

CYBER INTELLIGENCE SHARING AND PROTECTION ACT

APRIL 17, 2012.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. ROGERS of Michigan, from the Permanent Select Committee on Intelligence, submitted the following

R E P O R T

together with

MINORITY VIEWS

[To accompany H.R. 3523]

[Including cost estimate of the Congressional Budget Office]

The Permanent Select Committee on Intelligence, to whom was referred the bill (H.R. 3523) to provide for the sharing of certain cyber threat intelligence and cyber threat information between the intelligence community and cybersecurity entities, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

The amendment is as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the “Cyber Intelligence Sharing and Protection Act”.

SEC. 2. CYBER THREAT INTELLIGENCE AND INFORMATION SHARING.

(a) **IN GENERAL.**—Title XI of the National Security Act of 1947 (50 U.S.C. 442 et seq.) is amended by adding at the end the following new section:

“CYBER THREAT INTELLIGENCE AND INFORMATION SHARING

“SEC. 1104. (a) **INTELLIGENCE COMMUNITY SHARING OF CYBER THREAT INTELLIGENCE WITH PRIVATE SECTOR.**—

“(1) **IN GENERAL.**—The Director of National Intelligence shall establish procedures to allow elements of the intelligence community to share cyber threat intelligence with private-sector entities and to encourage the sharing of such intelligence.

“(2) **SHARING AND USE OF CLASSIFIED INTELLIGENCE.**—The procedures established under paragraph (1) shall provide that classified cyber threat intelligence may only be—

- “(A) shared by an element of the intelligence community with—
- “(i) certified entities; or
 - “(ii) a person with an appropriate security clearance to receive such cyber threat intelligence;
- “(B) shared consistent with the need to protect the national security of the United States; and
- “(C) used by a certified entity in a manner which protects such cyber threat intelligence from unauthorized disclosure.
- “(3) SECURITY CLEARANCE APPROVALS.—The Director of National Intelligence shall issue guidelines providing that the head of an element of the intelligence community may, as the head of such element considers necessary to carry out this subsection—
- “(A) grant a security clearance on a temporary or permanent basis to an employee or officer of a certified entity;
 - “(B) grant a security clearance on a temporary or permanent basis to a certified entity and approval to use appropriate facilities; and
 - “(C) expedite the security clearance process for a person or entity as the head of such element considers necessary, consistent with the need to protect the national security of the United States.
- “(4) NO RIGHT OR BENEFIT.—The provision of information to a private-sector entity under this subsection shall not create a right or benefit to similar information by such entity or any other private-sector entity.
- “(b) PRIVATE SECTOR USE OF CYBERSECURITY SYSTEMS AND SHARING OF CYBER THREAT INFORMATION.—
- “(1) IN GENERAL.—
- “(A) CYBERSECURITY PROVIDERS.—Notwithstanding any other provision of law, a cybersecurity provider, with the express consent of a protected entity for which such cybersecurity provider is providing goods or services for cybersecurity purposes, may, for cybersecurity purposes—
 - “(i) use cybersecurity systems to identify and obtain cyber threat information to protect the rights and property of such protected entity; and
 - “(ii) share such cyber threat information with any other entity designated by such protected entity, including, if specifically designated, the Federal Government.
 - “(B) SELF-PROTECTED ENTITIES.—Notwithstanding any other provision of law, a self-protected entity may, for cybersecurity purposes—
 - “(i) use cybersecurity systems to identify and obtain cyber threat information to protect the rights and property of such self-protected entity; and
 - “(ii) share such cyber threat information with any other entity, including the Federal Government.
- “(2) USE AND PROTECTION OF INFORMATION.—Cyber threat information shared in accordance with paragraph (1)—
- “(A) shall only be shared in accordance with any restrictions placed on the sharing of such information by the protected entity or self-protected entity authorizing such sharing, including appropriate anonymization or minimization of such information;
 - “(B) may not be used by an entity to gain an unfair competitive advantage to the detriment of the protected entity or the self-protected entity authorizing the sharing of information; and
 - “(C) if shared with the Federal Government—
 - “(i) shall be exempt from disclosure under section 552 of title 5, United States Code;
 - “(ii) shall be considered proprietary information and shall not be disclosed to an entity outside of the Federal Government except as authorized by the entity sharing such information; and
 - “(iii) shall not be used by the Federal Government for regulatory purposes.
- “(3) EXEMPTION FROM LIABILITY.—No civil or criminal cause of action shall lie or be maintained in Federal or State court against a protected entity, self-protected entity, cybersecurity provider, or an officer, employee, or agent of a protected entity, self-protected entity, or cybersecurity provider, acting in good faith—
- “(A) for using cybersecurity systems or sharing information in accordance with this section; or
 - “(B) for not acting on information obtained or shared in accordance with this section.

“(4) RELATIONSHIP TO OTHER LAWS REQUIRING THE DISCLOSURE OF INFORMATION.—The submission of information under this subsection to the Federal Government shall not satisfy or affect any requirement under any other provision of law for a person or entity to provide information to the Federal Government.

“(c) FEDERAL GOVERNMENT USE OF INFORMATION.—

“(1) LIMITATION.—The Federal Government may use cyber threat information shared with the Federal Government in accordance with subsection (b) for any lawful purpose only if—

“(A) the use of such information is not for a regulatory purpose; and

“(B) at least one significant purpose of the use of such information is—

“(i) a cybersecurity purpose; or

“(ii) the protection of the national security of the United States.

“(2) AFFIRMATIVE SEARCH RESTRICTION.—The Federal Government may not affirmatively search cyber threat information shared with the Federal Government under subsection (b) for a purpose other than a purpose referred to in paragraph (1)(B).

“(3) ANTI-TASKING RESTRICTION.—Nothing in this section shall be construed to permit the Federal Government to—

“(A) require a private-sector entity to share information with the Federal Government; or

“(B) condition the sharing of cyber threat intelligence with a private-sector entity on the provision of cyber threat information to the Federal Government.

“(d) REPORT ON INFORMATION SHARING.—

“(1) REPORT.—The Inspector General of the Intelligence Community shall annually submit to the congressional intelligence committees a report containing a review of the use of information shared with the Federal Government under this section, including—

“(A) a review of the use by the Federal Government of such information for a purpose other than a cybersecurity purpose;

“(B) a review of the type of information shared with the Federal Government under this section;

“(C) a review of the actions taken by the Federal Government based on such information;

“(D) appropriate metrics to determine the impact of the sharing of such information with the Federal Government on privacy and civil liberties, if any; and

“(E) any recommendations of the Inspector General for improvements or modifications to the authorities under this section.

“(2) FORM.—Each report required under paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

“(e) FEDERAL PREEMPTION.—This section supersedes any statute of a State or political subdivision of a State that restricts or otherwise expressly regulates an activity authorized under subsection (b).

“(f) SAVINGS CLAUSE.—Nothing in this section shall be construed to limit any other authority to use a cybersecurity system or to identify, obtain, or share cyber threat intelligence or cyber threat information.

“(g) DEFINITIONS.—In this section:

“(1) CERTIFIED ENTITY.—The term ‘certified entity’ means a protected entity, self-protected entity, or cybersecurity provider that—

“(A) possesses or is eligible to obtain a security clearance, as determined by the Director of National Intelligence; and

“(B) is able to demonstrate to the Director of National Intelligence that such provider or such entity can appropriately protect classified cyber threat intelligence.

