITY PURPOSE.—The term “cybersecurity purpose” means the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability.  
10  
11  
12  
13  
14

15 (5) CYBERSECURITY THREAT.—

16 (A) IN GENERAL.—Except as provided in  
17 subparagraph (B), the term “cybersecurity threat” means an action, not protected by the  
18 First Amendment to the Constitution of the  
19 United States, on or through an information  
20 system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on,  
21  
22  
23  
24

1 processed by, or transiting an information sys-  
2 tem.

3 (B) EXCLUSION.—The term “cybersecurity  
4 threat” does not include any action that solely  
5 involves a violation of a consumer term of serv-  
6 ice or a consumer licensing agreement.

7 (6) CYBER THREAT INDICATOR.—The term  
8 “cyber threat indicator” means information that is  
9 necessary to describe or identify—

10 (A) malicious reconnaissance, including  
11 anomalous patterns of communications that ap-  
12 pear to be transmitted for the purpose of gath-  
13 ering technical information related to a cyberse-  
14 curity threat or security vulnerability;

15 (B) a method of defeating a security con-  
16 trol or exploitation of a security vulnerability;

17 (C) a security vulnerability, including  
18 anomalous activity that appears to indicate the  
19 existence of a security vulnerability;

20 (D) a method of causing a user with legiti-  
21 mate access to an information system or infor-  
22 mation that is stored on, processed by, or  
23 transiting an information system to unwittingly  
24 enable the defeat of a security control or exploi-  
25 tation of a security vulnerability;

1 (E) malicious cyber command and control;

2 (F) the actual or potential harm caused by  
3 an incident, including a description of the infor-  
4 mation exfiltrated as a result of a particular cy-  
5 bersecurity threat;

6 (G) any other attribute of a cybersecurity  
7 threat, if disclosure of such attribute is not oth-  
8 erwise prohibited by law; or

9 (H) any combination thereof.

10 (7) DEFENSIVE MEASURE.—

11 (A) IN GENERAL.—Except as provided in  
12 subparagraph (B), the term “defensive meas-  
13 ure” means an action, device, procedure, signa-  
14 ture, technique, or other measure applied to an  
15 information system or information that is  
16 stored on, processed by, or transiting an infor-  
17 mation system that detects, prevents, or miti-  
18 gates a known or suspected cybersecurity threat  
19 or security vulnerability.

20 (B) EXCLUSION.—The term “defensive  
21 measure” does not include a measure that de-  
22 stroys, renders unusable, or substantially harms  
23 an information system or data on an informa-  
24 tion system not belonging to—

1 (i) the private entity operating the  
2 measure; or

3 (ii) another entity or Federal entity  
4 that is authorized to provide consent and  
5 has provided consent to that private entity  
6 for operation of such measure.

7 (8) ENTITY.—

8 (A) IN GENERAL.—Except as otherwise  
9 provided in this paragraph, the term “entity”  
10 means any private entity, non-Federal govern-  
11 ment agency or department, or State, tribal, or  
12 local government (including a political subdivi-  
13 sion, department, or component thereof).

14 (B) INCLUSIONS.—The term “entity” in-  
15 cludes a government agency or department of  
16 the District of Columbia, the Commonwealth of  
17 Puerto Rico, the Virgin Islands, Guam, Amer-  
18 ican Samoa, the Northern Mariana Islands, and  
19 any other territory or possession of the United  
20 States.

21 (C) EXCLUSION.—The term “entity” does  
22 not include a foreign power as defined in sec-  
23 tion 101 of the Foreign Intelligence Surveil-  
24 lance Act of 1978 (50 U.S.C. 1801).

1           (9) FEDERAL ENTITY.—The term “Federal en-  
2           tity” means a department or agency of the United  
3           States or any component of such department or  
4           agency.

5           (10) INFORMATION SYSTEM.—The term “infor-  
6           mation system”—

7                   (A) has the meaning given the term in sec-  
8                   tion 3502 of title 44, United States Code; and

9                   (B) includes industrial control systems,  
10                  such as supervisory control and data acquisition  
11                  systems, distributed control systems, and pro-  
12                  grammable logic controllers.

13           (11) LOCAL GOVERNMENT.—The term “local  
14           government” means any borough, city, county, par-  
15           ish, town, township, village, or other political sub-  
16           division of a State.

17           (12) MALICIOUS CYBER COMMAND AND CON-  
18           TROL.—The term “malicious cyber command and  
19           control” means a method for unauthorized remote  
20           identification of, access to, or use of, an information  
21           system or information that is stored on, processed  
22           by, or transiting an information system.

23           (13) MALICIOUS RECONNAISSANCE.—The term  
24           “malicious reconnaissance” means a method for ac-  
25           tively probing or passively monitoring an information

1 system for the purpose of discerning security  
2 vulnerabilities of the information system, if such  
3 method is associated with a known or suspected cy-  
4 bersecurity threat.

5 (14) MONITOR.—The term “monitor” means to  
6 acquire, identify, or scan, or to possess, information  
7 that is stored on, processed by, or transiting an in-  
8 formation system.

9 (15) PRIVATE ENTITY.—

10 (A) IN GENERAL.—Except as otherwise  
11 provided in this paragraph, the term “private  
12 entity” means any person or private group, or-  
13 ganization, proprietorship, partnership, trust,  
14 cooperative, corporation, or other commercial or  
15 nonprofit entity, including an officer, employee,  
16 or agent thereof.

17 (B) INCLUSION.—The term “private enti-  
18 ty” includes a State, tribal, or local government  
19 performing electric utility services.

20 (C) EXCLUSION.—The term “private enti-  
21 ty” does not include a foreign power as defined  
22 in section 101 of the Foreign Intelligence Sur-  
23 veillance Act of 1978 (50 U.S.C. 1801).

24 (16) SECURITY CONTROL.—The term “security  
25 control” means the management, operational, and

1 technical controls used to protect against an unau-  
2 thORIZED effort to adversely affect the confidentiality,  
3 integrity, and availability of an information system  
4 or its information.

5 (17) SECURITY VULNERABILITY.—The term  
6 “security vulnerability” means any attribute of hard-  
7 ware, software, process, or procedure that could en-  
8 able or facilitate the defeat of a security control.

9 (18) TRIBAL.—The term “tribal” has the  
10 meaning given the term “Indian tribe” in section 4  
11 of the Indian Self-Determination and Education As-  
12 sistance Act (25 U.S.C. 450b).

