

collectively gathered information to block attacks before they reach their target. Information collected by the center would need to have sensitive personally identifiable information from Americans removed and sanitized before it could be shared back to the government. It should be clear to all participants how information will be shared and for what purpose. The entity should also employ a privacy board to periodically audit information transmitted to the government to ensure that privacy standards are consistently upheld.

- We have been encouraged with the model of the Defense Industrial Base (DIB) pilot program where DIB companies, ISPs, and the government share information, including classified information, with one another to improve operational security among the participants, much like the model described above. This new entity should utilize lessons from this successful sharing of specific and actionable classified information.
- In order to utilize private sector and government information, this new active defense entity should coordinate with existing information sharing structures such as the Information Sharing and Analysis Centers (ISACs), the National Cybersecurity and Communications Integration Center (NCCIC), the Information Sharing Environment (ISE), and the United States Computer Emergency Readiness Team (US-CERT).
- For this entity to operate effectively, Congress must amend certain laws and provide narrowly targeted exceptions to allow carriers to share cybersecurity related information in order to protect themselves, their customers, and the government. An antitrust exemption might also be required.
- For those private sector entities that voluntarily participate in this new entity, Congress should provide some level of liability protection from lawsuits that result from an action to address malicious activity based upon information received as a member of the entity. Participation in the active defense entity would also limit participant liability in the case of a penetration of their system that resulted in a financial loss they reported in their required financial statements.

Legal Protections for Sharing Information

Liability concerns have also been a common roadblock for information sharing within existing structures. **We believe that information sharing within existing structures can be improved though limited safe harbors when private sector entities voluntarily disclose threat, vulnerability, or incident information to the federal government or ask for advice or assistance to help increase protections on their own systems.** These protections would need to address concerns about antitrust issues, liability, an exemption from the Freedom of Information Act (FOIA), protection from public disclosure, protection from regulatory use by government, and whether or not a private entity is operating as an agent of the government. However, the protection of personal privacy should be at the forefront of any limited legal protection proposal.

Awareness Campaign

Some estimate that 85% of the threat to our information networks can be eliminated with proper cybersecurity hygiene. Increasing the awareness of individual users will help them to protect their own information as well as to reduce the number of access points cyber criminals can use to gain access to businesses.

The first step is to educate Members of Congress. In addition to having a better understanding of the urgency of this issue, Members need to be equipped to help educate businesses and individuals within their districts. Members could also be involved in public service announcements (PSAs) about cybersecurity and good computer hygiene.

Stopthinkconnect.com is a cyber awareness campaign developed with the help of numerous private corporations, the Department of Homeland Security, and other agencies. The government should explore ways to promote cybersecurity hygiene awareness as well as support state and local efforts, through television, the Internet, and printed publications. The government should leverage the messaging talents of the Ad Council and private-sector businesses and target different age groups with similar but segmented messages on cybersecurity risks, consequences, and best practices.

Congress should also work with federal agencies to create a feedback process for this awareness campaign to measure its overall effectiveness (leveraging expertise from other government agencies, like the Broadcasting Board of Governors, Radio Free Europe/Radio Liberty, or the Undersecretary of Defense for Policy, which all have experience with this type of program assessment).

Data Breach

For many companies, the normal operation of business requires the collection and use of sensitive personally identifiable information. When this information is stolen, individuals are exposed to theft and identity loss. This threat is even greater when individuals are unaware their information has been compromised. Nearly every state has implemented its own data breach law that, at times, can make it difficult for businesses to be in compliance. Congress should address data breach notification legislation that simplifies compliance for businesses and protects the sensitive personally identifiable information of individuals.

A host of laws have not been updated to reflect changes in technology. A serious effort should be made to do so. Some updates are necessary to make progress in cybersecurity. Others are needed just to make the law relevant to today's environment. Some will be more controversial than others.

