

**Congress of the United States**  
**U.S. House of Representatives**  
**Committee on Small Business**  
2361 Rayburn House Office Building  
Washington, DC 20515-6315

**Memorandum**

To: Members, Committee on Small Business  
From: Committee Staff  
Date: July 5, 2016  
Re: Hearing: “Foreign Cyber Threats: Small Business, Big Target”

---

On Wednesday, July 6, 2016 at 2:00 p.m. in Room 2360 of the Rayburn House Office Building, the Committee on Small Business will hold a hearing to examine the impending cyber threat posed by foreign firms on small businesses. Information technology provides small businesses with the necessary tools to be competitive in the global economy. However, as small businesses increasingly rely on foreign technology products and services, they face an even greater threat from cyber attacks. As the Committee has learned through previous hearings, even a simple cyber attack can destroy a small business. Unfortunately, some foreign telecommunications firms are taking steps to develop an unbreakable link to American companies and markets, making small businesses a top target. These foreign firms strive to become highly integrated with American firms in order to evade the consequences associated with ignoring U.S. sanctions on rogue regimes. Not only does this pose a significant risk to our national security, but it also creates real concerns for the safety and sustainability of America’s small businesses – firms that are often ill-equipped to combat against cyber attacks and properly identify looming foreign threats.

**I. Background**

The Internet is altering small business operations and establishing a highly competitive marketplace in the 21st century. Advanced telecommunications technology provides a number of tools to help small firms increase their productivity, efficiency, and overall success. These tools include social media, mobile services, cloud data storage, and global video conferencing. However, the movement of information from paper to digital has resulted in greater opportunities for criminals and foreign threats. The risk of theft and manipulation of sensitive and valuable information has increased significantly. These events are referred to as cyber attacks.

Cyber attacks are a major threat to both the United States’ national security and economy. The scope and capabilities of cyber attackers can vary immensely; they are viewed today as “mainly individual hackers with purely malicious intent, or perhaps criminal groups intending to use

information networks for profit seeking.”<sup>1</sup> However, “actors with political or ideological agendas—including terrorist groups, rogue countries and even big powers such as China and Russia—will also pursue cyber power and will play roles of growing importance.”<sup>2</sup> Moreover, foreign governments – through subversive tactics – employ state-backed firms to implement and accomplish cyber attacks, cyber espionage, as well as accomplish other national strategic objectives, making it difficult to identify the responsible entity.<sup>3</sup> The outcome of an attack can be catastrophic for small business owners because many firms are unable to recover from the loss of their intellectual property and resources. In addition, small businesses generally have less capital to purchase computer security hardware and software, fewer staff members to monitor their systems, and less time to develop cyber security defense strategies.

In recent years, foreign-backed telecommunications firms<sup>4</sup> have reassessed their strategies to expose weaknesses in the United States’ information technology infrastructure, spurring interest among policymakers to investigate looming threats and develop methods to protect digital infrastructure and individuals’ information. This hearing will provide Committee Members with the opportunity to learn more about foreign-backed telecommunications firms and the increased threat and complexity of cyber attacks on small businesses.

## **II. Growth of the Internet and Information Technology (IT)**

Like a chain, the Internet is comprised of technology links that are dependent upon each other to function. Components include, but are not limited to, Internet service providers (ISP), website or application hosts, data storage facilities, and end users. The development and adoption of these technologies and the Internet continue to grow at a rapid pace. In a recent study, Cisco Systems stated that global Internet traffic has increased more than five-fold in the past five years and will increase three-fold over the next five years.<sup>5</sup>

The Internet is also of growing importance for small businesses because it provides opportunities for small businesses to utilize a variety of tools to increase productivity, reduce costs, increase sales, and increase overall efficiency. This is demonstrated by its ability to give small business access to global markets in a cost effective manner. According to the latest data, electronic commerce in the United States, also known as online sales, reached \$340.8 billion in 2015,<sup>6</sup>

---

<sup>1</sup> Richard Krugler, *Deterrence of Cyber Attacks* 5, in CYBERPOWER AND NATIONAL SECURITY (Franklin D. Kramer, Stuart H. Starr & Larry Wentz eds. 2009), available at <http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-13.pdf>.