13 **SEC. 3. SHARING OF INFORMATION BY THE FEDERAL GOV-**  
14 **ERNMENT.**

15 (a) IN GENERAL.—Consistent with the protection of  
16 classified information, intelligence sources and methods,  
17 and privacy and civil liberties, the Director of National  
18 Intelligence, the Secretary of Homeland Security, the Sec-  
19 retary of Defense, and the Attorney General, in consulta-  
20 tion with the heads of the appropriate Federal entities,  
21 shall develop and promulgate procedures to facilitate and  
22 promote—

23 (1) the timely sharing of classified cyber threat  
24 indicators in the possession of the Federal Govern-

1 ment with cleared representatives of relevant enti-  
2 ties;

3 (2) the timely sharing with relevant entities of  
4 cyber threat indicators or information in the posses-  
5 sion of the Federal Government that may be declas-  
6 sified and shared at an unclassified level;

7 (3) the sharing with relevant entities, or the  
8 public if appropriate, of unclassified, including con-  
9 trolled unclassified, cyber threat indicators in the  
10 possession of the Federal Government; and

11 (4) the sharing with entities, if appropriate, of  
12 information in the possession of the Federal Govern-  
13 ment about cybersecurity threats to such entities to  
14 prevent or mitigate adverse effects from such cyber-  
15 security threats.

16 (b) DEVELOPMENT OF PROCEDURES.—

17 (1) IN GENERAL.—The procedures developed  
18 and promulgated under subsection (a) shall—

19 (A) ensure the Federal Government has  
20 and maintains the capability to share cyber  
21 threat indicators in real time consistent with  
22 the protection of classified information;

23 (B) incorporate, to the greatest extent  
24 practicable, existing processes and existing roles  
25 and responsibilities of Federal and non-Federal

1 entities for information sharing by the Federal  
2 Government, including sector specific informa-  
3 tion sharing and analysis centers;

4 (C) include procedures for notifying enti-  
5 ties that have received a cyber threat indicator  
6 from a Federal entity under this Act that is  
7 known or determined to be in error or in con-  
8 travention of the requirements of this Act or  
9 another provision of Federal law or policy of  
10 such error or contravention;

11 (D) include requirements for Federal enti-  
12 ties receiving cyber threat indicators or defen-  
13 sive measures to implement and utilize security  
14 controls to protect against unauthorized access  
15 to or acquisition of such cyber threat indicators  
16 or defensive measures; and

17 (E) include procedures that require a Fed-  
18 eral entity, prior to the sharing of a cyber  
19 threat indicator—

20 (i) to review such cyber threat indi-  
21 cator to assess whether such cyber threat  
22 indicator contains any information that  
23 such Federal entity knows at the time of  
24 sharing to be personal information of or  
25 identifying a specific person not directly

1 related to a cybersecurity threat and re-  
2 move such information; or

3 (ii) to implement and utilize a tech-  
4 nical capability configured to remove any  
5 personal information of or identifying a  
6 specific person not directly related to a cy-  
7 bersecurity threat.

8 (2) COORDINATION.—In developing the proce-  
9 dures required under this section, the Director of  
10 National Intelligence, the Secretary of Homeland Se-  
11 curity, the Secretary of Defense, and the Attorney  
12 General shall coordinate with appropriate Federal  
13 entities, including the National Laboratories (as de-  
14 fined in section 2 of the Energy Policy Act of 2005  
15 (42 U.S.C. 15801)), to ensure that effective proto-  
16 cols are implemented that will facilitate and promote  
17 the sharing of cyber threat indicators by the Federal  
18 Government in a timely manner.

19 (c) SUBMITTAL TO CONGRESS.—Not later than 60  
20 days after the date of the enactment of this Act, the Direc-  
21 tor of National Intelligence, in consultation with the heads  
22 of the appropriate Federal entities, shall submit to Con-  
23 gress the procedures required by subsection (a).

1 **SEC. 4. AUTHORIZATIONS FOR PREVENTING, DETECTING,**  
2 **ANALYZING, AND MITIGATING CYBERSECU-**  
3 **RITY THREATS.**

4 (a) AUTHORIZATION FOR MONITORING.—

5 (1) IN GENERAL.—Notwithstanding any other  
6 provision of law, a private entity may, for cybersecu-  
7 rity purposes, monitor—

8 (A) an information system of such private  
9 entity;

10 (B) an information system of another enti-  
11 ty, upon the authorization and written consent  
12 of such other entity;

13 (C) an information system of a Federal en-  
14 tity, upon the authorization and written consent  
15 of an authorized representative of the Federal  
16 entity; and

17 (D) information that is stored on, proc-  
18 essed by, or transiting an information system  
19 monitored by the private entity under this para-  
20 graph.

21 (2) CONSTRUCTION.—Nothing in this sub-  
22 section shall be construed—

23 (A) to authorize the monitoring of an in-  
24 formation system, or the use of any information  
25 obtained through such monitoring, other than  
26 as provided in this Act; or

1 (B) to limit otherwise lawful activity.

2 (b) AUTHORIZATION FOR OPERATION OF DEFENSIVE  
3 MEASURES.—

4 (1) IN GENERAL.—Notwithstanding any other  
5 provision of law, a private entity may, for cybersecu-  
6 rity purposes, operate a defensive measure that is  
7 applied to—

8 (A) an information system of such private  
9 entity in order to protect the rights or property  
10 of the private entity;

11 (B) an information system of another enti-  
12 ty upon written consent of such entity for oper-  
13 ation of such defensive measure to protect the  
14 rights or property of such entity; and

15 (C) an information system of a Federal en-  
16 tity upon written consent of an authorized rep-  
17 resentative of such Federal entity for operation  
18 of such defensive measure to protect the rights  
19 or property of the Federal Government.

20 (2) CONSTRUCTION.—Nothing in this sub-  
21 section shall be construed—

22 (A) to authorize the use of a defensive  
23 measure other than as provided in this sub-  
24 section; or

25 (B) to limit otherwise lawful activity.

1 (c) AUTHORIZATION FOR SHARING OR RECEIVING  
2 CYBER THREAT INDICATORS OR DEFENSIVE MEAS-  
3 URES.—

4 (1) IN GENERAL.—Except as provided in para-  
5 graph (2) and notwithstanding any other provision  
6 of law, an entity may, for the purposes permitted  
7 under this Act and consistent with the protection of  
8 classified information, share with, or receive from,  
9 any other entity or the Federal Government a cyber  
10 threat indicator or defensive measure.

11 (2) LAWFUL RESTRICTION.—An entity receiving  
12 a cyber threat indicator or defensive measure from  
13 another entity or Federal entity shall comply with  
14 otherwise lawful restrictions placed on the sharing or  
15 use of such cyber threat indicator or defensive meas-  
16 ure by the sharing entity or Federal entity.

17 (3) CONSTRUCTION.—Nothing in this sub-  
18 section shall be construed—

19 (A) to authorize the sharing or receiving of  
20 a cyber threat indicator or defensive measure  
21 other than as provided in this subsection; or

22 (B) to limit otherwise lawful activity.