“(2) CYBER THREAT INFORMATION.—The term ‘cyber threat information’ means information directly pertaining to a vulnerability of, or threat to, a system or network of a government or private entity, including information pertaining to the protection of a system or network from—

“(A) efforts to degrade, disrupt, or destroy such system or network; or

“(B) theft or misappropriation of private or government information, intellectual property, or personally identifiable information.

“(3) CYBER THREAT INTELLIGENCE.—The term ‘cyber threat intelligence’ means information in the possession of an element of the intelligence community directly pertaining to a vulnerability of, or threat to, a system or network of a government or private entity, including information pertaining to the protection of a system or network from—

“(A) efforts to degrade, disrupt, or destroy such system or network; or

- “(B) theft or misappropriation of private or government information, intellectual property, or personally identifiable information.
- “(4) CYBERSECURITY PROVIDER.—The term ‘cybersecurity provider’ means a non-governmental entity that provides goods or services intended to be used for cybersecurity purposes.
- “(5) CYBERSECURITY PURPOSE.—The term ‘cybersecurity purpose’ means the purpose of ensuring the integrity, confidentiality, or availability of, or safeguarding, a system or network, including protecting a system or network from—
- “(A) efforts to degrade, disrupt, or destroy such system or network; or
- “(B) theft or misappropriation of private or government information, intellectual property, or personally identifiable information.
- “(6) CYBERSECURITY SYSTEM.—The term ‘cybersecurity system’ means a system designed or employed to ensure the integrity, confidentiality, or availability of, or safeguard, a system or network, including protecting a system or network from—
- “(A) efforts to degrade, disrupt, or destroy such system or network; or
- “(B) theft or misappropriation of private or government information, intellectual property, or personally identifiable information.
- “(7) PROTECTED ENTITY.—The term ‘protected entity’ means an entity, other than an individual, that contracts with a cybersecurity provider for goods or services to be used for cybersecurity purposes.
- “(8) SELF-PROTECTED ENTITY.—The term ‘self-protected entity’ means an entity, other than an individual, that provides goods or services for cybersecurity purposes to itself.”
- (b) PROCEDURES AND GUIDELINES.—The Director of National Intelligence shall—
- (1) not later than 60 days after the date of the enactment of this Act, establish procedures under paragraph (1) of section 1104(a) of the National Security Act of 1947, as added by subsection (a) of this section, and issue guidelines under paragraph (3) of such section 1104(a); and
- (2) following the establishment of such procedures and the issuance of such guidelines, expeditiously distribute such procedures and such guidelines to appropriate Federal Government and private-sector entities.
- (c) INITIAL REPORT.—The first report required to be submitted under subsection (d) of section 1104 of the National Security Act of 1947, as added by subsection (a) of this section, shall be submitted not later than one year after the date of the enactment of this Act.
- (d) TABLE OF CONTENTS AMENDMENT.—The table of contents in the first section of the National Security Act of 1947 is amended by adding at the end the following new item:

“Sec. 1104. Cyber threat intelligence and information sharing.”

PURPOSE

The purpose of H.R. 3523 is to provide for the sharing of certain cyber threat intelligence and cyber threat information between the intelligence community and cybersecurity entities, and other purposes.

COMMITTEE STATEMENT AND VIEWS

At the beginning of the 112th Congress, the Committee, under the direction of Chairman Rogers and Ranking Member Ruppberger, began a bipartisan effort to examine the issue of cybersecurity.¹ The goal of this effort was to better understand the threats

¹This effort involved a series of briefings and hearings, including one open hearing, to inform Committee members and, where possible, the public, about the serious national security threat posed by nation-state actors and other adversaries in the cyber realm. These meetings, briefings, and hearings were in turn supported by numerous meetings and briefings conducted by Committee staff with agencies and individuals from the Executive Branch including, among others, the White House, the Department of Homeland Security, the Department of Justice, including the Federal Bureau of Investigation, the Department of Defense, including the National Security Agency, and with experts from the academic and think-tank communities. The Committee staff also held numerous meetings with private sector companies and trade groups in industries including technology, telecommunications, financial services, utilities, aerospace, and defense. And the Committee staff met with representatives of privacy and civil liberties organizations including the Center for Democracy and Technology, the American Civil Liberties Union, the Electronic Frontier Foundation, the Constitution Project, and the CATO Institute, among others. In

facing the nation in cyberspace—with respect to both the government and in the private sector—and to determine what the Intelligence Community could do to help better protect the nation. The results of this review were stunning: a number of advanced nation-state actors are actively engaged in a series of wide-ranging, aggressive efforts to penetrate American computer systems and networks; these efforts extend well beyond government networks, and reach deep into nearly every sector of the American economy, including companies serving critical infrastructure needs.

Perhaps most troubling, these efforts are targeted not only at sensitive national security and infrastructure information, but are also often aimed at stealing the corporate research and development information that forms the very lifeblood of the American economy. China, in particular, is engaged in an extensive, day-in, day-out effort to pillage American corporate and government information. There can be no question that in today's modern world, economic security is national security, and the government must help the private sector protect itself.

The Committee's review also revealed that while the government is already doing much to provide support and assistance to the private sector to address this threat, in particular through DHS and the FBI, more can and should be done in the immediate future. In particular, the Committee determined that the Intelligence Community is currently in possession of tremendously valuable intelligence and strategic insights derived from its extensive overseas intelligence collection efforts that can and should be provided—in both classified and unclassified form (when possible)—to the private sector in order to help the owners and operators of the vast majority of America's information infrastructure better protect themselves. The Committee believes that the recent Defense Industrial Base Pilot project ("DIB Pilot") is a good model for demonstrating how sensitive government threat intelligence can be shared with the private sector in an operationally usable manner. Under the DIB Pilot, the government provides classified threat intelligence to key Internet Service Providers, who use the information to protect a limited number of companies in the defense industrial base, all on a voluntary basis.

The Committee's review also determined that while much cybersecurity monitoring and threat information sharing takes place today within the private sector, real and perceived legal barriers substantially hamper the efforts of the private sector to protect itself. The Committee determined that these issues are best resolved in the first instance by providing clear, positive authority to permit the monitoring—by the private sector—of privately-owned and operated networks and systems for the purpose of detecting cybersecurity threats and to permit the voluntary sharing of information about those threats and vulnerabilities with others, including entities within the private sector and with the federal government.

While some have suggested that the private sector needs more regulation or that the government ought to directly help defend certain portions of the private sector, the Committee's view is that the protection of the private sector is best left in private hands and

total, the Committee members and staff met with dozens of organizations in conducting its review over a nearly one-year period.

that the government ought to provide as much intelligence as possible to the private sector before reaching for a regulatory “stick.” In the view of the Committee, such an approach—voluntary, private sector defense of private sector systems and networks informed by government intelligence information—best protects individual privacy and takes advantage of the natural incentives built into our economic system, including harnessing private sector drive and innovation.

The Committee’s review revealed that America’s cyber infrastructure is distressingly vulnerable to espionage and attacks by nation-states and others with advanced capabilities. The Committee believes that immediate and serious action is necessary to staunch the bleeding of American corporate research and development information and to better protect our national security. In particular, the Committee believes that the Intelligence Community must take immediate and decisive action to provide intelligence to the private sector to help it better protect itself. In turn, the private sector must act aggressively to better monitor its own systems and to share information—both within the private sector and with the federal government on a purely voluntary basis. The Committee recognizes that because it focused on the issues within its jurisdiction, this legislation does not address many of the other issues facing the nation with respect to cybersecurity. At the same time, however, the Committee firmly believes that this legislation is an important first step in the effort to better protect the nation from advanced cyber threat actors.