<sup>2</sup> *Id.*

<sup>3</sup> As the U.S.-China Commission has highlighted, circumstantial evidence suggests that cyber incidents are state sponsored because the actors typically target key defense and foreign-policy sources, which are more useful to state and not commercial operations. U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION, 2015 ANNUAL REPORT TO CONGRESS 192 (2015), available at [http://www.uscc.gov/Annual\\_Reports/2015-annual-report-congress](http://www.uscc.gov/Annual_Reports/2015-annual-report-congress).

<sup>4</sup> *Id.*

<sup>5</sup> [http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white\\_paper\\_c11-481360.html](http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.html).

<sup>6</sup> BUREAU OF THE CENSUS, U.S. CENSUS BUREAU NEWS (FEB 2016), available at [https://www.census.gov/retail/mrts/www/data/pdf/ec\\_current.pdf](https://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf).

which represents a nearly 6855 percent increase from \$4.9 billion registered in 1998.<sup>7</sup> The Internet also has generated an entrepreneurship boom of businesses developing innovative technologies and new capabilities, such as cloud computing and mobile applications.

### **A. Cloud Computing**

The term “cloud computing” is defined by the National Institute of Standards and Technology (NIST) as “a model for enabling ubiquitous, convenient, on-demand access to a shared pool of configurable computing resources (including networks, servers, storage, applications, and services) that can be rapidly released with minimal effort or interaction from the service provider.”<sup>8</sup> For small businesses, cloud computing provides an opportunity to shift many of their information technology services (such as data storage, software, and security) to a cloud provider, instead of purchasing and managing the necessary IT on-site. Nearly 80 percent of United States small businesses will be fully adapted to cloud computing by 2020, more than doubling the current 37 percent rate.<sup>9</sup> However, the centralization of sensitive information to cloud computing data warehouses has made them a growing target for cyber attacks.

### **B. Mobile Applications**

The rapid growth of wireless smartphones and tablets has led to the innovation of mobile software applications. Mobile applications allow businesses and consumers to share information and communicate by a touch of a button. Smart phone and tablet manufacturers have reported that there are over 3 billion different applications available to be downloaded on their mobile devices.<sup>10</sup> There are a variety of mobile applications that increase productivity and efficiency of small businesses, including mobile banking and social media.<sup>11</sup> Mobile applications could be another avenue for potential cyber hackers to steal information.<sup>12</sup>

Given the evident benefits, it is not surprising that small businesses have reported an increase in utilization of technology, and, specifically, newer technology platforms such as cloud computing, smart phones, tablets, and high-speed internet options.<sup>13</sup> Additionally, the continued

---

<sup>7</sup> BUREAU OF THE CENSUS, MEASURING THE ELECTRONIC ECONOMY TABLE 5 (2010), available at <http://www.census.gov/econ/estats/2010/all2010tables.html>.

<sup>8</sup> NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, THE NIST DEFINITION OF CLOUD COMPUTING 2 (2011), available at <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>.

<sup>9</sup> <http://www.intuit.com/company/press-room/press-releases/2014/IntuitStudyShowsHowtheCloudWillTransformSmallBusinessby2020/>.

<sup>10</sup> *Modern Tools in a Modern World: How App Technology is Benefitting Small Businesses*, 114<sup>th</sup> Cong. (2015) (statement of Morgan Reed at 2, Executive Director, ACT | The App Association), available at [http://smbiz.house.gov/uploadedfiles/7-23-2015\\_morgan\\_reed\\_written\\_testimony.pdf](http://smbiz.house.gov/uploadedfiles/7-23-2015_morgan_reed_written_testimony.pdf).

<sup>11</sup> For example, mobile banking applications allow small businesses to expedite the processing of payments between customers, vendors, and financial institutions from a mobile device. Social media mobile applications, like Facebook and Twitter, provide an online platform for small businesses to communicate their marketing and branding messages from mobile phones and tablets to consumers who also have such devices.

<sup>12</sup> MCAFEE, 2015 THREATS PREDICTION (2015), available at <http://www.mcafee.com/us/security-awareness/articles/mcafee-labs-threats-predictions-2015.aspx>.

