Recommendations of the
House Republican
Cybersecurity Task Force

TABLE OF CONTENTS

CYBERSECURITY TASK FORCE MEMBERS

Rep. Robert Aderholt (4th AL)	**Appropriations**
Rep. Jason Chaffetz (3rd UT)	Budget Judiciary **Oversight and Government Reform**
Rep. Mike Coffman (6th CO)	**Armed Services** Natural Resources Small Business
Rep. Bob Goodlatte (6th VA)	Agriculture Education and the Workforce **Judiciary**
Rep. Robert Hurt (5th VA)	**Financial Services**
Rep. Bob Latta (5th OH)	Energy and Commerce
Rep. Dan Lungren (3rd CA)	House Administration, Chairman **Homeland Security** Judiciary
Rep. Michael McCaul (10th TX)	Ethics Foreign Affairs Homeland Security **Science, Space, and Technology**
Rep. Tim Murphy (18th PA)	**Energy and Commerce**
Rep. Steve Stivers (15th OH)	Financial Services
Rep. Lee Terry (2nd NE)	Energy and Commerce
Rep. Mac Thornberry (13th TX)	Armed Services **Permanent Select Committee on Intelligence**

Note: Bold denotes committee designee

INTRODUCTION – WHY CYBER?

Cybersecurity is a complex set of issues involving legal, economic, and national security considerations. In the House, at least nine committees have some significant jurisdictional claim on cyber issues. In May, the White House submitted its legislative language for discussion. The Senate has attempted to construct a comprehensive cyber bill for the last two consecutive congresses.

Given the difficulties, it is reasonable to ask why the House should devote time and energy to an issue that is not at the top of the public's expressed priorities. There are at least three reasons:

1) **Cyber is a major national security issue.** Top government, intelligence, and military leaders often point to cyber as the issue that worries them the most – partly because it touches every aspect of American life (and of military operations) and partly because our laws and policies clearly have not kept up with the rapid changes in technology. Earlier this year, CIA Director Leon Panetta testified about his fear of a "cyber Pearl Harbor."

2) **The threat is real and immediate.** Essentially, every week there are news reports of some company or organization that has had data stolen – from the Department of Defense to, increasingly, small businesses. Most incidents, of course, are never made public. The potential damage, as we will discuss, involves far more than stolen or damaged data.

3) **Cyber is connected to our economy and job creation.** It is not just national security information that is being stolen from databases in the U.S. All kinds of intellectual property are targeted. Information stolen from U.S. databases equals jobs stolen from the U.S. economy. There are many stories of a small business developing a new product, being hacked, and finding copies of its new product flooding the market at cut-rate prices from China within a few months. We must take steps to protect American ideas.

OUR CHARGE

On June 24, 2011, House Republican Leadership formed the House Republican Cybersecurity Task Force. The Task Force was asked to make recommendations to Leadership on how House Republicans should approach four issue areas within cybersecurity:

1) Critical Infrastructure and Incentives
2) Information Sharing and Public-Private Partnerships
3) Updating Existing Cybersecurity Laws
4) Legal Authorities

HOW TO APPROACH CYBER

Based on the charge given to this Task Force, we are recommending a general framework to use in dealing with the four areas we were assigned. Our hope is that this framework can help guide House action for the remainder of this Congress and beyond.

In each of the four areas, we have offered recommendations for the near term that can reasonably be acted upon during this Congress. We have also listed other issues that could be considered or at least advanced. At a minimum, committees should hold hearings on these other issues as they are often no less serious or pressing. Solutions on a portion of those topics may be harder to identify within limited time and resources.

We believe that the current standing committees are in the best position to write the legislation that is consistent with this framework – and even more than with most issues, getting the details exactly right here is very important. Therefore, we assume that the committees will mark-up cyber bills within their jurisdiction, using regular order with active participation by all Members.

At the same time, it has been very helpful for us to have a variety of perspectives brought to the table when discussing this issue. Each of the nine committee representatives and the committees' staffs support these recommendations. But even the limited recommendations we suggest for this Congress will require continuing cooperation among committees.

Legislative packaging and vehicles must, of course, be decided by Leadership, but we are generally skeptical of large, "comprehensive" bills on complex topics, at least as the bills are being written. Individual bills could, of course, be packaged together at some point later in the legislative process.

With the current fiscally constrained environment, any new or expanded programs and initiatives need to reflect fiscal realities. We must keep in mind the potential fiscal impact on both the public and private sectors.