23 (d) PROTECTION AND USE OF INFORMATION.—

24 (1) SECURITY OF INFORMATION.—An entity  
25 monitoring an information system, operating a de-

1       fensive measure, or providing or receiving a cyber  
2       threat indicator or defensive measure under this sec-  
3       tion shall implement and utilize a security control to  
4       protect against unauthorized access to or acquisition  
5       of such cyber threat indicator or defensive measure.

6               (2) REMOVAL OF CERTAIN PERSONAL INFORMA-  
7       TION.—An entity sharing a cyber threat indicator  
8       pursuant to this Act shall, prior to such sharing—

9               (A) review such cyber threat indicator to  
10       assess whether such cyber threat indicator con-  
11       tains any information that the entity knows at  
12       the time of sharing to be personal information  
13       of or identifying a specific person not directly  
14       related to a cybersecurity threat and remove  
15       such information; or

16              (B) implement and utilize a technical capa-  
17       bility configured to remove any information  
18       contained within such indicator that the entity  
19       knows at the time of sharing to be personal in-  
20       formation of or identifying a specific person not  
21       directly related to a cybersecurity threat.

22              (3) USE OF CYBER THREAT INDICATORS AND  
23       DEFENSIVE MEASURES BY ENTITIES.—

24              (A) IN GENERAL.—Consistent with this  
25       Act, a cyber threat indicator or defensive meas-

1           ure shared or received under this section may,  
2           for cybersecurity purposes—

3                   (i) be used by an entity to monitor or  
4                   operate a defensive measure on—

5                           (I) an information system of the  
6                           entity; or

7                           (II) an information system of an-  
8                           other entity or a Federal entity upon  
9                           the written consent of that other enti-  
10                          ty or that Federal entity; and

11                   (ii) be otherwise used, retained, and  
12                   further shared by an entity subject to—

13                           (I) an otherwise lawful restriction  
14                           placed by the sharing entity or Fed-  
15                           eral entity on such cyber threat indi-  
16                           cator or defensive measure; or

17                           (II) an otherwise applicable pro-  
18                           vision of law.

19                   (B) CONSTRUCTION.—Nothing in this  
20                   paragraph shall be construed to authorize the  
21                   use of a cyber threat indicator or defensive  
22                   measure other than as provided in this section.

23                   (4) USE OF CYBER THREAT INDICATORS BY  
24                   STATE, TRIBAL, OR LOCAL GOVERNMENT.—

25                           (A) LAW ENFORCEMENT USE.—

1 (i) PRIOR WRITTEN CONSENT.—Ex-  
2 cept as provided in clause (ii), a cyber  
3 threat indicator shared with a State, tribal,  
4 or local government under this section  
5 may, with the prior written consent of the  
6 entity sharing such indicator, be used by a  
7 State, tribal, or local government for the  
8 purpose of preventing, investigating, or  
9 prosecuting any of the offenses described  
10 in section 5(d)(5)(A)(vi).

11 (ii) ORAL CONSENT.—If exigent cir-  
12 cumstances prevent obtaining written con-  
13 sent under clause (i), such consent may be  
14 provided orally with subsequent docu-  
15 mentation of the consent.

16 (B) EXEMPTION FROM DISCLOSURE.—A  
17 cyber threat indicator shared with a State, trib-  
18 al, or local government under this section shall  
19 be—

20 (i) deemed voluntarily shared informa-  
21 tion; and

22 (ii) exempt from disclosure under any  
23 State, tribal, or local law requiring disclo-  
24 sure of information or records.

1 (C) STATE, TRIBAL, AND LOCAL REGU-  
2 LATORY AUTHORITY.—

3 (i) IN GENERAL.—Except as provided  
4 in clause (ii), a cyber threat indicator or  
5 defensive measure shared with a State,  
6 tribal, or local government under this Act  
7 shall not be directly used by any State,  
8 tribal, or local government to regulate, in-  
9 cluding an enforcement action, the lawful  
10 activity of any entity, including an activity  
11 relating to monitoring, operating a defen-  
12 sive measure, or sharing of a cyber threat  
13 indicator.

14 (ii) REGULATORY AUTHORITY SPE-  
15 CIFICALLY RELATING TO PREVENTION OR  
16 MITIGATION OF CYBERSECURITY  
17 THREATS.—A cyber threat indicator or de-  
18 fensive measures shared as described in  
19 clause (i) may, consistent with a State,  
20 tribal, or local government regulatory au-  
21 thority specifically relating to the preven-  
22 tion or mitigation of cybersecurity threats  
23 to information systems, inform the devel-  
24 opment or implementation of a regulation  
25 relating to such information systems.

1 (e) ANTITRUST EXEMPTION.—

2 (1) IN GENERAL.—Except as provided in sec-  
3 tion 8(e), it shall not be considered a violation of  
4 any provision of antitrust laws for 2 or more private  
5 entities to exchange or provide a cyber threat indi-  
6 cator, or assistance relating to the prevention, inves-  
7 tigation, or mitigation of a cybersecurity threat, for  
8 cybersecurity purposes under this Act.

9 (2) APPLICABILITY.—Paragraph (1) shall apply  
10 only to information that is exchanged or assistance  
11 provided in order to assist with—

12 (A) facilitating the prevention, investiga-  
13 tion, or mitigation of a cybersecurity threat to  
14 an information system or information that is  
15 stored on, processed by, or transiting an infor-  
16 mation system; or

17 (B) communicating or disclosing a cyber  
18 threat indicator to help prevent, investigate, or  
19 mitigate the effect of a cybersecurity threat to  
20 an information system or information that is  
21 stored on, processed by, or transiting an infor-  
22 mation system.

23 (f) NO RIGHT OR BENEFIT.—The sharing of a cyber  
24 threat indicator with an entity under this Act shall not

1 create a right or benefit to similar information by such  
2 entity or any other entity.

3 **SEC. 5. SHARING OF CYBER THREAT INDICATORS AND DE-**  
4 **FENSIVE MEASURES WITH THE FEDERAL**  
5 **GOVERNMENT.**

6 (a) REQUIREMENT FOR POLICIES AND PROCE-  
7 DURES.—

8 (1) INTERIM POLICIES AND PROCEDURES.—Not  
9 later than 60 days after the date of the enactment  
10 of this Act, the Attorney General, in coordination  
11 with the heads of the appropriate Federal entities,  
12 shall develop and submit to Congress interim policies  
13 and procedures relating to the receipt of cyber  
14 threat indicators and defensive measures by the  
15 Federal Government.

16 (2) FINAL POLICIES AND PROCEDURES.—Not  
17 later than 180 days after the date of the enactment  
18 of this Act, the Attorney General shall, in coordina-  
19 tion with the heads of the appropriate Federal enti-  
20 ties, promulgate final policies and procedures relat-  
21 ing to the receipt of cyber threat indicators and de-  
22 fensive measures by the Federal Government.