COMMITTEE CONSIDERATION AND ROLLCALL VOTES

On December 1, 2011, the Committee met in open session and ordered the bill H.R. 3523 favorably reported, as amended.

OPEN SESSION

In open session, the Committee considered the text of the bill H.R. 3523.

Chairman Rogers offered an amendment. The amendment places additional restrictions on the use by the government of information obtained pursuant to the bill. The amendment was agreed to by voice vote.

Mr. Thompson offered an amendment. The amendment requires an annual report by the Inspector General of the Intelligence Community reviewing the use of cyber threat information provided to the government pursuant to the bill. The amendment was agreed to by voice vote.

Ms. Schakowsky offered an amendment providing that the Director of National Intelligence shall develop and periodically review policies and procedures governing the acquisition, retention, use, and disclosure of information obtained by the intelligence community pursuant to the bill. Subsequently, Ms. Schakowsky asked for and received unanimous consent to withdraw the amendment.

The Committee then adopted a motion by the Chairman to favorably report the bill H.R. 3523 to the House, as amended. The motion was agreed to by a record vote of 17 ayes to 1 no:

Voting Aye: Chairman Rogers, Mr. Thornberry, Mrs. Myrick, Mr. Miller, Mr. Conaway, Mr. King, Mr. LoBiondo, Mr. Nunes, Mr.

Westmoreland, Mr. Rooney, Mr. Heck, Mr. Ruppersberger, Mr. Thompson, Mr. Langevin, Mr. Schiff, Mr. Boren, Mr. Chandler.
 Voting No: Ms. Schakowsky.

SECTION-BY-SECTION ANALYSIS

SECTION 1. SHORT TITLE

The short title of the Act is the Cyber Intelligence Sharing and Protection Act.

SECTION 2. CYBER THREAT INTELLIGENCE AND INFORMATION SHARING

Section 2(a): In General

This subsection of the Act amends Title XI of the National Security Act of 1947 by adding a new section, Section 1104.

Section 1104(a) of Title 50: Intelligence Community Sharing of Cyber Threat Intelligence with Private Sector

Subsection (a) of new Section 1104 provides for the sharing of cyber threat intelligence—both classified and unclassified—by elements of the Intelligence Community with entities in the private sector. It is the view of the Committee that the routine and fulsome sharing of such intelligence information with appropriate cleared entities and individuals within the private sector is critically important to protecting the nation from advanced cyber threats. It is critical that as much information as possible be shared at machine-speed, in real-time, and in a manner that the information—whether classified or not—is operationally usable by entities within the private sector.

This subsection seeks to set forth a general framework and requires the establishment of specific procedures and guidelines to make such sharing happen in the immediate future and to permit such sharing to continue so long as the nation faces this significant threat to our national security. The Committee intends to engage in vigorous oversight of the Intelligence Community use of the authorities under this section and, in particular, the Office of the Director of National Intelligence (ODNI), which is charged with promulgating appropriate procedures and guidelines under this subsection. The Committee expects to be consulted by ODNI in the formulation of these procedures and guidelines to ensure that the Committee's intent is achieved by them.

While the term “private sector” is not defined in the legislation, the Committee intends that term to be given the broadest possible meaning and specifically intends the term to include utilities, whether organized as public, private, or quasi-public entities, to ensure at the entities that provide Americans with access to power, water, gas, and other critical services are also provided with access to critical federal government intelligence regarding cyber threats.

In addition, the Committee expects that private sector entities receiving classified intelligence pursuant to this subsection will use this information not only to protect their own systems and networks, but also, where they find appropriate as a business matter, to sell cybersecurity goods and services appropriately incorporating this information to protect other corporate customers.

Paragraph 1: In General

Paragraph (1) of subsection (a) requires the Director of National Intelligence to establish procedures to allow intelligence community elements to share cyber threat intelligence with the private sector and to encourage the sharing of such intelligence. The Committee intends the DNI's procedures to create a sea change in the current intelligence sharing practices of the Intelligence Community with respect to the private sector.

First, the DNI's procedures should ensure that as much cyber threat intelligence as possible is downgraded to the lowest classification level possible, including declassification where appropriate, and made available to as broad an audience in the private sector as possible, consistent with the need to protect the national security.

Second, the DNI's procedures should ensure that cyber threat intelligence, including classified information, is routinely and consistently provided out to entities and individuals in the private sector with the appropriate clearances.

Paragraph 2: Sharing and Use of Classified Information

Paragraph (2) of subsection (a) requires that the DNI's procedures with respect to classified cyber threat intelligence require that classified information only be shared with certified entities, as defined by the legislation, or with individuals who possess appropriate security clearances, and be consistent with the need to protect national security. Certified entities are cybersecurity providers, protected entities, or self-protected entities that possess or are eligible to obtain a security clearance and can demonstrate to the Director of National Intelligence that they are able to appropriately protect such classified cyber threat intelligence.

Paragraph (2) also requires that the DNI's procedures provide that classified cyber threat intelligence only be used by certified entities in a manner that protects the classified information from unauthorized disclosure. This provision ensures that when certified entities employ classified intelligence to protect unclassified systems or networks, they do so in a way that does not reveal classified information directly or indirectly.

The Committee expects that the DNI's procedures will be flexible in nature and will take account of private sector innovation and incorporate current and future information sharing and security best practices. As a result, the Committee expects the DNI to work closely with the private sector to establish these procedures, to work with the private sector to meet the requirements of the procedures, and to ensure that these procedures result in the routine and consistent sharing of operationally-usable cyber threat intelligence. The Committee also expects the DNI to review and revise these procedures on a regular basis, at least annually, and to conduct such review in cooperation with the private sector, as well as to account for new technologies developed by the private sector in each set of revised procedures. The DNI should also strongly consider the establishment of a private-sector advisory committee composed of senior executives at key private companies to advise on these procedures on a regular basis.

Paragraph (3): Security Clearance Approvals

Paragraph (3) requires the DNI to issue guidelines allowing the head of intelligence community elements to grant temporary or permanent security clearances to certified entities and their employees and officers (including non-employee officers such as board members) in order to allow the government to share classified cyber security threat intelligence with those certified entities. The Committee's intent is that the intelligence community grant security clearances to entities that are involved in protecting their own and their corporate customers' networks from cyber threats and that the intelligence community share cyber threat intelligence to protect the nation from advanced cyber threat actors. In particular, the Committee wishes to ensure that the private sector be able to receive highly classified cyber threat intelligence, including at the Top Secret/Sensitive Compartmented Information level, as appropriate to protect national security. The Committee is concerned that certain industries and entities may currently lack sufficient clearances at the appropriate level.

Paragraph (3) also requires the DNI's guidelines to allow intelligence community elements to grant approval for the use of appropriate facilities and to expedite security clearances as necessary, consistent with the need to protect national security. The Committee's intent is that the approval process for the granting of security clearances and the use of facilities for the handling of classified information be expedited and broadened by these provisions.

