

ICIT - Institute for Critical Infrastructure Technology

Progress as Two Steps Forward and One Step Back: Analysis of H.R. 1560 Title I and Title II (H.R. 1731)

ICIT

The Institute for Critical Infrastructure Technology (ICIT) is a non-profit (status pending), non-partisan collaboration of the world's leading experts and companies in cybersecurity and technology, which provides solutions to support and protect our Nation's critical infrastructure. Comprised of fellows from all political backgrounds and sectors, ICIT is uniquely well positioned to offer niche advisory to the policy community in fields of critical infrastructure and technology.

Cybersecurity Reform is Long Overdue

Every single American is the victim of the cybersecurity breaches that permeate modern media. If the personal information of a given citizen is not compromised like that of the 110 million users in the Target breach, the 154 million compromised by the Adobe breach, the 145 million accounts stolen during the ebay breach, the 90 million users in the Anthem and Premera breaches, or countless others in recent news, then citizens suffer from the trickle-down financial burden placed on affected businesses. According to FBI Director James Comey, "There are two kinds of big companies in the United States. There are those who've been hacked...and those who don't know they've been hacked." Critical Infrastructure and government systems are often targeted as well. www.heritage.org predicts that for every business in the United States, an average of \$8.6 million was spent on cybersecurity defense in 2014. An average of \$16 million was spent for each successful breach in the Financial Services, Technology, and Communications sectors. The cost of many large breaches, such as the Target or Home Depot breach drastically exceed \$16 million. 42.8 million breaches occurred in 2014 and the rate of attacks is predicted to continue to increase at 66% each year. As the impact of attacks increase in this digital age, cybersecurity can no longer be considered as an afterthought. Congress must enact measures to reduce the likelihood of success of breaches and to promote a culture within the private sector that prioritizes cybersecurity. A given attacker often utilizes similar malware to attack businesses across multiple sectors, as was the case with Home Depot, Target, and Sally Beauty. Cybersecurity reform is long overdue. H.R. 1560 proposes a systematic approach to allow non-Federal entities to share cybersecurity threat information with each other and the Federal Government to mitigate the impact of breaches or prevent imminent threats from ever breaching systems.

Analysis of 1560 Title I: Protecting Cyber Networks Act

The Protecting Cyber Networks Act (PCNA) amends the National Security Act of 1947 "by providing clear legal authority for the sharing of information about cybersecurity threats between and among the non-Federal entities and the Federal Government." Within the first 90 days, the Director of

National Intelligence, in consultation with the heads of appropriate Federal entities¹, must create and disseminate procedures that facilitate the real time sharing of cyber threat indicators (CTI's) between the Federal Government and non-Federal entities in a manner that "is consistent with the protection of classified information, intelligence sources and methods, and privacy and civil liberties." The procedures must facilitate:

- the exchange of classified CTI's between the Federal Government and representatives of relevant non-Federal entities with proper security clearance;
- the exchange of declassified CTI's between the Federal Government and representatives of relevant non-Federal entities;
- the exchange of appropriate cybersecurity information in possession of the Federal Government about imminent or ongoing cybersecurity threats that may enable affected non-Federal entities to prevent or mitigate adverse impacts of the attack.

When possible, the procedures should utilize existing roles, responsibilities, and processes of Federal and non-Federal entities. The Federal Government notifies non-Federal entities if the former provides CTI's in error or violation of the Act to the latter. The Federal Government ensures secure transfer, access, and storage of received CTI's along with a review of the CTI to ensure that no personally identifiable information (PII) lingers prior to dissemination of the CTI to the intelligence community.

Section 103 of PCNA permits private entities to monitor and defend their own networks or networks under their authority provided express permission. Absolutely no part of the bill authorizes any action that limits lawful activity or permits the Federal Government to conduct surveillance of any person². Neither the Federal Government nor a non-Federal entity may employ a defensive measure that "destroys, renders unusable or inaccessible, or substantially harms an information system or information stored on, processed by, or transiting such information systems" not owned by the private entity or under the authority of the private entity with express permission. This provision prohibits "hack-back" attacks in which an entity would hack a presumed attacker based on information garnered from network surveillance. Among other reasons, "hack-back" action is problematic because some cyberattacks, such as DDos campaigns, utilize the resources of networks that the actor has infected with malware prior to the incident. Additionally, "hack-back" authorization is difficult to govern and cascading incidents could lead to an environment where parties perpetually revolve around a "hack-back" loop with no discernible indicator of origin. Conversely, some experts believe the provision limits user incident response. The provision restricts proactive action against attackers. An absolute restriction could impede the ability to disrupt some attacks. In numerous cases, "pulling the plug" on an infected machine is considered a viable option to halt an incident and minimize damage. This course of action may damage the system and result in loss of data; however, it could also minimize the impact of a breach.

