Written Testimony of
Scott Charney
Corporate Vice President, Trustworthy Computing, Microsoft Corporation
Before the
Senate Committee on Homeland Security and Governmental Affairs
Hearing on "Protecting America from Cyber Attacks: the Importance of Information Sharing"

Chairman Johnson, Ranking Member Carper, and members of the Committee, thank you for the opportunity to appear today at this important hearing. My name is Scott Charney, and I am the Corporate Vice President for Trustworthy Computing at Microsoft. I currently serve on the President's National Security Telecommunications Advisory Committee and I previously served as one of the co-chairs for the Center for Strategic and International Studies Commission on Cybersecurity for the 44th Presidency. Prior to joining Microsoft, I was Chief of the Computer Crime and Intellectual Property Section in the Criminal Division of the United States Department of Justice. During my government service, I oversaw every major hacker prosecution in the United States from 1991 to 1999, worked on major legislative initiatives, Chaired the G8 Subgroup on High-Tech Crime, and was Vice Chair of the Organisation for Economic Co-operation and Development's Group of Experts on Security and Privacy. Finally, I should note that I have had the privilege of testifying before Congress about cybersecurity several times.[1]

It is good to see that the committee's first hearing of the 114th Congress focuses on cybersecurity issues generally, and information sharing in particular. I commend this Committee and the members of the Senate for your continuing commitment to addressing one of America's most complex national and economic security challenges. You and your staff are creating a venue for private sector input into deliberations on cybersecurity, which is essential given that the U.S. private sector not only owns and operates most of this country's critical infrastructure, but also creates and provides information technology products and services used by governments, industries and consumers throughout the world.

The invitation to testify noted that the Committee has three primary objectives:

1. Develop an understanding of the scope and size of cybersecurity threats against U.S. businesses;
2. Discuss the role of various cybersecurity legislative and non-legislative proposals, such as improving information sharing and data-breach notification, in mitigating threats and filling gaps in current practices; and
3. Examine what such proposals must include in order to be effective.

[1] Scott Charney Corporate Vice President, Microsoft Corporation's Trustworthy Computing, Testimony before the Senate Committee on Homeland Security and Governmental Affairs Hearing on *Securing America's Future: The Cyber-Security Act of 2012* (February 16, 2012); Scott Charney Corporate Vice President, Microsoft Corporation's Trustworthy Computing "Implementing New Models for Information Age Security," Testimony before the House Committee on Science and Technology Subcommittee on Technology and Innovation Hearing on *Assessing Cybersecurity Activities at NIST and DHS* (June 25, 2009); Scott Charney Corporate Vice President, Microsoft Corporation's Trustworthy Computing "Securing America's Cyber Future: Simplify, Organize and Act," Testimony before the House Committee on Homeland Security Sub-Committee on Emerging Threats, Cybersecurity, and Science and Technology Hearing on *Reviewing the Federal Cybersecurity Mission* (March 10, 2009).

I will address each of these issues in turn.

The Size and Scope of the Cybersecurity Threats Against U.S. Businesses

There is no doubt that cybersecurity is an important issue for America, other nations, the private sector, and individuals. In an effort to better understand and help address the challenges we face, I regularly engage with government leaders from around the world, security-focused colleagues in the IT and Communications Sectors, companies that manage critical infrastructures, and customers of all sizes. From those interactions, I have concluded that cyber-attacks have joined terrorism and weapons of mass destruction as one of the new, asymmetric threats that puts the U.S., its allies, its corporations, and its citizens at risk.

These threats come in two forms. First, there are opportunistic cybercriminals who have discovered that the Internet's attributes – such as global connectivity, anonymous and untraceable communications, and rich targets (e.g., financial information) – make it an ideal place to commit crime. These cybercriminals engage in broad-based attacks, such as sending email spam to millions of users in the hope that some will click on a dangerous link, install malware and/or provide personal information. These cybercriminals do not care who in particular falls prey, as long as some do. It is also worth noting that these attackers do not need to be technically sophisticated; there are many hacker tools that automate the attack process.

The second form of attack is called an "advanced persistent threat" or "APT" although, in many cases, the attack is not advanced, merely persistent. These attackers are willing to work over time, firmly resolved to compromise a particular victim. Often times, the attacker has had access to the victim's system for a long period of time, moving through the organization and placing malware and backdoors throughout. In a very disturbing trend, these attacks – which previously focused on data exfiltration (the theft of data) – have become more destructive. In some cases, data has been erased from thousands of machines and normal operations were particularly hard to restore.