<sup>13</sup> NATIONAL SMALL BUSINESS ASSOCIATION, 2013 SMALL BUSINESS TECHNOLOGY SURVEY 6 (2013), available at <http://www.nsba.biz/wp-content/uploads/2013/09/Technology-Survey-2013.pdf>.

movement of information and commerce to the Internet has resulted in greater global market integrations and further interdependencies.<sup>14</sup>

### III. Foreign Attacks by State-Backed Firms and Implications for Small Business

Targeted cyber attacks are steadily increasing in the United States. As a global leader in producing intellectual property, America's private and public institutions will continue to be primary targets for cyber criminals. The Internet Crime Complaint Center within the United States Department of Justice recorded 269,422 cyber security related complaints in its 2014 report.<sup>15</sup> This is an increase of over 1500 percent from the year 2000 (16,838 reported complaints).<sup>16</sup> Some of the key targets include the nation's critical infrastructure,<sup>17</sup> federal and state governments, and private businesses. According to a report by Verizon Enterprise, 71 percent of cyber attacks occurred in businesses with fewer than 100 employees.<sup>18</sup>

The methods to steal information vary in scope and sophistication. The most common forms of attacks include hacking,<sup>19</sup> malware,<sup>20</sup> physical error, and lost or stolen devices.<sup>21</sup> Moreover, the expansion of global communications technology leaves United States businesses exceptionally vulnerable to cyber threats associated with integrated dependencies, particularly those resulting from foreign sourced telecommunications supply chains used for national security applications.<sup>22</sup>

The Government Accountability Office (GAO) notes in a 2012 report that the Federal Bureau of Investigation (FBI) has determined that foreign state actors pose a serious cyber threat to the telecommunications supply chain.<sup>23</sup> It is also clear that many foreign nations are responsible for direct cyber attacks on the United States in an effort to gain intellectual property and economic information. The Office of the National Counter Intelligence Executive released a report on

---

<sup>14</sup> Steven M. Rinaldi, James P. Peerenboom, and Terrence K. Kelly, "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies," *IEEE Control Systems Magazine*, December 2001.

<sup>15</sup> INTERNET CRIME COMPLAINT CENTER, 2014 INTERNET CRIME REPORT 6, *available at* [http://www.ic3.gov/media/annualreport/2014\\_IC3Report.pdf](http://www.ic3.gov/media/annualreport/2014_IC3Report.pdf).

<sup>16</sup> *Id.*

<sup>17</sup> The term "critical infrastructure" is defined as "those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private." Presidential Decision Directive No. 63 at PDD-63 (1998), *reprinted in* National Telecommunications and Information Administration, Notice, 63 Fed. Reg. 41,804 (Aug. 5, 1998).

<sup>18</sup> VERIZON, 2012 DATA BREACH INVESTIGATIONS REPORT at 9 [hereinafter Verizon], *available at* [http://www.verizonenterprise.com/resources/reports/rp\\_data-breach-investigations-report-2012-ebk\\_en\\_xg.pdf](http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf).

<sup>19</sup> Hacking is generally referred to as the act of an unauthorized user attempting to or gaining access to an information system. <http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf>.

<sup>20</sup> Malware is generally referred to as software that compromises the operation of a system by performing an unauthorized function or process, <http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf>.

<sup>21</sup> Verizon, *supra* note 18, at 12-13.

<sup>22</sup> PERMANENT SELECT COMMITTEE ON INTELLIGENCE, INVESTIGATIVE REPORT ON THE U.S. NATIONAL SECURITY ISSUES POSED BY CHINESE TELECOMMUNICATIONS COMPANIES HUAWAI AND ZTE 1 (2012), [hereinafter Intelligence Committee Report] *available at* <https://intelligence.house.gov/press-release/investigative-report-us-national-security-issues-posed-chinese-telecommunications>.

<sup>23</sup> GOVERNMENT ACCOUNTABILITY OFFICE (GAO), IT SUPPLY CHAIN, NATIONAL SECURITY RELATED AGENCIES NEED TO BETTER ADDRESS RISKS 11 (2012) (GAO-12-361), *available at* <http://www.gao.gov/assets/590/589568.pdf>.