¹ Appropriate Federal entities defined as Departments of Homeland Security, Treasury, Justice, Commerce, and Defense at the time of this writing.

² Section 103(a)(2)(B) and Section 103(c)(3)(F) expressly ban Federal entities from conducting surveillance of a person based on the Act.

Other experts believe this course of action to be rash and the result of improper risk assessment because an attack on an unplugged machine cannot be monitored or log the information necessary for legal proceedings or insurance claims. In fact, in some sectors, destructive action is illegal or discouraged; though many businesses still accept the sanctions if the fines and legal fees are lower than the potential value of compromised data. There is no incentive for H.R. 1560 to permit destructive action because cyber threat information cannot be gathered or shared from a destroyed system. H.R. 1560 is not intended to limit the avenues of response for a breach. A balanced alteration to this provision might require participants in information sharing to forfeit the right to engage in destructive action via a signed contract. Organizations that do not participate in the program would remain unaffected.

Section 103 also authorizes private entities to share CTI's and defensive methodology with other private entities and with the Federal Government (other than the Department of Defense and the NSA) for cybersecurity purposes, if the transaction does not violate any other laws. The transaction cannot inhibit lawful activity, allows the Federal Government to conduct surveillance on any person, or interrupt lawful channels that private entities utilize to report information to the DoD or NSA. While the Federal Government cannot use CTI's to monitor or prosecute an individual, State, tribal and local governments³ are given the express permission to use CTI's for law enforcement of:

- a cybersecurity purpose;
- the purpose of responding to, investigating, prosecuting, or otherwise preventing or mitigating a threat of death or serious bodily harm or an offense arising from such a threat;
- the purpose of responding to, investigating, prosecuting, or otherwise preventing or mitigating a serious threat to a minor, including threats of sexual exploitation and threats to physical safety ; or
- the purpose of preventing, investigating, disrupting, or prosecuting offenses listed in sections 1028, 1029, 1030, and 3559(c)(2)(F) and chapters 37 and 90 of Title 18, United States Code. These offenses include espionage, economic espionage, serious violent felonies, or violations of the Computer Fraud & Abuse Act.

Section 103 details that any PII must be removed from a CTI prior to transference from one party to another. If the recipient is the Federal Government, then the aforementioned secondary review of the will remove any PII that the sender failed to eliminate. PCNA does not mandate a secondary scrubbing procedure for private recipients. This topic and similar privacy issues will be discussed in later sections.

The Small Business Administration is required to provide assistance to small and medium businesses to monitor information systems, share and receive CTI's, and engage in defensive measures. Notably, H.R. 1560 does not require SBA to assist in small and medium businesses in scrubbing PII from CTI's. Since small and medium businesses are the most likely segment to lack the necessary resources and knowledge, a suggested provision would include such assistance and training.

³ Information shared with local, tribal, or State governments is exempt from disclosure laws.

The President is required to develop and submit to Congress policies and procedures governing the Federal Government reception of CTI's and defense measures and the real time dissemination of novel information amongst relevant Federal entities and appropriate components of those entities. The President's policies must be developed in accordance with privacy and civil liberty guidelines. Further, the policies must ensure that CTI's shared within the Federal Government are shared without delay, bias, or modification. The policy creates an audit capability, which "keeps honest people honest" by promoting transparency and inspiring compliance. Sanctions for negligent or malicious mishandling of cybersecurity or personal information by Federal officers, agents, and employees also deter detrimental activity.

The Attorney General is responsible for working with the heads of appropriate Federal entities to develop and periodically review privacy and civil liberty guidelines. These guidelines govern the receipt, retention, use, dissemination, and lifetime of CTI's. The guidelines will ensure that the recipient of CTI's knowingly agrees to only act on the information for cybersecurity purposes. Additionally, the guidelines mandate the prompt destruction of any PII prior to transmitting any information. Sanctions on participants who fail to eliminate PII should be implemented to deter willful misconduct or negligence.