The Cybersecurity Review conducted by the Obama White House in early 2009 identified a number of laws that are in need of an update. The May 2011 White House proposal suggests updates to laws related to law enforcement and federal information sharing as well as criminal penalties and the location of data centers. Portions of these provisions are consistent with our recommendations.

Attached as an appendix are some of the laws that have been suggested to us that should be examined with an eye toward reforms. The most essential laws in need of updating in order to defend the country include:

Federal Information Security Management Act (FISMA) of 2002

FISMA is the main law governing the federal government's information security program. It requires agencies to develop and implement appropriate information security protections according to the risk and degree of harm from unauthorized access.

What needs to change? A main concern with FISMA is that it is inefficient and unable to result in adequate cybersecurity protections. Many believe FISMA has turned into a checklist exercise with a focus on procedure and reporting rather than implementing the best protections. Multiple agencies have been found FISMA compliant even though their security was extremely poor in reality.

Recommendation: FISMA needs to be reformed to focus on secure, continuous, automated monitoring of IT systems rather than the current checklist exercise, which is ineffective. Any update should enable the government to secure its systems now and in the future. Changes in technology, such as cloud or distributed computing, should be contemplated in any update/reform. The federal government needs to lead by example and ensure its own computers and networks are secure. The authorities given to the Department of Homeland Security in two Office of Management and Budget memos, M-10-15 and M-10-28, should be supported and resourced appropriately. This effort of bringing FISMA up to technological date will require multiple committees to work together on appropriate language.

Computer Fraud and Abuse Act (CFAA) of 1986

CFAA governs the unauthorized access to computers used by the federal government, financial institutions, or those used for interstate commerce. The purpose of the act is to reduce hacking of federal and certain other computer systems and includes criminal penalties for violations of the law.

What needs to change? The current definition of protected computers is narrow and applies mainly to those used by the federal government and financial institutions. Federal courts have interpreted the CFAA to include critical infrastructure, but it is not explicitly specified in the statute. Additionally, some courts have interpreted the definitions of “access” and “authorization” in different ways to apply liability without hacking.

Recommendation: The definition of protected computers should be extended to cover critical infrastructures with attached criminal penalties. This definition could also be expanded to cover all private sector computers with differing criminal penalties. The CFAA could also criminalize the creation and distribution of malware. However, while increasing the penalties associated with activities that disrupt or damage protected computers, the CFAA should also be narrowly focused to avoid unintended liability beyond computer hacking.

Communication Laws

There are current laws in place governing the protection of electronic communications that contain certain exemptions for specific activities. Many organizations, including privacy groups, recognize the need for additional and specific flexibility within these laws to allow carriers to share appropriate cybersecurity related information, to protect themselves, their customers, and the government. In addition, some sort of anonymous reporting mechanism should be developed in order to facilitate a better evaluation of risk for the development of a functioning cyber insurance market. The clearing house described above could act as the repository to assuage privacy concerns. The reporting could be similar to the public health model where the Centers for Disease Control requires the reporting of infectious diseases without sacrificing privacy and corporate concerns.

Criminal Statutes

Congress should review the criminal statutes to ensure that law enforcement has adequate tools, including training in detection and mitigation, to investigate cyber crimes. The federal government should also increase cooperation with local and state prosecutors and judges to enhance the familiarity with appropriate evidentiary regimes for securing and using computer-based evidence in prosecutions. Congress should also change the Racketeer Influenced and Corrupt Organizations (RICO) law to include computer fraud within the definition of racketeering; provide criminal penalties for intentional failures to provide required notices of a security breach involving sensitive personally identifiable information; expand penalties for conspiracies to commit computer fraud and extortion attempts involving threats to access computers without authorization; provide for forfeiture of property used to commit computer fraud; and require restitution for victims of identity theft and computer fraud. Additionally, Congress should conduct a comprehensive examination of crimes involving computers to ensure that penalties are appropriate when compared to similar crimes committed “in person.”