October 11, 2011 stating that tens of billions of dollars in trade secrets, intellectual property, and technology are being stolen each year from computer systems in the federal government, corporations, and academic institutions. They identified China and Russia as the two largest participants in cyber espionage.<sup>24</sup>

In a report by the House Permanent Select Committee on Intelligence (HPSCI), United States businesses and cyber security experts reported persistent network disturbances that were traced back to China and were thought to be supported by the Chinese government.<sup>25</sup> The same report noted that some services and private companies display their cyber capabilities through a supply of telecommunications components and systems marketed directly to United States businesses and entities.<sup>26</sup> Furthermore, a Department of Defense (DOD) study states that when safeguarding against and assessing threats posed by nation-state actors “means and opportunity are present throughout the supply chain and lifecycle of software development.”<sup>27</sup> This is particularly troublesome for small businesses that, not only rely on products from, but also engage in commerce with, globalized telecommunications firms from countries like China.

Vulnerabilities in the information technology supply chain are especially at risk because foreign telecommunications firms are capable of exploiting these weaknesses to carry out criminal activities. For example, in documents made public by the Bureau of Industry and Security (BIS),<sup>28</sup> China based ZTE Corporation outlines the risks associated with doing business in sanctioned countries and provides a model, as well as advocates for the use of shell companies to subvert United States export control laws. In fact, the document states explicitly that “[t]he biggest advantage of [this model] is that it is more effective, [because it’s] harder for the U.S. Government to trace it or investigate the real flow of the controlled commodities.”<sup>29</sup> The document also notes that “once our company violates the relevant U.S. export control provisions, [the U.S. Government] might carry out civil and criminal punishments against U.S. suppliers, which will lead to increased difficulty for our company to obtain the relevant U.S. technologies and components later.”<sup>30</sup> Many of the American companies that provide component parts to ZTE are small businesses.

#### **IV. Federal Government’s Response to Foreign Cyber Threats**

Since President Clinton’s 1998 directive (PDD-63), the federal government has taken an increasingly active role in protecting critical infrastructure and preventing cyber attacks. The most recent efforts are encapsulated in the Department of Homeland Security’s (DHS) National

---

<sup>24</sup> OFFICE OF NATIONAL COUNTER INTELLIGENCE EXECUTIVE, FOREIGN SPIES STEALING US ECONOMIC SECRETS IN CYBERSPACE 4 (2011), *available at* [http://www.ncix.gov/publications/reports/fecie\\_all/Foreign\\_Economic\\_Collection\\_2011.pdf](http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf).

<sup>25</sup> Intelligence Committee Report.

<sup>26</sup> *Id.* at 2, 3.

<sup>27</sup> DOD, REPORT OF THE DEFENSE SCIENCE BOARD TASK FORCE ON MISSION IMPACT OF FOREIGN INFLUENCE ON DOD SOFTWARE VIII (2007), *available at* <http://www.acq.osd.mil/dsb/reports/ADA486949.pdf>.

<sup>28</sup> <https://www.bis.doc.gov/index.php/about-bis/newsroom>.

<sup>29</sup> [https://www.bis.doc.gov/index.php/forms-documents/doc\\_download/1436-proposal-for-english](https://www.bis.doc.gov/index.php/forms-documents/doc_download/1436-proposal-for-english).

<sup>30</sup> *Id.*

Infrastructure Protection Plan (NIPP).<sup>31</sup> In addition to the NIPP, other divisions within DHS, particularly the Office of Cybersecurity and Communications (CSC)<sup>32</sup> and the United States Computer Emergency Readiness Team<sup>33</sup> are tasked with protecting the nation's IT and coordinating these efforts with states, local governments, and private entities.

On February 12, 2013, President Obama issued an Executive Order aimed at improving the critical infrastructure's security against possible cyber attacks.<sup>34</sup> The order established DHS as having a lead role in cyber security<sup>35</sup> and encouraged the federal government to increase their information sharing with the private-sector entities.<sup>36</sup> The order also directed NIST to develop the framework to reduce cyber risks to the critical infrastructure, including working with the private sector to develop industry standards and best practices.<sup>37</sup> The NIST Cybersecurity Framework Version 1.0 was released on February 12, 2014.<sup>38</sup> NIST held a Cybersecurity Framework Workshop in April 2016 to develop future versions of the Cybersecurity Framework.