The most important aspect of either PCNA or NCPAA is that participation is voluntary. Participants who share information "in good faith" with the Federal Government or private entities are protected from liability associated with the monitoring of information systems and the liability associated with sharing and receiving CTI's⁴. The language describing liability protection in Section 106 of H.R. 1506 might be too broad to garner wide-scale participation. Congress should provide a more definition of liability to potential non-Federal partners so that the risks and benefits of the decision to share and receive CTI's can be measured against the organization's risk appetite. Organizations that find the clear liability definition appealing will participate and will be less likely to violate privacy or civil liberties intentionally or as a result of negligence. All other entities will not participate and therefore cannot violate the privacy and civil liberties of citizens as a result of the program.

Private entities are not liable for "good faith" failures to act on received information. Public concern opposes this allowance for informed inaction. In fact, the Office of Management and Budget of the President of the United States of America has likewise expressed displeasure that H.R. 1560 allows participating businesses to choose not to protect systems from imminent threat. As such, companies are risking the exposure of user information to an attacker if protective measures outweigh the cost of the breach. Companies can recover from financial impacts. It is significantly more difficult for the people affected by a breach to recover. As the overall intent of H.R. 1560 is to improve American cybersecurity for the sake of infrastructure and businesses in service of the American people, this allowance perverts the intention of the bill and could lead to cascading impacts in the future.

In a support letter from the Office of Budget and Management of the President of the United States, the Obama Administration expressed concern about offering "immunity" liability protection

⁴ This liability protection supersedes disclosure and anti-trust laws.

instead of a more restrained “incentive” liability protection. Organizations such as the ACLU and 55 others who signed a petition opposed to 1560 are concerned that the generous liability protection will deter the caution of private entities and lead to lax PII removal measures. The Federal Government can only guarantee PII removal on information passed to the Federal Government. The Federal Government implements every practical measure to protect privacy and civil liberties on its own behalf in PCNA. However, information passed between private entities, as allowed by Section 103 (c), is unregulated in the current form of the bill. Organizations vary in size and budget, reason dictates that without strict governance, the degree of PII removal is proportional to the size, resources, and concern of the organization under consideration.

The office of the President also expressed concern that the unmonitored private-private sharing could be used as a form of anti-competition. A private-private coalition could exclude competitors or share CTI’s in such a way as to gain a competitive edge. The use of a masking system that obfuscates the identity of the sender and receiver of CTI’s would mitigate this risk save for very creative signaling methods. An alternate solution that ensures PII removal and competitive market integrity at the cost of greater administrative burden would be to pass all requests through an intermediary such as DNI’s CTIIC or DHS’s NCCIS. The identity of the sender and receiver would be unknown to the other party and all exchanges could be monitored, logged, and audited. Further, the Federal Government could receive and analyze all CTI’s. Many organizations in support of H.R. 1560 have expressed displeasure with the “uni-directional” relationship with the Federal Government. A Federal information hub would offer the Federal Government greater insight into the cyber threat environment and it would allow the Federal Government to serve a more “bi-directional” role.

Section 119b (d)(2) stipulates that CTI’s remain the proprietary property of origin sender; however the liability blanket provides that sharing CTI’s cannot be used against said organization in court. This combination greatly limits viable legal action if the privacy or civil liberties of the public or injured parties become compromised through negligence or non-misconduct

The United States Government assumes all legal liability for the intentional or willful violation of the privacy or civil liberties of any person by a Federal department, agency, or employee thereof. While this policy demonstrates an accountable and transparent system, it forgoes critical insight. Legal burden of proof falls entirely upon the injured party who may not be cognizant of the disclosure of PII or other information due to the nebulous, and often classified, exchange of information. In the current form, only individual people qualify as litigants. Since businesses or organizations may fault the Government should data be misused, the language may need altered to reflect that concern. Daunted litigants still may not pursue legal action against the United States Federal Government even if information is misused. Conversely, the Federal Government assumption of liability may discourage contractor association. As before, opposed organizations have expressed displeasure that at the “high-bar” set for the litigant in the provision. Even more opposition to H.R.1560 stems from the lack of accountability of private entities that do not hold to the same standard of legal accountability.