Because additional security clearances or facility approvals may be necessary to effectuate the goals of this legislation, it is further the Committee's intent that the cost for these security clearances and facility approvals, as well as the underlying investigations and adjudications necessary to obtain and maintain them, be fully borne by the private sector. As noted above, it is the Committee's intent that private sector entities that become certified entities will be able to better protect themselves, as well as to sell cybersecurity goods and services appropriately incorporating this information to protect other corporate customers in the private sector. It is therefore the Committee's view that these entities should bear the full cost of obtaining access to the valuable cyber threat intelligence the government will provide under the legislation to certified entities. The Committee therefore expects that the DNI's guidelines authorized by the legislation will provide for full payment of such costs by the private sector entity obtaining the security clearances or facility approvals.

Paragraph 4: No Right or Benefit

Paragraph (4) makes clear that while the Committee expects the Intelligence Community to work with private sector entities to help them meet the requirements to serve as a certified entity, no private sector entity is entitled to receive cyber threat intelligence from the government and that no right or benefit to cyber threat intelligence is created by the provision of such intelligence to a particular private sector entity or group of entities.

Section 1104(b) of Title 50: Private Sector Use of Cybersecurity Systems and Sharing of Cyber Threat Information

Subsection (b) of new Section 1104 provides clear, positive authority, notwithstanding any other provision of law, to private sector entities to monitor their own systems and networks or those of their corporate customers through the use of cybersecurity systems to identify and obtain cyber threat information, and to mitigate threat or vulnerabilities to their own systems or networks or those of their corporate customers. The Committee intends the notwithstanding clauses contained in subsection (b), as applied to this authority, to have the effect of removing any prohibition, real or perceived, to the monitoring, for cybersecurity purposes, of private sector systems and networks by the private sector entities that own the systems or networks or by security companies contracted by the system or network owner to protect those networks and systems. Potential barriers to such cybersecurity monitoring include federal laws governing electronic surveillance.

Subsection (b) also provides clear, positive authority, notwithstanding any other provision of law, for the private sector to share cyber threat information identified and obtained through such cybersecurity monitoring with other entities within the private sector, as well as with the Federal Government on a purely voluntary basis, at the discretion of the private sector entities whose systems or networks are being protected. The Committee intends the notwithstanding clauses contained in subsection (b), as applied to this authority, to have the effect of removing any prohibition, real or perceived, to the sharing of cyber threat information within the private sector, as well as with the Federal Government. Potential barriers to such sharing that would be addressed by this provision include, but are not limited to, provisions of federal antitrust law, which some believe may limit sharing of cyber threat information between competitors in the private sector, as well as provisions of other federal laws including the telecommunications laws. The Committee's intent in addressing antitrust issues, amongst others, is to permit information sharing about cyber threats that might be hampered by such laws, not to permit inappropriate and unlawful activity, such as the coordinated fixing of prices.

The Committee notes that the protections related to the authorities provided in this section are fairly robust, even standing alone. First, as noted below, only cyber threat information—that is information about a threat to, or vulnerability of government or private systems or networks—may be identified, obtained, or shared. And any such monitoring or sharing may only take place for cybersecurity purposes. And finally, the liability protection provided in this subsection only applies when an entity is acting in good faith. These provisions, taken together and building on top of one another, in the Committee's view, are a strong step towards protecting the privacy and civil liberties of Americans.

Paragraph 1: In General

Paragraph (1) of subsection (b) provides the twin authorities discussed above to cybersecurity providers, who provide goods and services to their corporate customers for cybersecurity purposes and to self-protected entities, who provide such cybersecurity goods and services for themselves.

In providing these authorities, the legislation makes clear that the monitoring and sharing of information either by a cybersecurity provider or a self-protected entity may only take place for cybersecurity purposes, a defined term that, as discussed below, limits the identification, obtaining, and sharing of cyber threat information to the protection of private or government systems or networks from threat to, or vulnerabilities, of those systems or networks.

Similarly, the identification and obtaining of cyber threat information by a provider or a self-protected entity may only take place as part of an effort to protect the rights and properties of the provider's corporate customer or the self-protected entity itself, as the case may be. In this context, it is the Committee's intent that the protection of the rights and property of a corporate entity includes, but is not limited to, the protection of the systems and networks that make up its own corporate internal and external information systems but also the systems and networks over which it provides services to its customers. For example, the Committee expects that an internet service provider or telecommunications company may seek to protect not only its own corporate networks but also the backbone communications systems and networks over which it provides services to its customers. Similarly, for example, the Committee expects that a utility may seek not only to protect its corporate network but may seek to protect the systems and networks over which it provides electricity, water, or gas services to its customers. The Committee specifically intends the authorities provided in subsection (b) to permit private sector entities to protect such systems and networks.

Paragraph (1) also requires that a cybersecurity provider obtain the express consent, whether in writing, electronically, orally, or otherwise, of its corporate customer before conducting any cybersecurity monitoring or sharing under these authorities. It is the Committee's intent that express consent may be provided on a going-forward basis by a corporate customer to a provider for a specified period of time, to be determined by the corporate customer.

In addition, paragraph (1) makes clear that the sharing of information either by a cybersecurity provider or a self-protected entity is to be purely voluntary and at the discretion of the entity whose systems or networks are being protected. Moreover, the legislation requires that where a provider is doing the sharing on behalf of a corporate customer, the customer must designate the entities or group of entities it wishes to share information with, and that it must specifically designate the Federal Government if it wishes to share information with the government.

It is the Committee's expectation that many entities will be able to take advantage of the authorities provided in paragraph (1) when acting both as a cybersecurity provider and as a self-protected entity. For example, an entity such as an internet service provider may act as a cybersecurity provider when providing managed security services to a corporate customer and may simultaneously be acting as a self-protected entity when protecting its own corporate systems and networks as well as the systems and networks over which it provides services to its customers. The Committee's intent is that private sector entities will be able to simultaneously take advantage of multiple authorities provided within the legislation.

Paragraph 2: Use and Protection of Information

Paragraph (2) of subsection (b) provides protections to promote the robust sharing of cyber threat information both within the private sector as well as from the private sector to the government on a purely voluntary basis.

Paragraph (2) provides that cyber threat information shared pursuant to paragraph (1) may only be shared in accordance with restrictions placed upon such sharing by the protected entity or the self-protected entity whose systems and networks are being protected and who therefore authorized the sharing. Paragraph (2) further provides that these restrictions may include the appropriate anonymization or minimization as determined by the protected entity or self-protected entity authorizing the sharing.

The Committee's intent is that through paragraph (1) and paragraph (2), a private sector entity choosing to share cyber threat information under these provisions has complete control over whom it shares with and what information it shares, including whether the information it shares is anonymized or minimized. The Committee believes that leaving the decision to share and the execution of desired anonymization and minimization in the hands of the private sector entities whose systems and networks are being protected, rather than in the hands of the party receiving the information, including the government, helps enhance privacy and civil liberties.