However, federal agencies tasked with protecting and supporting small businesses are at risk. An October 2014 investigation conducted by the Small Business Administration (SBA) Office of the Inspector General (OIG) found that the SBA is challenged by long-standing security weaknesses identified in 35 open information technology audit recommendations.<sup>39</sup> Specifically, "the SBA's system software controls have 6 open recommendations averaging more than 700 days past their original target corrective action date."<sup>40</sup> The OIG observed that the SBA continues to face significant security vulnerabilities, including establishing baseline configurations of the SBA's IT platforms.<sup>41</sup>

Moreover, in January 2016, the GAO testified before the Committee on Small Business that "contrary to OMB guidance SBA has not conducted regular reviews of its operational IT investments to ensure that they continue to meet agency needs."<sup>42</sup> GAO also noted that the SBA is currently unable to confirm that its IT investments are cost-effective, meeting agency goals or are being effectively managed.<sup>43</sup>

---

<sup>31</sup> DHS, NATIONAL INFRASTRUCTURE PROTECTION PLAN 15-16 (2009), *available at* [http://www.dhs.gov/xlibrary/assets/NIPP\\_Plan.pdf](http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf). The plan was originally issued in 2006 and revised in 2009.

<sup>32</sup> [http://www.dhs.gov/xabout/structure/editorial\\_0794.shtm](http://www.dhs.gov/xabout/structure/editorial_0794.shtm).

<sup>33</sup> <http://www.us-cert.gov/about-us>.

<sup>34</sup> Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 19, 2013).

<sup>35</sup> *Id.* at § 4, 78 Fed. Reg. at 11,739.

<sup>36</sup> *Id.* at § 4(e), 78 Fed. Reg. at 11,740.

<sup>37</sup> *Id.* at § 7, 78 Fed. Reg. at 11,740-41.

<sup>38</sup> NIST, CYBERSECURITY FRAMEWORK VERSION 1.0 (2012), *available at* <http://www.nist.gov/cyberframework/>.

<sup>39</sup> SBA, REPORT ON THE MOST SERIOUS MANAGEMENT AND PERFORMANCE CHALLENGES FACING THE SMALL BUSINESS ADMINISTRATION IN FISCAL YEAR 2015 2 (2014) (REPORT NUMBER 15-01), *available at* [https://www.sba.gov/sites/default/files/oig/SBA%20OIG%20Report%2015-01%20-%20FY%202015%20Management%20Challenges\\_0.pdf](https://www.sba.gov/sites/default/files/oig/SBA%20OIG%20Report%2015-01%20-%20FY%202015%20Management%20Challenges_0.pdf).

<sup>40</sup> *Id.*

<sup>41</sup> *Id.*

<sup>42</sup> *Attention Needed: Mismanagement at the SBA – The GAO Findings: Hearing Before the H. Comm. On Small Business*, 114<sup>th</sup> Cong. (2016) (statement of William B. Shear, Director, Financial Markets and Community Investment, United States Government Accountability Office), *available at* [http://smbiz.house.gov/uploadedfiles/1-06-2016\\_shear\\_testimony.pdf](http://smbiz.house.gov/uploadedfiles/1-06-2016_shear_testimony.pdf).

<sup>43</sup> *Id.*

## V. Key Issues and Best Practices for Small Businesses

The government efforts to counter cyber attacks are vital to protect critical infrastructure. However, government sharing of information still requires implementation activities by the private sector. Small businesses generally have fewer resources available to combat security threats, which make them an easy target for cyber criminals. In a recent survey, 81 percent of small businesses are concerned about a cyber attack; 63 percent have cyber security measures in place; and 71 percent of small businesses received a phishing email.<sup>44</sup> To help small businesses be better prepared, the Federal Communications Commission (FCC) launched the *Small Biz Cyber Planner* – an online tool to help small businesses create a customized plan to guide against cyber threats.<sup>45</sup>