One prominent feature of Title I of H.R. 1560 is the focus on transparency and accountability. Processes often require audit procedures. Reports to Congress and the President will be publically

available, save classified annexes. The intent of the bill and the ban on Federal surveillance of any person through the bill is apparent throughout the document. The scope of the bill is limited through definitions and restrictions. Some broad language, notably “reasonable”, “timely”, etc., bears consideration for refinement. Quantitative qualifiers provide greater efficiency than qualitative, relative terms.

4. Analysis of 1560 Title II: National Cybersecurity Protection Advancement Act (Formerly H.R. 1731)

The National Cybersecurity Protection Advancement Act (NCPAA) amends the Homeland Security Act of 2002 to expand the composition of the National Cybersecurity and Communications and Integration Center (NCCIC) to allow it to collaborate with local and state governments, information sharing and analysis centers, and private entities on issues pertaining to cybersecurity. NCCIC is capable of serving as the primary interface between the Federal Government and non-Federal entities. Title II fails to include facilitation of the transfer of classified information between the Federal Government and cleared entities. Addition of the distinction will mitigate the likelihood of erroneous transactions. Further, the addition allows for inclusion of guidelines detailing processes that organizations can follow to apply for clearances.

With the addition of a U.S. Computer Emergency Response Team (U.S. CERT) that provides technical information and assistance and the addition of an Industrial Control System Cyber Emergency Response Team (ICS CERT) that coordinates trains and pioneers new technology, NCCIC can fulfill the role of the multi-directional, cross sector facilitator that non-Federal entities expect the Federal Government to provide. The DHS Inspector General will review the ability of U.S. CERT and ICS CERT to assist, train and inspire compliance in non-Federal entities. Congress can include provisions mandating that the CERTs monitor the annual trend in cybersecurity events/ incidents as a quantitative measure of the success of the program. Current cybersecurity trends and future predictions can benchmark the metric.

DHS may assist any Federal entity in dealing with a cybersecurity incident. NCCIC is equipped to coordinate small and medium businesses, collaborate with state and local governments on cybersecurity risks and incidents, and provide a National Coordinating Center for Communications that “coordinates the protection, response, and recovery of emergency communications. “ NCCIC will also engage in the improvement of the security and resiliency of existing public communication networks. In all of these efforts, NCCIC should train partners in best practices in areas such as inventory control and disposal. The CERT divisions can assist with regular vulnerability and risk assessments.

NCCIC would be required to collaborate with global cybersecurity partners, state and major urban fusion centers, small and medium businesses, and Congress (through biannual reports regarding significant violations of information retention or disclosure policies). NCCIC will also advise Congress improving cybersecurity collaboration efforts with international partners. The Under Secretary for Science and Technology will advise Congress biennially about critical infrastructure security risks and associated security technology gaps.

Since NCCIC must participate in DHS's National Exercise Program, NCCIC will be more capable in training non-Federal entities. Further, NCCIC will begin a national awareness program to teach the general public about the significance of information security. Public service announcements will be targeted to reach teens, the elderly, local governments, members of Armed Forces, and other high target demographics. Voluntary best practices for the public, vendors, and businesses will also be disseminated to improve user action. By training businesses and users, NCCIC will greatly diminish errors due to negligence and ignorance in the future. DHS will establish a National Cybersecurity Preparedness Consortium to train officials and emergency responders to properly respond during a cybersecurity attack. Congress could also provide the resources to allow NCCIC to train organizations to remove PII and better ensure the protection of privacy and civil liberties.

As PCNA in Title I, NCPAA focuses on limiting unauthorized disclosure and protecting privacy and civil liberties. Unlike PCNA, NCPAA directly monitors non-Federal privacy and civil liberty management by directing the NCCIC to work directly with the Chief Privacy Officer. The CPO ensures privacy and civil liberty policy compliance by monitoring the organization, updating practices, and submitting regular assessments. The impact of sharing CTI's and defensive measures on DHS retention, use, and disclosure policies is explored alongside impact mitigation strategies.

Rather than maintain the specified departmental roles in PCNA, NCPAA seeks to develop capabilities that use the existing industry standards to advance and automate real time CTI sharing within and across relevant sectors. Advancements are reported to Congress biannually to establish accountability and transparency. Non-Federal entities operate much the same as under PCNA. NCCIC, like the DNI, does all that it can to ensure that non-Federal entities remove PII and destroyed the sensitive information.