23 (3) REQUIREMENTS CONCERNING POLICIES AND  
24 PROCEDURES.—Consistent with the guidelines re-  
25 quired by subsection (b), the policies and procedures

1 developed and promulgated under this subsection  
2 shall—

3 (A) ensure that cyber threat indicators are  
4 shared with the Federal Government by any en-  
5 tity pursuant to section 4(c) through the real-  
6 time process described in subsection (c) of this  
7 section—

8 (i) are shared in an automated man-  
9 ner with all of the appropriate Federal en-  
10 tities;

11 (ii) are not subject to any delay, modi-  
12 fication, or any other action that could im-  
13 pede real-time receipt by all of the appro-  
14 priate Federal entities; and

15 (iii) may be provided to other Federal  
16 entities;

17 (B) ensure that cyber threat indicators  
18 shared with the Federal Government by any en-  
19 tity pursuant to section 4 in a manner other  
20 than the real-time process described in sub-  
21 section (c) of this section—

22 (i) are shared as quickly as operation-  
23 ally practicable with all of the appropriate  
24 Federal entities;

1           (ii) are not subject to any unnecessary  
2           delay, interference, or any other action  
3           that could impede receipt by all of the ap-  
4           propriate Federal entities; and

5           (iii) may be provided to other Federal  
6           entities;

7           (C) consistent with this Act, any other ap-  
8           plicable provisions of law, and the fair informa-  
9           tion practice principles set forth in appendix A  
10          of the document entitled “National Strategy for  
11          Trusted Identities in Cyberspace” and pub-  
12          lished by the President in April 2011, govern  
13          the retention, use, and dissemination by the  
14          Federal Government of cyber threat indicators  
15          shared with the Federal Government under this  
16          Act, including the extent, if any, to which such  
17          cyber threat indicators may be used by the Fed-  
18          eral Government; and

19          (D) ensure there is—

20               (i) an audit capability; and

21               (ii) appropriate sanctions in place for  
22               officers, employees, or agents of a Federal  
23               entity who knowingly and willfully conduct  
24               activities under this Act in an unauthor-  
25               ized manner.

1           (4) GUIDELINES FOR ENTITIES SHARING CYBER  
2 THREAT INDICATORS WITH FEDERAL GOVERN-  
3 MENT.—

4           (A) IN GENERAL.—Not later than 60 days  
5 after the date of the enactment of this Act, the  
6 Attorney General shall develop and make pub-  
7 licly available guidance to assist entities and  
8 promote sharing of cyber threat indicators with  
9 Federal entities under this Act.

10          (B) CONTENTS.—The guidelines developed  
11 and made publicly available under subpara-  
12 graph (A) shall include guidance on the fol-  
13 lowing:

14           (i) Identification of types of informa-  
15 tion that would qualify as a cyber threat  
16 indicator under this Act that would be un-  
17 likely to include personal information of or  
18 identifying a specific person not directly  
19 related to a cyber security threat.

20           (ii) Identification of types of informa-  
21 tion protected under otherwise applicable  
22 privacy laws that are unlikely to be directly  
23 related to a cybersecurity threat.

24           (iii) Such other matters as the Attor-  
25 ney General considers appropriate for enti-

1                   ties sharing cyber threat indicators with  
2                   Federal entities under this Act.

3           (b) PRIVACY AND CIVIL LIBERTIES.—

4                   (1) GUIDELINES OF ATTORNEY GENERAL.—Not  
5           later than 60 days after the date of the enactment  
6           of this Act, the Attorney General shall, in coordina-  
7           tion with heads of the appropriate Federal entities  
8           and in consultation with officers designated under  
9           section 1062 of the National Security Intelligence  
10          Reform Act of 2004 (42 U.S.C. 2000ee–1), develop,  
11          submit to Congress, and make available to the public  
12          interim guidelines relating to privacy and civil lib-  
13          erties which shall govern the receipt, retention, use,  
14          and dissemination of cyber threat indicators by a  
15          Federal entity obtained in connection with activities  
16          authorized in this Act.

17                  (2) FINAL GUIDELINES.—

18                          (A) IN GENERAL.—Not later than 180  
19           days after the date of the enactment of this  
20           Act, the Attorney General shall, in coordination  
21           with heads of the appropriate Federal entities  
22           and in consultation with officers designated  
23           under section 1062 of the National Security In-  
24           telligence Reform Act of 2004 (42 U.S.C.  
25           2000ee–1) and such private entities with indus-

1 try expertise as the Attorney General considers  
2 relevant, promulgate final guidelines relating to  
3 privacy and civil liberties which shall govern the  
4 receipt, retention, use, and dissemination of  
5 cyber threat indicators by a Federal entity ob-  
6 tained in connection with activities authorized  
7 in this Act.

8 (B) PERIODIC REVIEW.—The Attorney  
9 General shall, in coordination with heads of the  
10 appropriate Federal entities and in consultation  
11 with officers and private entities described in  
12 subparagraph (A), periodically review the guide-  
13 lines promulgated under subparagraph (A).

14 (3) CONTENT.—The guidelines required by  
15 paragraphs (1) and (2) shall, consistent with the  
16 need to protect information systems from cybersecu-  
17 rity threats and mitigate cybersecurity threats—

18 (A) limit the impact on privacy and civil  
19 liberties of activities by the Federal Government  
20 under this Act;

21 (B) limit the receipt, retention, use, and  
22 dissemination of cyber threat indicators con-  
23 taining personal information of or identifying  
24 specific persons, including by establishing—

1 (i) a process for the timely destruction  
2 of such information that is known not to  
3 be directly related to uses authorized under  
4 this Act; and

5 (ii) specific limitations on the length  
6 of any period in which a cyber threat indi-  
7 cator may be retained;

8 (C) include requirements to safeguard  
9 cyber threat indicators containing personal in-  
10 formation of or identifying specific persons  
11 from unauthorized access or acquisition, includ-  
12 ing appropriate sanctions for activities by offi-  
13 cers, employees, or agents of the Federal Gov-  
14 ernment in contravention of such guidelines;

15 (D) include procedures for notifying enti-  
16 ties and Federal entities if information received  
17 pursuant to this section is known or determined  
18 by a Federal entity receiving such information  
19 not to constitute a cyber threat indicator;

20 (E) protect the confidentiality of cyber  
21 threat indicators containing personal informa-  
22 tion of or identifying specific persons to the  
23 greatest extent practicable and require recipi-  
24 ents to be informed that such indicators may

1           only be used for purposes authorized under this  
2           Act; and

3                   (F) include steps that may be needed so  
4           that dissemination of cyber threat indicators is  
5           consistent with the protection of classified and  
6           other sensitive national security information.