Protective activities (such as those offered by the FCC) are particularly important to small business; even one cyber attack could be disastrous for a small business. In a 2014 survey, the average cost of a cyber attack on a small business was \$32,020.56.<sup>46</sup> Some statistics show that nearly 60 percent of small businesses will close within six months after a cyber attack.<sup>47</sup>

Additionally, NIST has developed InfraGard, a co-sponsorship agreement with the SBA and FBI to conduct regional workshops that focus specifically on IT security for small businesses.<sup>48</sup> The workshops provide small businesses access to IT security personnel to provide advice and education on security threats pose to businesses, as well as how to assess vulnerabilities and identify the necessary protections for such threats.<sup>49</sup> InfraGard also emphasizes the importance of information sharing between the federal government – facilitated through the FBI – and private sector entities.<sup>50</sup>

## VI. Policy Initiatives for the 114th Congress

There is a strong bipartisan commitment from both chambers of Congress and the President to update certain domestic laws related to cyber security. Recent legislative proposals have addressed data security, stronger federal agency coordination, reporting requirements, increased law enforcement and workforce, and education outreach. The most controversial issues involve the appropriate role of the federal government in working with private industry to protect critical infrastructure.

On January 8, 2015, House Intelligence Committee Ranking Member C.A. Dutch Ruppertsberger introduced H.R. 234, the Cyber Intelligence and Sharing Protection Act.<sup>51</sup> This legislation would allow the federal government to provide classified cyber threat information to the private

---

<sup>44</sup> <http://www.nationalcybersecurityinstitute.org/small-business/business-cybersecurity-statistics/>.

<sup>45</sup> <http://www.fcc.gov/document/genachowski-small-biz-cyber-planner>.

<sup>46</sup> NSBA, 2015 YEAR-END ECONOMIC REPORT, available at <http://www.nsba.biz/wp-content/uploads/2016/02/Year-End-Economic-Report-2015.pdf>.

<sup>47</sup> <http://www.businessinsider.com/the-challenges-in-defending-against-malware-2011-9>.

<sup>48</sup> <http://csrc.nist.gov/groups/SMA/sbc/overview.html>.

<sup>49</sup> *Id.*

<sup>50</sup> *Id.*

<sup>51</sup> H.R. 234, 114th Cong., 1st Sess. (2015).

sector to better protect against a possible cyber attack.<sup>52</sup> H.R. 234 also provides liability protection against companies acting in good faith to protect their network.<sup>53</sup>

On April 13, 2015 House Homeland Security Committee Chairman Michael McCaul introduced the National Cybersecurity Protection Advancement Act of 2015.<sup>54</sup> This legislation seeks to strengthen the National Cybersecurity and Communications Integration Center's role as the lead civilian interface for the sharing of cyber security risks and incidents.<sup>55</sup> It also aims to preserve existing public-private partnerships to ensure ongoing collaboration on cyber security.<sup>56</sup> The National Cybersecurity Protection Advancement Act of 2015 passed the House on April 23, 2015.<sup>57</sup> It is awaiting action in the Senate.

## **VII. Conclusion**

The Internet and new technology are a key component for small businesses to compete in the 21st century. However, the movement of information and commerce to the Internet has provided a new opportunity for bad actors, both foreign and domestic to steal sensitive and valuable information from small businesses, as well as exploit vulnerabilities in the global supply chain to engage in criminal activities. Unlike large corporations, small businesses do not have the resources and capabilities to mitigate against nation-state coercions. Cyber security must be made a priority for small businesses, as well as the federal agencies that work with them. There must also be a balance between the imposition of overly onerous burdens on small business and the need to protect America's IT from foreign cyber threats.

---

<sup>52</sup> *Id.* at § 1104.

<sup>53</sup> *Id.* at § 1104(b)(4).

<sup>54</sup> <http://homeland.house.gov/press-release/mccaul-ratcliffe-introduce-pro-privacy-pro-security-cybersecurity-bill-committee>.

<sup>55</sup> *Id.*

<sup>56</sup> *Id.*

<sup>57</sup> H.R. 1731, 114th Cong., 1st Sess. (2015).