OBSERVATIONS

1. The country is very dependent on computer networks and information infrastructure, and that dependency is growing.

2. The advantage lies with the attacker, and that advantage is growing.

3. Currently, we are very vulnerable to a variety of attacks and exploitations from a variety of actors across the entire spectrum of sophistication.

4. We face a wide range of threats – from vandalism and petty crime to, potentially, cyber warfare and cyber terrorism, but we may not be able to tell which it is at the moment of attack.

5. Most attacks and exploitations can be stopped with 'good hygiene.'

6. Using 'good hygiene' reduces the clutter that more sophisticated actors use to mask their attacks, enabling government and industry to put an increased focus on the more advanced and dangerous threats.

7. Government insights and capabilities, often derived from intelligence collection, can significantly augment the private sector's efforts to defend against more sophisticated threats, which are often, but not always, from state actors.

8. Many malicious cyber attacks are based on U.S. servers because of the legal protection given entities in the U.S.

9. The Stuxnet computer worm represents a new, more sophisticated and more dangerous level of threat. It does more than steal or destroy data. It alters the control systems that affect physical things, like machinery.

10. Threats change and adapt rapidly. Change occurs so fast in this area that attempts to directly regulate a specific cybersecurity solution will be outdated by the time it is written.

11. Most infrastructure is owned by the private sector, and it has a responsibility to protect its networks. Government should also improve its own network security. However, government information can augment the private sector's efforts to defend its own networks, and private sector knowledge and information can significantly assist the defense of the government's networks.

12. There is a cultural challenge of trust and ownership involved in sharing information among government agencies and among private companies. That is even more true when it comes to sharing between government and industry.

ISSUE 1: CRITICAL INFRASTRUCTURE AND INCENTIVES

Critical infrastructures are certain physical assets, functions, and systems that facilitate the production and distribution of our nation's goods and services that we depend on every day, such as power distribution, water supply, and telecommunications. The Department of Homeland Security (DHS) has divided our nation's critical infrastructures and key resources into 18 sectors.

As computer technology has advanced, so has the dependence on computerized industrial control systems to monitor and control equipment that supports modern critical infrastructures. Malicious code that alters these control systems has the potential to inflict serious – even lethal – damage.

Yet, we have been told that the free market alone may not be able to improve security sufficiently. The return on investment may be hard to prove, and businesses will only do what makes sense for the bottom line. We are generally skeptical of direct regulation and of government agencies grading the security of a private company, which is another form of regulation. Threats and practices change so quickly that government-imposed standards cannot keep up. Regulations can add to costs that ultimately come out of consumers' pockets.

Voluntary Incentives

We believe Congress should adopt a menu of voluntary incentives to encourage private companies to improve cybersecurity. Some incentives may have a cost and would have to be offset. Others do not. However, incentives should be largely voluntary, recognizing that most critical infrastructures are privately owned. Many of these incentives could also be utilized by companies that do not own critical infrastructures.

We also have to recognize that different companies and sectors will need different incentives – one size does not fit all. Committees should evaluate incentives that will be effective within their jurisdiction.

Among the incentives for committees to consider are:

- **Standards Tied to Incentives:** Congress should encourage participation in the development of voluntary cybersecurity standards and guidance through non-regulatory agencies, such as the National Institute of Standards and Technology (NIST), to help the private sector improve security. These standards should be developed by a public-private partnership, focus on security best practices, and remain technology-neutral as much as possible. Additionally, the public-private partnership should evaluate which incentives or strategies would increase the adoption of successful security best

practices. An example would include varying degrees of liability protections afforded to companies that voluntarily implement the enhanced security practices.

- **Streamline Information Security Regulations:** Many private sector corporations are subject to more than one regulator for the protection of their data. For example, Sarbanes-Oxley requires companies to certify that their financial systems are appropriately controlled; HIPAA requires control of any personal information regarding health care, similar to the requirement that the Gramm-Leach-Bliley (GLB) Act puts on personal financial information. Congress could require the Administration to coordinate with critical infrastructure sectors to develop strong performance standards that, if a company was found compliant with the new standard, would satisfy the information security/privacy protections of SOX, HIPAA, GLB etc. A company would be encouraged to implement stronger security standards by allowing it to save money and time by avoiding multiple audits from multiple regulators.

- **Existing Tax Credits:** To encourage companies to increase their investment in network security, Congress should consider expanding or extending existing tax credits, such as the R&D tax credit, to apply to cyber investments as an alternative to creating new tax credits.

- **Existing Grant Funding:** Existing grant funding should be evaluated as an alternative to new funds. Congress could also evaluate including minimum cybersecurity protection standards in grant proposals for grantees dealing with issues such as national security, law enforcement, and critical infrastructures as a condition for receiving government funds. These would include general protection standards such as updating computer patches or running anti-virus software that would not be overly burdensome to grant recipients.