7           (c) CAPABILITY AND PROCESS WITHIN THE DEPART-  
8   MENT OF HOMELAND SECURITY.—

9                   (1) IN GENERAL.—Not later than 90 days after  
10          the date of the enactment of this Act, the Secretary  
11          of Homeland Security, in coordination with the  
12          heads of the appropriate Federal entities, shall de-  
13          velop and implement a capability and process within  
14          the Department of Homeland Security that—

15                   (A) shall accept from any entity in real  
16          time cyber threat indicators and defensive  
17          measures, pursuant to this section;

18                   (B) shall, upon submittal of the certifi-  
19          cation under paragraph (2) that such capability  
20          and process fully and effectively operates as de-  
21          scribed in such paragraph, be the process by  
22          which the Federal Government receives cyber  
23          threat indicators and defensive measures under  
24          this Act that are shared by a private entity with  
25          the Federal Government through electronic mail

1 or media, an interactive form on an Internet  
2 website, or a real time, automated process be-  
3 tween information systems except—

4 (i) communications between a Federal  
5 entity and a private entity regarding a pre-  
6 viously shared cyber threat indicator; and

7 (ii) communications by a regulated en-  
8 tity with such entity's Federal regulatory  
9 authority regarding a cybersecurity threat;

10 (C) ensures that all of the appropriate  
11 Federal entities receive in an automated man-  
12 ner such cyber threat indicators shared through  
13 the real-time process within the Department of  
14 Homeland Security;

15 (D) is in compliance with the policies, pro-  
16 cedures, and guidelines required by this section;  
17 and

18 (E) does not limit or prohibit otherwise  
19 lawful disclosures of communications, records,  
20 or other information, including—

21 (i) reporting of known or suspected  
22 criminal activity, by an entity to any other  
23 entity or a Federal entity;

24 (ii) voluntary or legally compelled par-  
25 ticipation in a Federal investigation; and

1 (iii) providing cyber threat indicators  
2 or defensive measures as part of a statu-  
3 tory or authorized contractual requirement.

4 (2) CERTIFICATION.—Not later than 10 days  
5 prior to the implementation of the capability and  
6 process required by paragraph (1), the Secretary of  
7 Homeland Security shall, in consultation with the  
8 heads of the appropriate Federal entities, certify to  
9 Congress whether such capability and process fully  
10 and effectively operates—

11 (A) as the process by which the Federal  
12 Government receives from any entity a cyber  
13 threat indicator or defensive measure under this  
14 Act; and

15 (B) in accordance with the policies, proce-  
16 dures, and guidelines developed under this sec-  
17 tion.

18 (3) PUBLIC NOTICE AND ACCESS.—The Sec-  
19 retary of Homeland Security shall ensure there is  
20 public notice of, and access to, the capability and  
21 process developed and implemented under paragraph  
22 (1) so that—

23 (A) any entity may share cyber threat indi-  
24 cators and defensive measures through such  
25 process with the Federal Government; and

1           (B) all of the appropriate Federal entities  
2           receive such cyber threat indicators and defen-  
3           sive measures in real time with receipt through  
4           the process within the Department of Home-  
5           land Security.

6           (4) OTHER FEDERAL ENTITIES.—The process  
7           developed and implemented under paragraph (1)  
8           shall ensure that other Federal entities receive in a  
9           timely manner any cyber threat indicators and de-  
10          fensive measures shared with the Federal Govern-  
11          ment through such process.

12          (5) REPORT ON DEVELOPMENT AND IMPLE-  
13          MENTATION.—

14               (A) IN GENERAL.—Not later than 60 days  
15               after the date of the enactment of this Act, the  
16               Secretary of Homeland Security shall submit to  
17               Congress a report on the development and im-  
18               plementation of the capability and process re-  
19               quired by paragraph (1), including a description  
20               of such capability and process and the public  
21               notice of, and access to, such process.

22               (B) CLASSIFIED ANNEX.—The report re-  
23               quired by subparagraph (A) shall be submitted  
24               in unclassified form, but may include a classi-  
25               fied annex.

1 (d) INFORMATION SHARED WITH OR PROVIDED TO  
2 THE FEDERAL GOVERNMENT.—

3 (1) NO WAIVER OF PRIVILEGE OR PROTEC-  
4 TION.—The provision of cyber threat indicators and  
5 defensive measures to the Federal Government  
6 under this Act shall not constitute a waiver of any  
7 applicable privilege or protection provided by law, in-  
8 cluding trade secret protection.

9 (2) PROPRIETARY INFORMATION.—Consistent  
10 with section 4(e)(2), a cyber threat indicator or de-  
11 fensive measure provided by an entity to the Federal  
12 Government under this Act shall be considered the  
13 commercial, financial, and proprietary information of  
14 such entity when so designated by the originating  
15 entity or a third party acting in accordance with the  
16 written authorization of the originating entity.

17 (3) EXEMPTION FROM DISCLOSURE.—Cyber  
18 threat indicators and defensive measures provided to  
19 the Federal Government under this Act shall be—

20 (A) deemed voluntarily shared information  
21 and exempt from disclosure under section 552  
22 of title 5, United States Code, and any State,  
23 tribal, or local law requiring disclosure of infor-  
24 mation or records; and

1 (B) withheld, without discretion, from the  
2 public under section 552(b)(3)(B) of title 5,  
3 United States Code, and any State, tribal, or  
4 local provision of law requiring disclosure of in-  
5 formation or records.

6 (4) EX PARTE COMMUNICATIONS.—The provi-  
7 sion of a cyber threat indicator or defensive measure  
8 to the Federal Government under this Act shall not  
9 be subject to a rule of any Federal agency or depart-  
10 ment or any judicial doctrine regarding ex parte  
11 communications with a decisionmaking official.

12 (5) DISCLOSURE, RETENTION, AND USE.—

13 (A) AUTHORIZED ACTIVITIES.—Cyber  
14 threat indicators and defensive measures pro-  
15 vided to the Federal Government under this Act  
16 may be disclosed to, retained by, and used by,  
17 consistent with otherwise applicable provisions  
18 of Federal law, any Federal agency or depart-  
19 ment, component, officer, employee, or agent of  
20 the Federal Government solely for—

21 (i) a cybersecurity purpose;

22 (ii) the purpose of identifying a cyber-  
23 security threat, including the source of  
24 such cybersecurity threat, or a security  
25 vulnerability;

1 (iii) the purpose of identifying a cy-  
2 bersecurity threat involving the use of an  
3 information system by a foreign adversary  
4 or terrorist;

5 (iv) the purpose of responding to, or  
6 otherwise preventing or mitigating, an im-  
7 minent threat of death, serious bodily  
8 harm, or serious economic harm, including  
9 a terrorist act or a use of a weapon of  
10 mass destruction;

11 (v) the purpose of responding to, or  
12 otherwise preventing or mitigating, a seri-  
13 ous threat to a minor, including sexual ex-  
14 ploitation and threats to physical safety; or

15 (vi) the purpose of preventing, inves-  
16 tigating, disrupting, or prosecuting an of-  
17 fense arising out of a threat described in  
18 clause (iv) or any of the offenses listed  
19 in—

20 (I) section 3559(c)(2)(F) of title  
21 18, United States Code (relating to  
22 serious violent felonies);

23 (II) sections 1028 through 1030  
24 of such title (relating to fraud and  
25 identity theft);

1 (III) chapter 37 of such title (re-  
2 lating to espionage and censorship);  
3 and

4 (IV) chapter 90 of such title (re-  
5 lating to protection of trade secrets).