These two different types of threats warrant somewhat different responses. Basic computer hygiene – running the latest version of software, applying updates, running anti-virus, and exercising common sense (e.g., not opening attachments from strangers) – can thwart many opportunistic attacks. To address advanced persistent threats, however, requires much more. In such cases, those responsible for computer security must focus on the entire "prevent, detect, and respond" lifecycle. Even when they do, it is generally recognized that breaches are inevitable because the old adage that "offense beats defense on the Internet" is true. This is because defenders have to secure everything, while attackers have to find only one entry point. That entry point can be through supply chain taint, exploitation of a vulnerability, exploitation of a system misconfiguration, or through social engineering (tricking a user into providing access).

Complicating matters further is that some advanced persistent threats may come from governments, and it is important to appreciate that governments have developed a very complex relationship with the Internet. First, they are large users of information and communications technologies ("ICT"), but their "customers" are "citizens" who may want to find information, file for benefits, pay their taxes, etc. Second, governments are responsible for protecting the Internet as well as the security and privacy of Internet users, and to fulfill that mission, may use its regulatory powers. Third, even though it wants to protect computer security, a government may exploit networks for a number of reasons, including

economic espionage, military espionage, and military operations.[2] Finally, governments often want access to data, in large part to fulfill law enforcement and intelligence missions.

Consistent with these various roles, an increasing numbers of nation states are currently developing both defensive and offensive cyberspace capabilities. Based on internal Microsoft research, we have determined that:

- In the last 6 months, 95 countries have discussed legislative initiatives focused on cybersecurity;
- 42 countries have developed defensive capabilities against cyber-attacks on their networks;
- 18 have developed defensive capabilities, and possibly also have offensive capabilities;
- 13 likely have offensive capabilities that have not been acknowledged, but can be inferred from operational activity; and
- 16 have specifically declared offensive and defensive capabilities.

Attacks by governments pose a particular problem for the private sector, since a government can utilize a range of tactics and capabilities that non-government cybercriminals normally will not. For example, governments are more likely to taint the supply chain, intercept communications, engage in surreptitious physical searches, and/or affirmatively embed spies into private sector organizations of interest. Additionally, deterrents to cyber-attacks, such as arrest and prosecution, are less applicable to government agents pursuing government missions. This is one reason why Microsoft has been promoting cyber norms, as it has become critical that governments (collectively) exercise self-restraint based upon an agreed set of norms.

Finally, it is clear but worth repeating why this threat environment is so problematic: many parts of the world are completely dependent on ICT for every aspect of digital life and work, with new advances in technology creating incredible civic, social, educational, and economic opportunities. Additionally, while all have not yet benefitted from these advances in technology, it is estimated that over the next decade the number of Internet users will more than double to 4.75 billion, connecting more than 91 percent of people in developed countries and nearly 69 percent of those in emerging countries. This will not just be through traditional computing devices and smartphones, but wearables and other devices not yet imagined. As the "Internet of Things" and cloud services are broadly adopted, connectivity and insights from data will yield overwhelmingly positive and beneficial outcomes. The downside of that ubiquitous connectedness is that attacks will have increasingly disruptive effects. In sum, we have a lot to gain from the continued advancement and deployment of ICT, but we must take concrete actions to limit the threats that may undermine these positive outcomes and cause real harm to computer users worldwide. This is of particular concern to Microsoft, as we have hundreds of millions of consumer and commercial customers using over 200 cloud services (such as Office 365, Azure, Outlook, Skype, and Xbox Live) and 1.4 billion people who use Windows in 76 markets worldwide. Our customers demand – and our business depends – on robust computer security and appropriate risk management.

Why Information Sharing Is Important

With global threats, global actors, and global networks, no one organization – public or private – can have full awareness of all the threats, vulnerabilities, and incidents that shed light on what must be managed. There is no doubt that sharing such information can and has protected computer users and increased the effectiveness of the security community's response to an attack. For example, in 2009, the Conficker Working Group came together to share information and develop a coordinated response to the Conficker

[2] *See* Scott Charney, "Governments and APTs: The Need for Norms," *available at* http://aka.ms/rethink2.

worm, which had infected millions of computers around the world. After the working group developed a mitigation strategy, Information Sharing and Analysis Centers ("ISACs") were mobilized, company incident response teams were activated, government responders were engaged, and the media reported as milestones were reached and services were restored. The challenge was addressed, and quickly.

Another example of information sharing that was designed to solve a specific problem can be seen in Microsoft's partnerships with other companies to takedown botnets through civil action, coordinated industry efforts, and with the support of law enforcement in the U.S. and internationally. Working with the Financial Services ISAC, financial services institutions, pharmaceutical companies, and law enforcement, Microsoft has disrupted cyber threats to our customers and increased the risks for criminals. Two particular operations, the Zeus and Citadel botnets, were each responsible for over $500 million in financial fraud. The collective efforts of industry and government freed millions of infected computers from the control of the cybercriminals.