Paragraph (2) also provides that information shared pursuant to paragraph (1) may not be used by a receiving entity to gain an unfair competitive advantage to the detriment of the entity sharing the information. The Committee intends this provision to highlight that cybersecurity is enhanced by robust threat information sharing within the private sector, both amongst partners and competitors, without fear that a competitor will use the cyber threat or vulnerability information to unfairly obtain greater market share rather than simply to protect itself. The situation the Committee intends this provision to address is best demonstrated by an example: Company A shares information about a cyber vulnerability in one of its products with Company B, a competitor in the same marketplace; Company B the next day puts out an advertisement saying, "Don't buy Company A's product because it has the following vulnerability . . . instead, buy our product which doesn't have the same vulnerabilities." This example would, in the Committee's view, constitute gaining an unfair competitive advantage at the expense of the entity sharing the information. This provision does not prevent any company from obtaining a fair competitive advantage by, for example, using the shared information to build a better, more secure product that can be marketed without reference to a vulnerability shared by a particular entity.

Paragraph (2) further provides that cyber threat information voluntarily shared with the Federal Government pursuant to paragraph (1) shall be exempt from disclosure under the Freedom of Information Act, shall be considered proprietary information, shall not be disclosed by the Federal Government to an entity outside the Federal Government except as authorized by the entity sharing the information, and shall not be used by the Federal Government for regulatory purposes. The Committee intends this provision to address the key concerns expressed by the private sector regarding

the sharing of their sensitive information with the federal government: first, that the government might expose its most sensitive threat and vulnerability information to a wide audience either through FOIA or by publishing the information, thereby providing a roadmap for attacks by cyber threat actors; second, that the government might take the information provided by the private sector and use it to regulate or impose sanctions upon them.

The Committee determined that the best way to address these concerns and incentivize the sharing of cyber threat information with the government was to explicitly and clearly protect the information provided in this cybersecurity channel from being disclosed under FOIA, to require the government to carefully protect the information, and finally, to prohibit the government from using information provided in this cybersecurity channel from being used for regulatory purposes.

The Committee was cognizant of the fact that cyber threat information provided to the government under these authorities might also be required to be provided by certain private sector entities to their regulators and therefore provided elsewhere in the legislation that the mere classification of the information as cyber threat information or its provision to the government under this mechanism does not satisfy those regulatory requirements nor override any appropriate regulation that may take place based on the provision of such information to the government through other channels. Nor would these provisions prevent a third party from obtaining appropriate information through an otherwise appropriate FOIA request to a regulator who obtained the information under other regulatory authorities. Rather, the limitations here were designed to provide a safe harbor where private sector entities could provide real-time cyber threat information to the government without fear that that particular information would be used to regulate them directly or be exploited by bad actors.

Paragraph 3: Exemption from Liability

Paragraph (3) provides a bar to civil or criminal causes of action being brought or maintained in federal or state court against an entity or its officers, employees, or agents acting in good faith to use cybersecurity systems for monitoring to identify and obtain cyber threat information in accordance with the provisions of the legislation. The Committee's intent is to provide strong liability protection for private sector entities when they act to take advantage of the authorities provided under paragraph (1) of subsection (b) to do what the statute seeks to encourage them to do: robustly monitor their own systems and networks and those of their corporate customers and share information about threats and vulnerabilities to better protect their systems. Specifically, the Committee intends that civil or criminal actions based on the use of cybersecurity systems to monitor systems or networks to identify and obtain cyber threat information using the authorities of this statute shall be dismissed immediately by the courts and prior to significant discovery and extensive motion practice.

Paragraph (3) also provides an identical bar to actions against such entities acting in good faith for not acting on information obtained or shared in accordance with the provisions of the legislation. The Committee's intent is likewise to provide strong liability

protection to entities when they engage in robust cyber threat information sharing so that they are not held liable for not acting on every piece of cyber threat intelligence provided by the government or every piece of cyber threat information that they detect or receive from another private sector entity. The Committee believes that if information sharing does become truly robust, the amount of cyber threat information and the speed with which such information will be shared will make it nearly impossible to always protect against every threat in real-time and, as such, private sector entities ought not be held liable for such actions. Similarly, the Committee recognizes that particular entities may engage in a cost-benefit analysis with respect to implementing protections against particular threats and the Committee intends this provision to help ensure that a private sector entity making such a judgment not be held liable for making such reasonable determinations.

At the same time, the Committee was fully cognizant of the concern that it not create a moral hazard by providing too broad a liability protection provision and that it not incentivize bad acts. As a result, Paragraph (3) requires that the entity be acting in good faith to obtain the benefits of this liability protection. That is, where an entity acts in bad faith, it does not receive the benefit of the strong liability protection provided by the legislation. Of course, where an entity is seeking to take advantage of specific statutory authority provided by Congress and where Congress is seeking to incentivize cybersecurity activities, as with government action taken pursuant to statutory authority and the presumption of regularity that attaches to such actions, the Committee expects that good faith will be presumed in the absence of substantial evidence to the contrary.

Paragraph 4: Relationship to Other Laws Requiring the Disclosure of Information

Paragraph (4) provides that the provision of cyber threat information to the government under the voluntary system established by this statute does not satisfy or affect any requirement under other provisions of law to provide information to the Federal Government. As noted briefly earlier, the Committee intends this provision to ensure that while information provided to the government under this legislation is protected from use by the government for regulatory purposes, that information otherwise required to be provided to the government must still be provided and that such information—required by other law to be provided to the government—may still be used for all lawful purposes, including, as required by law, for regulatory purposes.

Section 1104(c) of Title 50: Federal Government Use of Information

Subsection (c) of new Section 1104 provides certain limitations on the government's use of information provided by the private sector and ensures that the private sector's provision of information to the government is purely voluntary. The Committee intends these provisions, along with others in the legislation, to help protect the privacy and civil liberties of Americans.

Paragraph (1): Limitation

Paragraph (1) of subsection (c) limits the Federal Government's use of information shared with the government by the private sector by requiring at least one significant purpose of the government's use of such information to be either a cybersecurity purpose or the protection of the national security of the United States. As such, the Committee intends this provision not to create a wall between cybersecurity and national security uses of information on one hand and all other lawful government uses on the other, rather it intends this provision simply to ensure that the government is using the information at least for cybersecurity or national security, amongst the other uses it might make of the information.

Paragraph (2): Affirmative Search Restriction

Paragraph (2) limits the Federal Government's affirmative searching of data provided exclusively under this legislation to the government by the private sector to only conducting such searches for cybersecurity purposes or the protection of the national security. The Committee intends this provision to ensure that information provided under this authority not be affirmatively searched by the government for evidence of garden-variety crimes like tax evasion or money laundering.

Paragraph 3: Anti-Tasking Restrictions

Paragraph (3) makes clear that nothing in this legislation permits the government to require a private sector entity to share with the Federal Government nor to condition the sharing of cyber threat intelligence under subsection (a) on the provision of cyber threat information back to the Federal Government under subsection (b). The Committee intends this provision to ensure that cyber threat information sharing by the private sector with the Federal Government remains purely voluntary and that the government not attempt to compel such sharing by withholding valuable cyber threat intelligence. The Committee believes that this provision also prevents the government from "tasking" the collection of information as the government might do under appropriate criminal or foreign intelligence surveillance authority because it ensures that the private sector cannot be required to provide information back to the government.

Section 1104(d) of Title 50: Report on Information Sharing

Subsection (d) of new Section 1104 requires the Inspector General of the Intelligence Community to report annually to the Congressional intelligence committees, in unclassified form accompanied by a classified annex as needed, on the use of the information shared with the Federal Government under this legislation. The report on the use of information shared with the Federal Government will include: (1) a review of the use of such information for purposes other than cybersecurity; (2) a review of the type of information shared with the Federal Government; (3) a review of the actions taken by the Federal Government based on the information shared; (4) appropriate metrics to determine the impact of such sharing on privacy and civil liberties, if any such impact exists; and (5) any recommendations of the Inspector General for improvements or modifications to the authorities provided under this

legislation. It is the Committee's intent that this report provide the Committee with the information it needs to ensure that the privacy and civil liberties of Americans are being appropriately protected.