6 (B) PROHIBITED ACTIVITIES.—Cyber  
7 threat indicators and defensive measures pro-  
8 vided to the Federal Government under this Act  
9 shall not be disclosed to, retained by, or used  
10 by any Federal agency or department for any  
11 use not permitted under subparagraph (A).

12 (C) PRIVACY AND CIVIL LIBERTIES.—  
13 Cyber threat indicators and defensive measures  
14 provided to the Federal Government under this  
15 Act shall be retained, used, and disseminated by  
16 the Federal Government—

17 (i) in accordance with the policies,  
18 procedures, and guidelines required by sub-  
19 sections (a) and (b);

20 (ii) in a manner that protects from  
21 unauthorized use or disclosure any cyber  
22 threat indicators that may contain personal  
23 information of or identifying specific per-  
24 sons; and

1 (iii) in a manner that protects the  
2 confidentiality of cyber threat indicators  
3 containing personal information of or iden-  
4 tifying a specific person.

5 (D) FEDERAL REGULATORY AUTHORITY.—

6 (i) IN GENERAL.—Except as provided  
7 in clause (ii), cyber threat indicators and  
8 defensive measures provided to the Federal  
9 Government under this Act shall not be di-  
10 rectly used by any Federal, State, tribal,  
11 or local government to regulate, including  
12 an enforcement action, the lawful activities  
13 of any entity, including activities relating  
14 to monitoring, operating defensive meas-  
15 ures, or sharing cyber threat indicators.

16 (ii) EXCEPTIONS.—

17 (I) REGULATORY AUTHORITY  
18 SPECIFICALLY RELATING TO PREVEN-  
19 TION OR MITIGATION OF CYBERSECU-  
20 RITY THREATS.—Cyber threat indica-  
21 tors and defensive measures provided  
22 to the Federal Government under this  
23 Act may, consistent with Federal or  
24 State regulatory authority specifically  
25 relating to the prevention or mitiga-

1                   tion of cybersecurity threats to infor-  
2                   mation systems, inform the develop-  
3                   ment or implementation of regulations  
4                   relating to such information systems.

5                   (II) PROCEDURES DEVELOPED  
6                   AND IMPLEMENTED UNDER THIS  
7                   ACT.—Clause (i) shall not apply to  
8                   procedures developed and imple-  
9                   mented under this Act.

10 **SEC. 6. PROTECTION FROM LIABILITY.**

11           (a) MONITORING OF INFORMATION SYSTEMS.—No  
12 cause of action shall lie or be maintained in any court  
13 against any private entity, and such action shall be  
14 promptly dismissed, for the monitoring of information sys-  
15 tems and information under section 4(a) that is conducted  
16 in accordance with this Act.

17           (b) SHARING OR RECEIPT OF CYBER THREAT INDI-  
18 CATORS.—No cause of action shall lie or be maintained  
19 in any court against any entity, and such action shall be  
20 promptly dismissed, for the sharing or receipt of cyber  
21 threat indicators or defensive measures under section 4(c)  
22 if—

23                   (1) such sharing or receipt is conducted in ac-  
24                   cordance with this Act; and

1           (2) in a case in which a cyber threat indicator  
2 or defensive measure is shared with the Federal  
3 Government, the cyber threat indicator or defensive  
4 measure is shared in a manner that is consistent  
5 with section 5(c)(1)(B) and the sharing or receipt,  
6 as the case may be, occurs after the earlier of—

7           (A) the date on which the interim policies  
8 and procedures are submitted to Congress  
9 under section 5(a)(1); or

10           (B) the date that is 60 days after the date  
11 of the enactment of this Act.

12       (c) CONSTRUCTION.—Nothing in this section shall be  
13 construed—

14           (1) to require dismissal of a cause of action  
15 against an entity that has engaged in gross neg-  
16 ligence or willful misconduct in the course of con-  
17 ducting activities authorized by this Act; or

18           (2) to undermine or limit the availability of oth-  
19 erwise applicable common law or statutory defenses.

20 **SEC. 7. OVERSIGHT OF GOVERNMENT ACTIVITIES.**

21       (a) BIENNIAL REPORT ON IMPLEMENTATION.—

22           (1) IN GENERAL.—Not later than 1 year after  
23 the date of the enactment of this Act, and not less  
24 frequently than once every 2 years thereafter, the  
25 heads of the appropriate Federal entities shall joint-

1 ly submit and the Inspector General of the Depart-  
2 ment of Homeland Security, the Inspector General  
3 of the Intelligence Community, the Inspector Gen-  
4 eral of the Department of Justice, the Inspector  
5 General of the Department of Defense, and the In-  
6 spector General of the Department of Energy, in  
7 consultation with the Council of Inspectors General  
8 on Financial Oversight, shall jointly submit to Con-  
9 gress a detailed report concerning the implementa-  
10 tion of this Act.

11 (2) CONTENTS.—Each report submitted under  
12 paragraph (1) shall include the following:

13 (A) An assessment of the sufficiency of the  
14 policies, procedures, and guidelines required by  
15 section 5 in ensuring that cyber threat indica-  
16 tors are shared effectively and responsibly with-  
17 in the Federal Government.

18 (B) An evaluation of the effectiveness of  
19 real-time information sharing through the capa-  
20 bility and process developed under section 5(c),  
21 including any impediments to such real-time  
22 sharing.

23 (C) An assessment of the sufficiency of the  
24 procedures developed under section 3 in ensur-  
25 ing that cyber threat indicators in the posses-

1           sion of the Federal Government are shared in  
2           a timely and adequate manner with appropriate  
3           entities, or, if appropriate, are made publicly  
4           available.

5           (D) An assessment of whether cyber threat  
6           indicators have been properly classified and an  
7           accounting of the number of security clearances  
8           authorized by the Federal Government for the  
9           purposes of this Act.

10          (E) A review of the type of cyber threat in-  
11          dicators shared with the Federal Government  
12          under this Act, including the following:

13               (i) The degree to which such informa-  
14               tion may impact the privacy and civil lib-  
15               erties of specific persons.

16               (ii) A quantitative and qualitative as-  
17               sessment of the impact of the sharing of  
18               such cyber threat indicators with the Fed-  
19               eral Government on privacy and civil lib-  
20               erties of specific persons.

21               (iii) The adequacy of any steps taken  
22               by the Federal Government to reduce such  
23               impact.