NCPAA addresses and extends many of the policies as PCNA. As in PCNA, the Federal Government cannot use any information from the bill to engage in the surveillance of any person. The Federal Government expressly cannot require a non-Federal entity to share information. Additionally, under NCPAA, the government cannot use information for regulatory purposes. Symmetrically, NCPAA addresses the issue of anti-competition among private entities by expressly invoking anti-trust laws on suspect economic partnerships.

The Protection Privacy and Civil Liberties

The primary debate over of H.R. 1560 centers on the removal of personally identifiable information (PII) from shared cybersecurity threat indicators (CTI's) and the use of information sharing networks for surveillance. The current form of H.R. 1560 requires businesses to take "reasonable efforts" to remove PII prior to sharing. Additionally, the Federal Government will take efforts to remove PII from received information prior to dissemination within the intelligence community. As alluded to in the April 21, 2015 letter of support from the Office of Management and Budget of the President of the United States, these statements are insufficient. No quantitative metric defines "reasonable measures" nor is shared information investigated to ensure the removal of PII. Because H.R. 1560 offers liability protection more as immunity than incentive, there is no incentive for businesses to take adequate

measures to remove PII. H.R. 1560 does not detail penalties for PII shared unless the transaction falls under the purview of willful misconduct.

Without accountability governance, businesses will negligently⁵ share PII and unwilling and unknowing consumers will assume additional, albeit unnecessary, risk. Clarifications to H.R. 1560 can prevent this outcome before negative impacts spoil the positive potential of the bill. In the current form, the Director of National Intelligence and the President of the United States are responsible for submitting to Congress policies and procedures for the transmission and reception of cybersecurity indicators within 90-180 days of the passage of the bill. “Reasonable measures” of scrubbing data to remove PII should be explicitly defined prior to passage of H.R. 1560. Policy and practice to transfer CTI’s securely should likewise be defined prior to the first transaction. Definition and specification of the information necessary to include in CTI composition greatly mitigates much of the privacy debate because there is extremely limited reason that PII would ever be included unless a breach had occurred; at which point, the victims of compromised information have a right to be informed. H.R. 1560 should restrict shared information to include only information necessary for cybersecurity improvement. Participants in the program should sign contracts affirming their acknowledgement of secure and necessary practices and legally committing to adhere to specified measures. DHS should offer to assist small and medium businesses remove PII from CTI’s, provided that need of the financial assistance can be verified. Budget constraints should never be an acceptable excuse for the exposure of PII nor should companies be capable of utilizing the liability protection offered by H.R. 1560 to prevent legal action resulting from negligence. Public opinion indicates the recommendation that DHS and Congress enact punishments, up to and including redaction of liability protection and expulsion from the program, for partners who misuse the program when sharing information with Federal or non-Federal entities.

Similarly, DHS should submit standardized formats for CTI transfer and submission. These formats may differ according to sector. Organizations log and react to events and incidents differently. Without a standardization of logging procedures and reporting procedures, recipients of data will spend unnecessary resources translating transferred information into useful data. Standardized data can be correlated to discern noticeable trends and patterns that indicate attacks. Such measures will also prevent data-bloat, the obfuscation of necessary data amidst an overabundance of “big-data”. The efficiency of the entire program will greatly increase, as received data will be devoid of an accompanying period of inaction and confusion.

Privacy and civil liberties are best preserved when security and accountability are implemented at each stage. The Federal Government goes to great length to offer a transparent and accountable process of information sharing. Participating non-Federal entities need to adopt similar policies relating to punishment of insider-threat employees who misuse or misappropriate data. Without appropriate caution, a single insider threat, with less privileged access to information than Edward Snowden, could irrevocably harm the cybersecurity of the entire nation. The impact of CTI exposure increases as the scale of the program increases and as the Federal Government becomes more involved. Conversely, the

⁵ Often attributed to “budget constraints” after a breach has occurred.

Federal Government should create and support procedures⁶ to allow white-hat insiders to report misuse of information acquired through H.R. 1560. “Whistle-blower” procedures also allow insiders to report breaches to the Federal Government when the partner organization fails to protect consumer data.