Section 1104(e) of Title 50: Federal Preemption

Subsection (e) of new Section 1104 provides that the legislation supersedes any provision of state or local law that may prohibit the activities authorized by this legislation. The Committee's intent is to ensure, as with the federal provisions discussed above, that state and local law on wiretapping, antitrust, and public disclosure, to name but a few, do not stand as a bar to the kind of robust cyber threat intelligence and information sharing that the Committee hopes to engender through the process of legislation.

Section 1104(f) of Title 50: Savings Clause

Subsection (f) of new Section 1104 makes clear that nothing in this legislation trumps existing laws or authorities permitting the use of cybersecurity systems or efforts to identify, obtain, or share cyber threat information. Many private sector entities today take advantage of certain provisions of federal law to conduct the limited monitoring for cybersecurity purposes. While this legislation provides much more robust authorities, the Committee believed it important to ensure that existing authorities remained in place and that those authorities could continue to be used by the appropriate government agencies and entities.

Section 1104(g) of Title 50: Definitions

Subsection (g) of the new Section 1104 provides important definitions for the purpose of this legislation. The Committee notes that much of the work on limiting the scope and breadth of this legislation is done by the definitions and commends those interested in this legislation to carefully review these definitions in the context of the legislation.

Paragraph 1: Certified Entity

As noted briefly above, a certified entity is defined as a cybersecurity provider, a protected entity, or a self-protected entity that also possesses or is eligible to obtain a security clearance at the level appropriate to receive classified cyber threat intelligence, as determined by the DNI, and can demonstrate to the Director of National Intelligence that it can appropriately protect that classified information.

Paragraph 2: Cyber Threat Information

Cyber threat information is defined to mean information that directly pertains to a vulnerability of, or threat to, a system or network of a government or private entity. Such information includes, but is not limited to, information pertaining to the protection of a system or network from efforts to degrade, disrupt or destroy the network, as well as the protection of a system or network from the theft or misappropriation of private or government information, among other things.

Paragraph 3: Cyber Threat Intelligence

The definition of cyber threat intelligence is consistent with the definition of cyber threat information except that cyber threat intelligence is information that is originally in the possession of an element of the intelligence community. The Committee used different terms in this legislation with similar definitions in order to distinguish the origin of information. Cyber threat intelligence thus originates with the government while cyber threat information originates with the private sector.

Paragraph 4: Cybersecurity Provider

A cybersecurity provider is defined to be a non-governmental entity that provides goods or services intended to be used for cybersecurity purposes. The Committee intentionally excluded governmental entities from this construct to avoid any concern that government agencies might serve as cybersecurity providers to private sector entities.

Paragraph 5: Cybersecurity Purpose

A cybersecurity purpose is defined as the purpose of ensuring the integrity, confidentiality, and availability of, or safeguarding, a system or network. This includes, but is not limited to, the protection of a system or network from efforts to degrade, disrupt or destroy the network, as well as the protection of a system or network from the theft or misappropriation of private or government information, among other things.

Paragraph 6: Cybersecurity System

A cybersecurity system is defined as a system designed or employed to ensure the integrity, confidentiality, and availability of, or safeguard, a system or network. This includes, but is not limited to, a system designed or employed to protect a system or network from efforts to degrade, disrupt or destroy the network, as well as a system designed or employed to protect a system or network from the theft or misappropriation of private or government information, among other things.

Paragraph 7: Protected Entity

A protected entity is defined as an entity, other than an individual, that contracts with a cybersecurity provider for goods or services to be used for cybersecurity purposes. The Committee intentionally excluded individuals from this definition so as to limit the direct scope of the legislation to the protection of corporate entities.

Paragraph 8: Self-Protected Entity

A self-protected entity is defined as an entity, other than an individual, that provides goods or services for cybersecurity purposes to itself. As with the definition of a protected entity, the Committee intentionally excluded individuals from this definition so as to limit the direct scope of the legislation to the protection of corporate entities.

Section 2(b): Procedures and Guidelines

This subsection of the Act requires the DNI to establish the procedures for sharing of cyber threat intelligence and to issue the guidelines for granting security clearances within 60 days of the date of enactment of the Act. This subsection of the Act also requires the DNI to expeditiously distribute the procedures and guidelines to appropriate federal government and private sector entities. The Committee intends to require the DNI to meet these deadlines and to broadly distribute the procedures and guidelines. As previously noted, the Committee expects the DNI to work closely with the private sector in developing these procedures and guidelines.

Section 2(c): Initial Report

This subsection of the Act requires the first report to be provided to the Congressional intelligence committees by the Inspector General of the Intelligence Community under new subsection (d) of section 1104 to be provided no later than one year after the date of the enactment of this Act.

Section 2(d): Table of Contents Amendment

This subsection of the Act provides for amendments to the table of contents of the National Security Act of 1947.

OVERSIGHT FINDINGS AND RECOMMENDATIONS

With respect to clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee held two closed hearings, one open hearing, and four informal meetings or briefings relating to the subject matter of the legislation. The bill, as reported by the Committee, reflects conclusions reached by the Committee in light of this oversight activity.

GENERAL PERFORMANCE GOALS AND OBJECTIVES

In accordance with clause 3(c) of House rule XIII, the Committee's performance goals and objectives are reflected in the descriptive portions of this report.

UNFUNDED MANDATE STATEMENT

Section 423 of the Congressional Budget and Impoundment Control Act (as amended by Section 101(a)(2) of the Unfunded Mandates Reform Act, P.L. 104-4) requires a statement of whether the provisions of the reported bill include unfunded mandates. In compliance with this requirement, the Committee has received a letter from the Congressional Budget Office included herein.

STATEMENT ON CONGRESSIONAL EARMARKS

Pursuant to clause 9 of rule XXI of the Rules of the House of Representatives, the Committee states that the bill as reported contains no congressional earmarks, limited tax benefits, or limited tariff benefits.

BUDGET AUTHORITY AND CONGRESSIONAL BUDGET OFFICE
COST ESTIMATE

With respect to the requirements of clause 3(c)(2) of rule XIII of the Rules of the House of Representatives and section 308(a) of the Congressional Budget Act of 1974 and with respect to requirements of 3(c)(3) of rule XIII of the Rules of the House of Representatives and section 402 of the Congressional Budget Act of 1974, the Committee has received the following cost estimate for H.R. 3523 from the Director of the Congressional Budget Office:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, December 16, 2011.

Hon. MIKE ROGERS,
*Chairman, Permanent Select Committee on Intelligence,
House of Representatives, Washington, DC.*

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 3523, the Cyber Intelligence Sharing Act.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Jason Wheelock.

Sincerely,

DOUGLAS W. ELMENDORF.

Enclosure.