24          (F) A review of actions taken by the Fed-  
25          eral Government based on cyber threat indica-

1           tors shared with the Federal Government under  
2           this Act, including the appropriateness of any  
3           subsequent use or dissemination of such cyber  
4           threat indicators by a Federal entity under sec-  
5           tion 5.

6           (G) A description of any significant viola-  
7           tions of the requirements of this Act by the  
8           Federal Government.

9           (H) A summary of the number and type of  
10          entities that received classified cyber threat in-  
11          dicators from the Federal Government under  
12          this Act and an evaluation of the risks and ben-  
13          efits of sharing such cyber threat indicators.

14          (3) RECOMMENDATIONS.—Each report sub-  
15          mitted under paragraph (1) may include rec-  
16          ommendations for improvements or modifications to  
17          the authorities and processes under this Act.

18          (4) FORM OF REPORT.—Each report required  
19          by paragraph (1) shall be submitted in unclassified  
20          form, but may include a classified annex.

21          (b) REPORTS ON PRIVACY AND CIVIL LIBERTIES.—

22                  (1) BIENNIAL REPORT FROM PRIVACY AND  
23          CIVIL LIBERTIES OVERSIGHT BOARD.—Not later  
24          than 2 years after the date of the enactment of this  
25          Act and not less frequently than once every 2 years

1 thereafter, the Privacy and Civil Liberties Oversight  
2 Board shall submit to Congress and the President a  
3 report providing—

4 (A) an assessment of the effect on privacy  
5 and civil liberties by the type of activities car-  
6 ried out under this Act; and

7 (B) an assessment of the sufficiency of the  
8 policies, procedures, and guidelines established  
9 pursuant to section 5 in addressing concerns re-  
10 lating to privacy and civil liberties.

11 (2) BIENNIAL REPORT OF INSPECTORS GEN-  
12 ERAL.—

13 (A) IN GENERAL.—Not later than 2 years  
14 after the date of the enactment of this Act and  
15 not less frequently than once every 2 years  
16 thereafter, the Inspector General of the Depart-  
17 ment of Homeland Security, the Inspector Gen-  
18 eral of the Intelligence Community, the Inspec-  
19 tor General of the Department of Justice, the  
20 Inspector General of the Department of De-  
21 fense, and the Inspector General of the Depart-  
22 ment of Energy shall, in consultation with the  
23 Council of Inspectors General on Financial  
24 Oversight, jointly submit to Congress a report  
25 on the receipt, use, and dissemination of cyber

1 threat indicators and defensive measures that  
2 have been shared with Federal entities under  
3 this Act.

4 (B) CONTENTS.—Each report submitted  
5 under subparagraph (A) shall include the fol-  
6 lowing:

7 (i) A review of the types of cyber  
8 threat indicators shared with Federal enti-  
9 ties.

10 (ii) A review of the actions taken by  
11 Federal entities as a result of the receipt  
12 of such cyber threat indicators.

13 (iii) A list of Federal entities receiving  
14 such cyber threat indicators.

15 (iv) A review of the sharing of such  
16 cyber threat indicators among Federal en-  
17 tities to identify inappropriate barriers to  
18 sharing information.

19 (3) RECOMMENDATIONS.—Each report sub-  
20 mitted under this subsection may include such rec-  
21 ommendations as the Privacy and Civil Liberties  
22 Oversight Board, with respect to a report submitted  
23 under paragraph (1), or the Inspectors General re-  
24 ferred to in paragraph (2)(A), with respect to a re-  
25 port submitted under paragraph (2), may have for

1 improvements or modifications to the authorities  
2 under this Act.

3 (4) FORM.—Each report required under this  
4 subsection shall be submitted in unclassified form,  
5 but may include a classified annex.

6 **SEC. 8. CONSTRUCTION AND PREEMPTION.**

7 (a) OTHERWISE LAWFUL DISCLOSURES.—Nothing in  
8 this Act shall be construed—

9 (1) to limit or prohibit otherwise lawful disclo-  
10 sures of communications, records, or other informa-  
11 tion, including reporting of known or suspected  
12 criminal activity, by an entity to any other entity or  
13 the Federal Government under this Act; or

14 (2) to limit or prohibit otherwise lawful use of  
15 such disclosures by any Federal entity, even when  
16 such otherwise lawful disclosures duplicate or rep-  
17 licate disclosures made under this Act.

18 (b) WHISTLE BLOWER PROTECTIONS.—Nothing in  
19 this Act shall be construed to prohibit or limit the disclo-  
20 sure of information protected under section 2302(b)(8) of  
21 title 5, United States Code (governing disclosures of ille-  
22 gality, waste, fraud, abuse, or public health or safety  
23 threats), section 7211 of title 5, United States Code (gov-  
24 erning disclosures to Congress), section 1034 of title 10,  
25 United States Code (governing disclosure to Congress by

1 members of the military), section 1104 of the National  
2 Security Act of 1947 (50 U.S.C. 3234) (governing disclo-  
3 sure by employees of elements of the intelligence commu-  
4 nity), or any similar provision of Federal or State law.

5 (c) PROTECTION OF SOURCES AND METHODS.—  
6 Nothing in this Act shall be construed—

7 (1) as creating any immunity against, or other-  
8 wise affecting, any action brought by the Federal  
9 Government, or any agency or department thereof,  
10 to enforce any law, executive order, or procedure  
11 governing the appropriate handling, disclosure, or  
12 use of classified information;

13 (2) to affect the conduct of authorized law en-  
14 forcement or intelligence activities; or

15 (3) to modify the authority of a department or  
16 agency of the Federal Government to protect classi-  
17 fied information and sources and methods and the  
18 national security of the United States.

19 (d) RELATIONSHIP TO OTHER LAWS.—Nothing in  
20 this Act shall be construed to affect any requirement  
21 under any other provision of law for an entity to provide  
22 information to the Federal Government.

23 (e) PROHIBITED CONDUCT.—Nothing in this Act  
24 shall be construed to permit price-fixing, allocating a mar-  
25 ket between competitors, monopolizing or attempting to

1 monopolize a market, boycotting, or exchanges of price or  
2 cost information, customer lists, or information regarding  
3 future competitive planning.

4 (f) INFORMATION SHARING RELATIONSHIPS.—Nothing  
5 in this Act shall be construed—

6 (1) to limit or modify an existing information  
7 sharing relationship;

8 (2) to prohibit a new information sharing rela-  
9 tionship;

10 (3) to require a new information sharing rela-  
11 tionship between any entity and the Federal Govern-  
12 ment; or

13 (4) to require the use of the capability and  
14 process within the Department of Homeland Secu-  
15 rity developed under section 5(c).