ISSUE 4: LEGAL AUTHORITIES

Cyber challenges our underlying assumptions about warfare and conflict, about jurisdiction and responsibility for dealing with illegal acts, and about the relationship and interaction between government and the private sector.

Updating the legal authorities for our country to act to protect itself is among the most complex issues related to cyber. It is not at all clear what the government's responsibility is, if any, to protect a private business from cyber attack – even if the attacker is believed to be a foreign state. Increasingly, attacks are launched from servers inside the United States because of our relatively strict laws protecting private entities and because of the cumbersome process which government must use to take action against such servers. There are a number of questions that need to be addressed in this area:

1. What is the responsibility and/or authority of the federal government to defend a private business when it is attacked in cyberspace?
 - What if it is a foreign state attacking the business?
 - What if we do not know the source and what level of confidence do we need in attribution in order to take action?
2. How should we use the full range of instruments of national power and influence to discourage bad actors in cyberspace?
 - How do we develop and apply concepts of deterrence?
3. The Intelligence Community collects much information on cyber threats.
 - How do we decide which information to use to defend?
 - How do we share information at network speed?
 - How do we incorporate open source or proprietary information along with classified information to protect our networks?
4. What should the military's role be in relation to other agencies of the federal government- do the military's authorities match up with its role?
5. Apart from when the military is acting pursuant to a congressionally authorized use of force, do sufficient authorities exist to allow for offensive cyber operations necessary to protect our national security?

These are difficult questions. But it is the responsibility of Congress to pursue answers so that the nation can be protected. However, there are some areas where Congress can begin to pursue action with legal authorities.

Classified Security Networks, Information, and Role of Military

The federal government should better define a proactive process for Defense Support of Civil Authorities (DSCA) as they relate to cyber. The Department of Defense can also provide increased support to the broader federal government (as well as state, local, and tribal entities) through better leveraging of technology transition mechanisms and training opportunities.

Civilian Agency and Critical Infrastructure Networks

The federal government should continue to work to secure its own networks ensuring its data is safe and resourced efficiently. As a start, Congress should formalize the Department of Homeland Security's current role in coordinating cybersecurity for federal civilian agencies' computers and networks. As discussed above, Congress should also update the Federal Information Security Management Act (FISMA).

Embargoed until 1:00pm
Wednesday, October 5, 2011

There are many issues that do not necessarily fit within one of the four areas the Task Force was asked to address. Some of them require more time for study. We believe committees should continue to evaluate and advance these issues.

Workforce Development

As we continue to work to increase our cybersecurity protections, the federal government and the private sector alike will have an increasing demand for effective skilled cybersecurity professionals. We should continue to advance educational and awareness initiatives to help meet this demand for the federal workforce, which, in turn, will benefit the private sector as well. Advancing this goal is a good step towards increasing our national security.

Recruitment, Retention, and Training

Congress should also reform the way cybersecurity personnel are recruited, hired, and trained to ensure the federal government has the talent necessary to lead the national cybersecurity effort and protect its own networks. The federal government could do more to leverage institutions designated as National Centers of Academic Excellence in Information Assurance (IA) Education by the National Security Agency and the Department of Homeland Security, including providing expedited hiring authority to graduates of these programs.

The federal government could also provide more guidance to the Centers of Academic Excellence in Research on research needs for the various federal agencies (especially those federal agencies that don't have dedicated research budgets). Congress could also consider emphasizing cybersecurity issues—detection, mitigation, resilience and rehabilitation—as priorities for development of a cadre within the National Defense Executive Reserve. The Task Force also supports revitalizing the Department of Defense's IT Exchange Program (ITEP) and granting the Department of Homeland Security additional hiring and compensation authorities similar to the White House proposal.

Federal Research and Development

Along with private sector innovation, the federal government should continue to look for ways to utilize, leverage, and coordinate its research resources and capabilities to further develop cybersecurity protections. Many departments and agencies, such as the Department of Defense, Department of Energy, Department of Homeland Security, National Science Foundation, National Institute of Standards and Technology and the Defense Advanced Research Projects Agency, can assist with this effort. The government should also have a coordinated plan to ensure that it is not duplicating industry efforts but instead making a unique contribution to safer computing.