In the event that a business unintentionally shares or receives PII, policy measures can mitigate the likelihood that a black-hat actor will use that information. Further, requirements on the security of databases and servers containing CTI’s ensure that attackers cannot breach a participant to learn or poison shared information. The burden of securing CTI’s through encryption, cyber-infrastructure security, and data integrity checks⁷ belongs to the holder of the data. The responsibility of the Federal Government is to ensure that participants adopt such policies.

H.R. 1560 prohibits the Federal Government, and associated intelligence communities, from conducting surveillance of any person, seven times in the document. Along with the provisions banning “hacking back” and the focus on the removal of PII, there is little more that the Government can do to stress that H.R. 1560 is not a “Big Brother” bill, short of a public relations campaign. Even if a CTI, associated with the program, helps identify a potential threat agent, for better or worse, the activities of the agent cannot be monitored by the Federal Government or the intelligence community. CTI information likely would not be correlated in a manner that would allow for the identification of a single threat agent. Surveillance is not the focus or intent of H.R. 1560. The only allowance for the use of CTI’s in law enforcement is at the State and local levels for narrowly defined purposes specified in the Analysis of 1560 Title I above.

The Proper Interface

Section 104 of PCNA establishes a Cyber Threat Intelligence Integration Center (CTIIC) within DNI. CTIIC serves as “the primary organization within the Federal Government for analyzing and integrating all intelligence possessed or acquired by the United States pertaining to cyber threats.” CTIIC guarantees that appropriate agencies and relevant components of Federal entities have full access to all cyber threat intelligence passed to the Federal Government; as a result, each entity can form an alternate analysis using the information, then compare, collaborate, and combine the varying analyses. CTIIC disseminates the cyber threat analyses to the President, appropriate Congressional committees, and relevant departments and agencies of the Federal Government. Under Title I, CTIIC is responsible for coordinating all cyber threat activities and for strategic cyber intelligence planning for the Federal Government.

H.R. 1560 does not specify the coordination between DNI and DHS. This may be the result of the combination of H.R. 1560 and H.R. 1731; however, a clear reporting structure improves efficiency. Given the capabilities of NCCIC over those of CCIC, a sensible decision would position NCCIC as the interface between Federal and non-Federal entities. NCCIC would filter received information for PII, then pass information to CCIC for dissemination to the intelligence community. CTIIC can focus on analysis of CTI’s and dissemination of information within the intelligence community. This decision also

⁶ The American public favor publically promoted “Whistle-blower” procedures.

⁷ Hash values, certificates, etc.

distances the bill from the public resentment of the intelligence community born from the Snowden and Manning leaks.

If CTIIC receives filtered information from NCCIC, then there is no foreseeable reason that the restriction on passing information to the NSA or DoD could not be removed. The limitations exist predominantly to preclude the use of PII for monitoring purposes. As the CTIIC also filters received information for PII. If the information passes through three filters to remove PII before dissemination then the likelihood of any PII remaining upon dissemination to the intelligence community is miniscule. The powerful research and analysis facilities within the entire intelligence community could greatly help advance United States cybersecurity for organizations and citizens alike.

NCPAA possesses the facilities and scope to act as an intermediary between private-private exchanges. Even if NCPAA does not collect information for the Federal Government from private-private sharing, it could filter the exchanges to anonymize senders and receivers from one another while logging the exchange for accountability purposes. Information could not conceivably be withheld for anti-competition or financial purposes. Information would pass through an additional PII filter; as a result, privacy and civil liberties could be assured with greater confidence.

Effective programs require enough resources to accomplish tasks and build a cultural framework that propagates lasting systematic societal change. CBO estimates that PCNA costs \$186 million over the 2016-2020 period. Likewise, CBO estimates that NCPAA costs \$20 million over the 2016-2020 period. Implementation of both plans averages to ~\$51.5 million annually, which is a meager sum considering that every additional dollar saves thousands of dollars for American businesses and prevents countless breaches from affecting the lives of every citizen in America.

Due to concerns over information gathering and sharing within the intelligence community, CTIIC is limited to a staff of no more than 50 permanent employees. However, under the new structure of H.R. 1560, this limitation is unnecessary because NCPAA is a better-suited interface between the Federal Government and non-Federal entities.