16 (g) PRESERVATION OF CONTRACTUAL OBLIGATIONS  
17 AND RIGHTS.—Nothing in this Act shall be construed—

18 (1) to amend, repeal, or supersede any current  
19 or future contractual agreement, terms of service  
20 agreement, or other contractual relationship between  
21 any entities, or between any entity and a Federal en-  
22 tity; or

23 (2) to abrogate trade secret or intellectual prop-  
24 erty rights of any entity or Federal entity.

1 (h) ANTI-TASKING RESTRICTION.—Nothing in this  
2 Act shall be construed to permit the Federal Govern-  
3 ment—

4 (1) to require an entity to provide information  
5 to the Federal Government;

6 (2) to condition the sharing of cyber threat in-  
7 dicators with an entity on such entity's provision of  
8 cyber threat indicators to the Federal Government;  
9 or

10 (3) to condition the award of any Federal  
11 grant, contract, or purchase on the provision of a  
12 cyber threat indicator to a Federal entity.

13 (i) NO LIABILITY FOR NON-PARTICIPATION.—Noth-  
14 ing in this Act shall be construed to subject any entity  
15 to liability for choosing not to engage in the voluntary ac-  
16 tivities authorized in this Act.

17 (j) USE AND RETENTION OF INFORMATION.—Noth-  
18 ing in this Act shall be construed to authorize, or to mod-  
19 ify any existing authority of, a department or agency of  
20 the Federal Government to retain or use any information  
21 shared under this Act for any use other than permitted  
22 in this Act.

23 (k) FEDERAL PREEMPTION.—

24 (1) IN GENERAL.—This Act supersedes any  
25 statute or other provision of law of a State or polit-

1 ical subdivision of a State that restricts or otherwise  
2 expressly regulates an activity authorized under this  
3 Act.

4 (2) STATE LAW ENFORCEMENT.—Nothing in  
5 this Act shall be construed to supersede any statute  
6 or other provision of law of a State or political sub-  
7 division of a State concerning the use of authorized  
8 law enforcement practices and procedures.

9 (1) REGULATORY AUTHORITY.—Nothing in this Act  
10 shall be construed—

11 (1) to authorize the promulgation of any regu-  
12 lations not specifically authorized by this Act;

13 (2) to establish or limit any regulatory author-  
14 ity not specifically established or limited under this  
15 Act; or

16 (3) to authorize regulatory actions that would  
17 duplicate or conflict with regulatory requirements,  
18 mandatory standards, or related processes under an-  
19 other provision of Federal law.

20 (m) AUTHORITY OF SECRETARY OF DEFENSE TO  
21 RESPOND TO CYBER ATTACKS.—Nothing in this Act shall  
22 be construed to limit the authority of the Secretary of De-  
23 fense to develop, prepare, coordinate, or, when authorized  
24 by the President to do so, conduct a military cyber oper-  
25 ation in response to a malicious cyber activity carried out

1 against the United States or a United States person by  
2 a foreign government or an organization sponsored by a  
3 foreign government or a terrorist organization.

4 **SEC. 9. REPORT ON CYBERSECURITY THREATS.**

5 (a) REPORT REQUIRED.—Not later than 180 days  
6 after the date of the enactment of this Act, the Director  
7 of National Intelligence, in coordination with the heads of  
8 other appropriate elements of the intelligence community,  
9 shall submit to the Select Committee on Intelligence of  
10 the Senate and the Permanent Select Committee on Intel-  
11 ligence of the House of Representatives a report on cyber-  
12 security threats, including cyber attacks, theft, and data  
13 breaches.

14 (b) CONTENTS.—The report required by subsection  
15 (a) shall include the following:

16 (1) An assessment of the current intelligence  
17 sharing and cooperation relationships of the United  
18 States with other countries regarding cybersecurity  
19 threats, including cyber attacks, theft, and data  
20 breaches, directed against the United States and  
21 which threaten the United States national security  
22 interests and economy and intellectual property, spe-  
23 cifically identifying the relative utility of such rela-  
24 tionships, which elements of the intelligence commu-

1 nity participate in such relationships, and whether  
2 and how such relationships could be improved.

3 (2) A list and an assessment of the countries  
4 and nonstate actors that are the primary threats of  
5 carrying out a cybersecurity threat, including a  
6 cyber attack, theft, or data breach, against the  
7 United States and which threaten the United States  
8 national security, economy, and intellectual property.

9 (3) A description of the extent to which the ca-  
10 pabilities of the United States Government to re-  
11 spond to or prevent cybersecurity threats, including  
12 cyber attacks, theft, or data breaches, directed  
13 against the United States private sector are de-  
14 graded by a delay in the prompt notification by pri-  
15 vate entities of such threats or cyber attacks, theft,  
16 and breaches.

17 (4) An assessment of additional technologies or  
18 capabilities that would enhance the ability of the  
19 United States to prevent and to respond to cyberse-  
20 curity threats, including cyber attacks, theft, and  
21 data breaches.

22 (5) An assessment of any technologies or prac-  
23 tices utilized by the private sector that could be rap-  
24 idly fielded to assist the intelligence community in  
25 preventing and responding to cybersecurity threats.

1 (c) FORM OF REPORT.—The report required by sub-  
2 section (a) shall be made available in classified and unclas-  
3 sified forms.

4 (d) INTELLIGENCE COMMUNITY DEFINED.—In this  
5 section, the term “intelligence community” has the mean-  
6 ing given that term in section 3 of the National Security  
7 Act of 1947 (50 U.S.C. 3003).

8 **SEC. 10. CONFORMING AMENDMENTS.**

9 (a) PUBLIC INFORMATION.—Section 552(b) of title  
10 5, United States Code, is amended—

11 (1) in paragraph (8), by striking “or” at the  
12 end;

13 (2) in paragraph (9), by striking “wells.” and  
14 inserting “wells; or”; and

15 (3) by inserting after paragraph (9) the fol-  
16 lowing:

17 “(10) information shared with or provided to  
18 the Federal Government pursuant to the Cybersecu-  
19 rity Information Sharing Act of 2015.”.

20 (b) MODIFICATION OF LIMITATION ON DISSEMINA-  
21 TION OF CERTAIN INFORMATION CONCERNING PENETRA-  
22 TIONS OF DEFENSE CONTRACTOR NETWORKS.—Section  
23 941(c)(3) of the National Defense Authorization Act for  
24 Fiscal Year 2013 (Public Law 112–239; 10 U.S.C. 2224  
25 note) is amended by inserting at the end the following:

1 “The Secretary may share such information with other  
2 Federal entities if such information consists of cyber  
3 threat indicators and defensive measures and such infor-  
4 mation is shared consistent with the policies and proce-  
5 dures promulgated by the Attorney General under section  
6 5 of the Cybersecurity Information Sharing Act of 2015.”.



**Calendar No. 28**

114<sup>TH</sup> CONGRESS  
1<sup>ST</sup> Session  
**S. 754**

---

---

**A BILL**

To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes.

---

---

MARCH 17, 2015

Read twice and placed on the calendar