International Cooperation and Coordination

Our world has become increasingly interconnected with consumers, businesses, and governments operating in cyberspace. Unfortunately, digital globalization has also increased our risks and made it more difficult to identify and mitigate threats between countries with different laws and different protections. For example, a bad actor can create botnets by using a computer in one country to compromise several computers in another country to carry out malicious activity often in a third country. If the host country refuses to address the bad actor, it makes it difficult for the other country to mitigate the threat of botnets.

Many perpetrators are untraceable, outside the country, or cannot be extradited. Cyber attacks are a borderless activity. The U.S. must take the lead in developing international and universal legal instruments for the prevention and punishment of nefarious cyber activity, similar to the instruments in use against terrorism and narcotics trafficking. Developing international “norms of behavior” should be encouraged.

We should also work through international development organizations to ensure that legal systems in developing countries recognize that cyber crime originating in or occurring within their jurisdiction is a serious crime with international implications, and that their legal systems move toward international standards of treatment and prosecution of such crimes. The U.S. at all levels should continue to stay actively engaged with the international community to address global cybersecurity threats.

The Task Force is also encouraged by the recent actions taken by the U.S. and Australia in adding cyber warfare to our joint defense treaty. The Administration should evaluate adding cyber to all joint defense treaties to reflect the future nature of conflicts. The U.S. should also look at foreign models for cyber defense to determine if there are lessons that might be applied to our own efforts.

Internet Service Provider (ISP) Code of Conduct

Some countries have developed certain codes of conduct that provide best practices for ISPs to apply consistently to their customers to enhance cybersecurity protections. For example, Australia has developed “icode,” a voluntary code of practice, where the country’s ISPs voluntarily agree to notify customers if they have compromised computers and inform users what to do about them. The Task Force encourages the U.S. ISPs to work together to develop an industry-wide voluntary code.

Supply Chain

The increasing vulnerability of the international IT supply chain suggests a legitimate need for enhanced security standards. Any approach must involve international cooperation and heavy engagement with the private sector but should not include language that might put the government in a position to determine the future design and development of technology. Congress should also investigate, perhaps through hearings, whether aspects of the 'Trusted Foundry' approach, or similar approaches, could promote innovation and help ensure domestic production capabilities for some key components.

Much like the law enforcement provisions, the U.S. must work with other governments to establish international security standards in order to prevent hobbling U.S. industry with U.S.-only standards. We are concerned about the impact on U.S. global competitiveness as well as technology innovation and development of having the U.S. government set specific technical standards.

Federal Procurement

The Federal Acquisition Regulations (FAR) and the Defense Federal Acquisition Regulations (DFAR) should be amended to require appropriate security technology, processes, and performance measurement in all government IT procurements. The government should use its buying leverage to create a growing market for higher security. Security technology to be included, as a matter of course, in all government procurements must be developed in conjunction with the private sector to ensure appropriate development of the regulations so that requirements do not limit the ability to use future technology.

APPENDIX

Other Cybersecurity Laws to Consider Updating

Cyber Security Research and Development Act, 2002

National Institute of Standards and Technology Act

- The Science, Space, and Technology Committee has reported H.R. 2096 updating these two laws as they relate to cybersecurity.

High Performance Computing Act of 1991

Federal Power Act

Posse Comitatus Act of 1879

The Communications Act of 1934

State Department Basic Authorities Act of 1968

Federal Advisory Committee Act

The Privacy Act of 1974

Communications Decency Act of 1996

Identity Theft Assumption Deterrence Act of 1998

Identity Theft Penalty Enhancement Act of 2004

The Homeland Security Act of 2002

Terrorism Risk Insurance Act of 2002, as amended

Intelligence Reform and Terrorism Prevention Act of 2004 (IRPTA)

Economic Espionage Act of 1996