H.R. 3523—Cyber Intelligence Sharing Act

H.R. 3523 would amend the National Security Act of 1947 to require the Director of National Intelligence (DNI) to establish procedures to promote the sharing of information about cyberthreats between intelligence agencies and the private sector. The DNI also would be directed to establish guidelines for granting security clearances to employees of the private-sector entities with which the government shares such information. CBO estimates that implementing the bill would have a discretionary cost of \$15 million over the 2012–2016 period, assuming appropriation of the necessary amounts. Enacting H.R. 3523 would not affect direct spending or revenues; therefore, pay-as-you-go procedures do not apply.

CBO anticipates additional personnel would be needed to administer the program and to manage the exchange of information between intelligence agencies and the private sector. Based on information from the DNI and the Office of Personnel Management, CBO estimates that those activities would cost approximately \$3 million annually over the 2012–2016 period, assuming appropriation of the necessary amounts.

The bill would impose intergovernmental and private-sector mandates, as defined in the Unfunded Mandates Reform Act (UMRA), by extending civil and criminal liability protection to entities and cybersecurity providers that share or use cyberthreat information. The bill also would impose additional intergovernmental mandates by preempting state laws. Because CBO is uncertain about the number of cases that would be limited and any forgone compensation that would result, CBO cannot determine whether the costs of the mandate would exceed the annual threshold established in UMRA for private-sector mandates (\$142 million in 2011, adjusted

annually for inflation). However, CBO estimates that the aggregate costs of the mandates on public entities would fall below the threshold for intergovernmental mandates (\$71 million in 2011, adjusted annually for inflation).

The CBO staff contacts for this estimate are Jason Wheelock (for federal costs), J'nell J. Blanco (for the intergovernmental impact), and Elizabeth Bass (for the private-sector impact). This estimate was approved by Theresa Gullo, Deputy Assistant Director for Budget Analysis.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (new matter is printed in italic and existing law in which no change is proposed is shown in roman):

NATIONAL SECURITY ACT OF 1947

SHORT TITLE

That this Act may be cited as the “National Security Act of 1947”.

TABLE OF CONTENTS

Sec. 2. Declaration of policy.

* * * * *

TITLE XI—OTHER PROVISIONS

* * * * *

Sec. 1104. *Cyber threat intelligence and information sharing.*

* * * * *

TITLE XI—ADDITIONAL MISCELLANEOUS PROVISIONS

* * * * *

CYBER THREAT INTELLIGENCE AND INFORMATION SHARING

SEC. 1104. (a) INTELLIGENCE COMMUNITY SHARING OF CYBER THREAT INTELLIGENCE WITH PRIVATE SECTOR.—

(1) *IN GENERAL.—The Director of National Intelligence shall establish procedures to allow elements of the intelligence community to share cyber threat intelligence with private-sector entities and to encourage the sharing of such intelligence.*

(2) *SHARING AND USE OF CLASSIFIED INTELLIGENCE.—The procedures established under paragraph (1) shall provide that classified cyber threat intelligence may only be—*

(A) *shared by an element of the intelligence community with—*

(i) *certified entities; or*

(ii) *a person with an appropriate security clearance to receive such cyber threat intelligence;*

(B) *shared consistent with the need to protect the national security of the United States; and*

(C) *used by a certified entity in a manner which protects such cyber threat intelligence from unauthorized disclosure.*

(3) *SECURITY CLEARANCE APPROVALS.*—The Director of National Intelligence shall issue guidelines providing that the head of an element of the intelligence community may, as the head of such element considers necessary to carry out this subsection—

(A) grant a security clearance on a temporary or permanent basis to an employee or officer of a certified entity;

(B) grant a security clearance on a temporary or permanent basis to a certified entity and approval to use appropriate facilities; and

(C) expedite the security clearance process for a person or entity as the head of such element considers necessary, consistent with the need to protect the national security of the United States.

(4) *NO RIGHT OR BENEFIT.*—The provision of information to a private-sector entity under this subsection shall not create a right or benefit to similar information by such entity or any other private-sector entity.

(b) *PRIVATE SECTOR USE OF CYBERSECURITY SYSTEMS AND SHARING OF CYBER THREAT INFORMATION.*—

(1) *IN GENERAL.*—

(A) *CYBERSECURITY PROVIDERS.*—Notwithstanding any other provision of law, a cybersecurity provider, with the express consent of a protected entity for which such cybersecurity provider is providing goods or services for cybersecurity purposes, may, for cybersecurity purposes—

(i) use cybersecurity systems to identify and obtain cyber threat information to protect the rights and property of such protected entity; and

(ii) share such cyber threat information with any other entity designated by such protected entity, including, if specifically designated, the Federal Government.

(B) *SELF-PROTECTED ENTITIES.*—Notwithstanding any other provision of law, a self-protected entity may, for cybersecurity purposes—

(i) use cybersecurity systems to identify and obtain cyber threat information to protect the rights and property of such self-protected entity; and

(ii) share such cyber threat information with any other entity, including the Federal Government.

(2) *USE AND PROTECTION OF INFORMATION.*—Cyber threat information shared in accordance with paragraph (1)—

(A) shall only be shared in accordance with any restrictions placed on the sharing of such information by the protected entity or self-protected entity authorizing such sharing, including appropriate anonymization or minimization of such information;

(B) may not be used by an entity to gain an unfair competitive advantage to the detriment of the protected entity or the self-protected entity authorizing the sharing of information; and

(C) if shared with the Federal Government—

(i) shall be exempt from disclosure under section 552 of title 5, United States Code;

(ii) shall be considered proprietary information and shall not be disclosed to an entity outside of the Federal Government except as authorized by the entity sharing such information; and

(iii) shall not be used by the Federal Government for regulatory purposes.

(3) *EXEMPTION FROM LIABILITY.*—No civil or criminal cause of action shall lie or be maintained in Federal or State court against a protected entity, self-protected entity, cybersecurity provider, or an officer, employee, or agent of a protected entity, self-protected entity, or cybersecurity provider, acting in good faith—

(A) for using cybersecurity systems or sharing information in accordance with this section; or

(B) for not acting on information obtained or shared in accordance with this section.

(4) *RELATIONSHIP TO OTHER LAWS REQUIRING THE DISCLOSURE OF INFORMATION.*—The submission of information under this subsection to the Federal Government shall not satisfy or affect any requirement under any other provision of law for a person or entity to provide information to the Federal Government.

(c) *FEDERAL GOVERNMENT USE OF INFORMATION.*—

(1) *LIMITATION.*—The Federal Government may use cyber threat information shared with the Federal Government in accordance with subsection (b) for any lawful purpose only if—

(A) the use of such information is not for a regulatory purpose; and

(B) at least one significant purpose of the use of such information is—

(i) a cybersecurity purpose; or

(ii) the protection of the national security of the United States.

(2) *AFFIRMATIVE SEARCH RESTRICTION.*—The Federal Government may not affirmatively search cyber threat information shared with the Federal Government under subsection (b) for a purpose other than a purpose referred to in paragraph (1)(B).

(3) *ANTI-TASKING RESTRICTION.*—Nothing in this section shall be construed to permit the Federal Government to—

(A) require a private-sector entity to share information with the Federal Government; or

(B) condition the sharing of cyber threat intelligence with a private-sector entity on the provision of cyber threat information to the Federal Government.