- **Insurance:** Congress should study whether the insurance industry can help play a role in increasing the level of cybersecurity of firms that purchase cyber or data breach insurance and whether the cybersecurity insurance market is currently structured in a manner to accomplish that goal.

Targeted and Limited Regulation

There may be instances where additional direct regulation of an industry that is already highly regulated (nuclear power, electricity, chemical plants, water treatment) may be warranted. **Congress should consider carefully targeted directives for limited regulation of particular critical infrastructures to advance the protection of cybersecurity at these facilities using existing regulators.** Any additional regulation should consider the burden on the private sector by requiring agencies to conduct a thorough cost/benefit analysis.

- **Defining Critical Infrastructure:** Nearly every organization is susceptible to a cyber attack. However, it is cost prohibitive to protect everything, and not every asset, even those within critical infrastructures, will have an impact on national security or critical functions. The government should work closely with each sector to identify elements of critical infrastructure that, if damaged or destroyed, could cause great loss of life or significant economic damage impacting our national security. Further, any targeted or limited regulation should only apply to critical functions or facilities rather than entire organizations to ensure that the impact is not overly broad.

- **Private Industry Input:** Industries with identified critical infrastructures should have full and complete participation in the development of cybersecurity standards and best practices. Any standards should be performance-based rather than technology-based to ensure that they are not out-paced by the advancement of technology. Owners and operators know best how to protect their own systems, and it is nearly impossible for the speed of bureaucracy to keep pace with ever changing threats.

- **Liability Protections:** If existing regulators are imposing a jointly developed cybersecurity standard, the company should be granted some level of liability protection for following this standard. To encourage compliance, regulated entities would be granted limited liability protection in the instance of a breach if they meet or exceed mandated standards. Compliance would be determined through oversight of existing regulators.

- **Oversight:** Entities that currently regulate an element of critical infrastructure that has been defined as higher risk should be responsible for oversight. Enforcement of these standards should be incorporated into already established safety or security reviews. Any element of critical infrastructure that has processes or technology that exceed the established standard should be deemed compliant with the standard. The Department of Homeland Security should work with other regulators to help coordinate security standards across sectors and within sectors subject to multiple regulators.

- **Cybersecurity Reporting Requirements:** Congress should investigate the possibility that significant cyber incidents and vulnerabilities could be included in existing mandatory reporting to improve both law enforcement response and protection of critical infrastructure.

Private sector entities control the vast majority of information networks and assets vulnerable to a cyber attack. Consequently, such entities are often in the best position to identify and defend against cyber-related threats. Owners and operators are, and should be, responsible for the protection, response, and recovery of private assets. The government is also responsible for its own assets.

There is widespread agreement that greater sharing of information is needed within industries, among industries, and between government and industry in order to improve cybersecurity and to prevent and respond to rapidly changing threats. For example, through intelligence collection, the federal government has insights and capabilities that many times are classified but would be useful to help defend private companies from cybersecurity attacks.

There are several organizations designed to help facilitate information sharing now, and there is some sharing going on with varying degrees of success. But not nearly enough.

We largely agree with those who believe that a new entity – separate from the federal government but perhaps partially funded by the federal government – is needed to sponsor this sharing to allow for active defense. But whether a new entity is created or an effort is made to invigorate existing structures, changes to the law are required to allow government and industry to share.

Improving Information Sharing and Developing Active Defense Capability

Companies, including Internet Service Providers (ISPs) and security and software vendors, are already conducting active operations to mitigate cybersecurity attacks. However, these are largely done independently according to their individual business interests and priorities. **Congress should facilitate an organization outside of government to act as a clearing house of information and intelligence sharing between the government and critical infrastructure to improve security and disseminate real-time information designed to help target and defeat malicious cyber activity.**

- The purpose of this entity is not to replace or preclude the enhancement of existing sharing structures, but to expand information sharing to detect and mitigate cyber attacks in real time before they reach their target. Many current efforts provide threat and vulnerability information sharing after the attack has occurred. While this information is still very valuable and, in fact, will help mitigate future attacks, the main focus of this privately led facility is to provide real time defense at network speed.

- This entity would operate outside of government. There is substantial and understandable concern with the government monitoring private networks. This entity would provide a place for the federal government to plug in its knowledge of classified threat signatures and combine this information with the knowledge of threats from across the private sector. ISPs and other large network enterprises could use this

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 through 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).

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 competiveness 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.

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