CTIIC and NCPAA serve as the backbone to an overhaul of the entire cybersecurity community. It is imperative that the backbone can support the weight of the responsibilities burdened upon it. Increasing the resources available to CTIIC and NCPAA allow for better dissemination, analysis, and correlation of cybersecurity threat indicators in a federally regulated system. H.R. 1560 is a necessary, long overdue improvement to the American cybersecurity network; as a result, it is important that these programs are implemented efficiently and funded sufficiently to serve their intended purposes.

Inclusion of a Sunset Clause

Both PCNA and NCPAA are voluntary. As such, a balance between public support and organization support must be reached. Businesses dislike sunset clauses because they make long-term investments more risky. The public dislike “eternal” programs because detrimental policies can last for

an unnecessary amount of time. Considering the needs of both user bases, Congress should set the Sunset clause at the lowest possible value to appease the public and make long-term investment viable.

Concluding Remarks:

The Protection Cyber Networks Act of 2015 and the National Cybersecurity Protection Advancement Act of 2015 that form H.R. 1560 make great strides at promoting a culture of cybersecurity consciousness and public accountability in the Federal Government and private sector. H.R. 1560 prioritizes the protection of privacy and civil liberties. The information shared and the cyber threat indicators correlated have the potential to drastically stymie the dire rate of increase of successful cybersecurity breaches. However, H.R. 1560 is not perfect. These two steps forward could use one slight step back to allow for additional considerations that would enable the practical implementation to align with the intent of the bill.

*Expert research contributed by the following ICIT Fellows:

- Drew Spaniel (ICIT Visiting Scholar, Carnegie Mellon University)
- Rob Roy (ICIT Fellow – Federal Chief Technology Officer, U.S. Public Sector, HP)
- Cynthia Cullen (ICIT Fellow - Security Strategist, Northeast, HP)
- Stan Wisseman (ICIT Fellow - Security Strategist, Southeast, HP)
- Chris Schumacher (ICIT Fellow - Sr. Technology Consultant, New Light Technologies)
- Dan Waddell (ICIT Fellow - Director, Government Affairs, (ISC)2)
- Daniel Skinner (ICIT Fellow – Chief Product Officer, Watchdox)
- Danyetta Fleming (ICIT Fellow – President & Founder, Covenant Security Solutions)

Sources:

American Civil Liberties Union:

<https://www.aclu.org/letter/open-government-groups-opposes-hr-1560-protecting-cyber-networks-act>

Business Solutions:

<http://www.bsminfo.com/doc/how-will-cybersecurity-data-sharing-bill-impact-healthcare-it-0001>

Congressional Budget Office:

<https://www.cbo.gov/publication/50110>

CSO Online:

<http://www.csoonline.com/article/2843820/data-protection/cybersecurity-2014-breaches-and-costs-rise-confidence-and-budgets-are-low.html>

Executive Office of the President of the United States: Office of Management and Budget:

https://www.whitehouse.gov/.../saphr1560r_20150421.pdf

Govtrack:

<https://www.govtrack.us/congress/bills/114/hr1731>

<https://www.govtrack.us/congress/bills/114/hr1560>

The Heritage Foundation:

<http://www.heritage.org/research/reports/2014/10/cyber-attacks-on-us-companies-in-2014>

<http://www.heritage.org/research/reports/2015/04/house-cyber-information-sharing-bills-right-approach-but-require-fixes>

House Republicans:

<http://gop.gov/bill/h-r-1560-the-protecting-cyber-networks-act/>

KrebsonSecurity:

<http://krebsonsecurity.com/tag/home-depot-breach/>

<http://krebsonsecurity.com/2013/12/cards-stolen-in-target-breach-flood-underground-markets/>

Official Blog of U.S. Representative Beto O' Rourke (TX):

<https://medium.com/@RepBetoORourke/vote-explanation-for-h-r-1560-c740276da188>

Open Technology Institute:

<https://www.newamerica.org/oti/coalition-letter-from-55-civil-society-groups-security-experts-and-academics-opposing-pcna/>

U.S. House of Representatives Permanent Select Committee on Intelligence:

<http://intelligence.house.gov/ProtectingCyberNetworksAct>

The Week in Congress:

<http://theweekincongress.com/2015/04/23/h-r-1560-protecting-cyber-networks-act/>