(d) *REPORT ON INFORMATION SHARING.*—

(1) *REPORT.*—The Inspector General of the Intelligence Community shall annually submit to the congressional intelligence committees a report containing a review of the use of information shared with the Federal Government under this section, including—

(A) a review of the use by the Federal Government of such information for a purpose other than a cybersecurity purpose;

(B) a review of the type of information shared with the Federal Government under this section;

(C) a review of the actions taken by the Federal Government based on such information;

(D) appropriate metrics to determine the impact of the sharing of such information with the Federal Government on privacy and civil liberties, if any; and

(E) any recommendations of the Inspector General for improvements or modifications to the authorities under this section.

(2) *FORM.*—Each report required under paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

(e) *FEDERAL PREEMPTION.*—This section supersedes any statute of a State or political subdivision of a State that restricts or otherwise expressly regulates an activity authorized under subsection (b).

(f) *SAVINGS CLAUSE.*—Nothing in this section shall be construed to limit any other authority to use a cybersecurity system or to identify, obtain, or share cyber threat intelligence or cyber threat information.

(g) *DEFINITIONS.*—In this section:

(1) *CERTIFIED ENTITY.*—The term “certified entity” means a protected entity, self-protected entity, or cybersecurity provider that—

(A) possesses or is eligible to obtain a security clearance, as determined by the Director of National Intelligence; and

(B) is able to demonstrate to the Director of National Intelligence that such provider or such entity can appropriately protect classified cyber threat intelligence.

(2) *CYBER THREAT INFORMATION.*—The term “cyber threat information” means information directly pertaining to a vulnerability of, or threat to, a system or network of a government or private entity, including information pertaining to the protection of a system or network from—

(A) efforts to degrade, disrupt, or destroy such system or network; or

(B) theft or misappropriation of private or government information, intellectual property, or personally identifiable information.

(3) *CYBER THREAT INTELLIGENCE.*—The term “cyber threat intelligence” means information in the possession of an element of the intelligence community directly pertaining to a vulnerability of, or threat to, a system or network of a government or private entity, including information pertaining to the protection of a system or network from—

(A) efforts to degrade, disrupt, or destroy such system or network; or

(B) theft or misappropriation of private or government information, intellectual property, or personally identifiable information.

(4) *CYBERSECURITY PROVIDER.*—The term “cybersecurity provider” means a non-governmental entity that provides goods or services intended to be used for cybersecurity purposes.

(5) *CYBERSECURITY PURPOSE.*—The term “cybersecurity purpose” means the purpose of ensuring the integrity, confidentiality, or availability of, or safeguarding, a system or network, including protecting a system or network from—

(A) efforts to degrade, disrupt, or destroy such system or network; or

(B) theft or misappropriation of private or government information, intellectual property, or personally identifiable information.

(6) *CYBERSECURITY SYSTEM.*—The term “cybersecurity system” means a system designed or employed to ensure the integrity, confidentiality, or availability of, or safeguard, a system or network, including protecting a system or network from—

(A) efforts to degrade, disrupt, or destroy such system or network; or

(B) theft or misappropriation of private or government information, intellectual property, or personally identifiable information.

(7) *PROTECTED ENTITY.*—The term “protected entity” means an entity, other than an individual, that contracts with a cybersecurity provider for goods or services to be used for cybersecurity purposes.

(8) *SELF-PROTECTED ENTITY.*—The term “self-protected entity” means an entity, other than an individual, that provides goods or services for cybersecurity purposes to itself.

MINORITY VIEWS

CYBER INTELLIGENCE SHARING AND PROTECTION ACT, H.R. 3523

As members of the Intelligence Committee, it is our responsibility to ensure that intelligence support to the cybersecurity of our nation is focused and robust. The Intelligence Community's unique insight and knowledge of cyberspace are critical to our nation's ability to defend, not only U.S. Government information technology, but also our Critical Infrastructure and Defense Industrial Base.

This Bill is the culmination of a strong bipartisan effort and provides an innovative, yet pragmatic, approach to cybersecurity. It leverages the Intelligence Community's expertise and incentivizes the private sector to share cyber threat information in order to build an enduring private-public partnership for this strategic threat to our nation's security. Specifically, the Cyber Intelligence Sharing and Protection Act provides the authority for the Intelligence Community to share classified cyber threat intelligence with properly-vetted industry partners and encourages the voluntary sharing of cyber threat information with the U.S. Government.

It is the Minority's strong intent in supporting this Bill to facilitate this private-public sharing of information regarding malevolent cyber activity in a way that ensures that the privacy and civil liberties of U.S. persons are respected and protected. An equitable and ethical balance between flexible information sharing and privacy must be established, maintained and vigilantly reviewed.

We express continued interest in working with the Majority to further address concerns raised by the Administration and civil liberties organizations.

We believe that this Bill and its amendments strike this delicate balance by requiring that any shared information used by the Government meet a cybersecurity or national security threshold and by prohibiting the Government's use of shared information for regulatory purposes. Moreover, in recognition that this Bill is a pioneering effort, this Committee is fully committed to diligent oversight of the parties' conduct pursuant to this Bill.

The Bill directs the Intelligence Community Inspector General to be alert to and review any U.S. Government activity or use of shared information that goes beyond the cybersecurity focus of this Bill. Should that oversight identify significant concerns or abuse, the Minority is committed to working with the Majority to take all appropriate and timely action to further enhance privacy protections.

To repeat: the Minority supported this Bill in the expectation that, both the participating private companies and the Government, will appreciate and not abuse the flexibility and liability protection afforded by this Bill. With the dedicated support of both

government and industry—overlaid with Congressional oversight—we are optimistic that this Bill will work as envisioned to strengthen cybersecurity in a manner that respects American values.

C.A. DUTCH RUPPERSBERGER.
MIKE THOMPSON.
JIM LANGEVIN.
ADAM B. SCHIFF.
DAN BOREN.
BEN CHANDLER.

MINORITY VIEWS

CYBER INTELLIGENCE SHARING AND PROTECTION ACT, H.R. 3523

The intent of this Bill is to authorize the U.S. Government to share classified cybersecurity intelligence with the private sector in a secure manner and to enable the private sector to share cybersecurity information with the U.S. Government in real-time, without fear of liability if acting in good faith.

I agree that we are facing serious cyber threats and that all Americans will benefit from strong cybersecurity protections for our critical infrastructure. However, I believe we need to balance those concerns with measures to protect the privacy and civil liberties that Americans also deserve. While I appreciate the efforts of authors of this bipartisan bill and its focus on cybersecurity, I believe that balance has not yet been achieved.

Although the Bill includes adequate protections for classified information and corporate proprietary information, its language does not provide commensurate protection for the personal accounts of U.S. persons or personal identifiable information (PII). For example, the Bill's language does not restrict the nature or volume of the information that the private sector can share with the Government, does not provide for mandatory minimization of PII, does not significantly curtail the Government's use of shared information, and does not include most of the privacy protections recommended by the White House in its proposed cybersecurity legislation.

I am also concerned that the new liability shield provided in the Bill is overly broad and is less protective of consumers than similar shields provided under many state laws. We should be very careful whenever we limit injured consumers' ability to seek legal redress. If a good faith requirement is to be used, it should be based on clear and objective criteria. In no event, however, should cybersecurity entities be protected if injuries are the result of neglect, recklessness or misconduct.

Accordingly, while I strongly agree with the need to enact effective cybersecurity legislation, and commend the constructive bipartisan effort underlying this Bill, I respectfully dissent because the Bill does not sufficiently protect individual privacy rights and civil liberties.

JANICE D. SCHAKOWSKY.

○