Why is it, then, that after 20 years of discussion and proof of effectiveness, information sharing efforts are viewed as insufficient? The short answer is that while there are success stories, it is often true that those with critical information are unable or unwilling to share it. They may be unable to share it due to law, regulation, or contract, all of which can create binding obligations of secrecy and expose a company to legal risk if information is shared. Even when those restrictions permit sharing pursuant to authorized exceptions, legal risks remain, as parties may disagree on the scope of the exception. There are also non-legal, non-contractual risks; for example, a company that discloses its vulnerabilities may suffer reputational risk, causing both customers and investors to become concerned. It may even suggest to hackers that security is inadequate, encouraging other attacks.

Additionally, even though information sharing may be designed to protect computer users, the misuse of shared information can have the opposite effect. Let me provide a concrete example. For some time, the second Tuesday of each month has been known as "Patch Tuesday:" the day Microsoft releases updates to fix vulnerabilities in products. When these patches are released, others can reverse-engineer the patch, see what was changed, and craft malware. Thus, the Wednesday after Patch Tuesday became known as "Exploit Wednesday." The problem is that large enterprise customers, including governments, cannot deploy patches the moment they are released; these customers must test patches for compatibility with their own network configurations and programs. Thus, these temporarily unpatched customers were vulnerable to new malware created the day after a patch was released.

To address this problem and better protect customers, Microsoft created the Microsoft Active Protections Program ("MAPP"). Under MAPP, we share information on upcoming patches with anti-virus and intrusion detection companies the week before the patch is released. They then write signatures and deploy them to their customers. Thanks to the MAPP program, here is the new sequence of events:

1. Microsoft releases vulnerability information to MAPP partners;
2. MAPP partners write malware signatures and deploy them to their customers;
3. Microsoft releases updates on Patch Tuesday; and
4. Malware is released on Exploit Wednesday, *but customers are already protected even if the update is not yet deployed.*

This is a powerful example of the benefits of information sharing, as MAPP currently has 80 participants worldwide and helps secure 1 billion customers.

Yet that is not the end of the story. Occasionally, we would see vulnerability information released *before* Patch Tuesday; it turns out that a very small number of MAPP partners were inappropriately disclosing our information early, thus allowing malware to be crafted prior to Patch Tuesday. Needless to say, those violating our confidentiality requirements were removed from the program, but this series of events reveals another reason why organizations may be reluctant to share information; it may be disclosed without authorization or otherwise misused.

In addition to the substantive concerns described above, there are at least four operational challenges posed by today's information sharing arrangements. First, most information sharing programs involve organizations in the same industry: banks share information, electric utilities share information, etc. But ICT is horizontal and underpins all of these sectors, thus rendering these sectoral approaches insufficient. Simply put, ICT threats, vulnerabilities, or incidents may affect disparate companies across multiple sectors.

Second, sharing may occur among industry players, from industry to government, and/or from government to industry, and each of these models pose different issues. Companies in the same sector sharing information may worry about antitrust concerns (partially addressed by letters from the Justice Department and the Federal Trade Commission); private organizations sharing with the government may worry about the use of such information for regulatory enforcement or that customers will view such sharing as inappropriate; and the government itself may worry about disclosing sensitive information to non-government personnel.

Third, while sharing may involve indicators of compromise ("IOCs," such as malware signatures) and anonymized data, it may also include personally identifiable information ("PII"), thus raising privacy concerns. While it may be tempting to permit only the sharing of anonymized data, it is impractical for at least two reasons. First, some IOCs may in fact be PII in some parts of the world. For example, when malware steals data and sends it to a particular IP address in a foreign country, looking for other systems sending content to that same IP address is strong evidence of a security breach. Yet, IP addresses are PII in some countries. Additionally, if we hope to deter cyber-attacks through stronger attribution, it is important to identify the attacker, which, in turn, requires analyzing data that often includes PII (e.g., IP addresses, names of account holders).

Fourth, with so many people dependent on ICT and concerned about cybersecurity, it is challenging to define the scope of any disclosures. Many today would say they need threat, vulnerability, and incident information to manage risk but, as we have seen, sharing information poses its own risks.
With all these challenges in mind, we believe there are six core tenets that must guide information sharing arrangements.

Six Tenets to Guide Effective Information Sharing

1. **Information sharing is a tool, not an objective.**

   Information sharing succeeds when it is targeted at solving specific problems and challenges. Put another way, clarity is needed about what should be shared, with whom, and for what purpose. We also need to know how sensitive information will be protected to avoid causing harm or other unintended consequences. Approaches that call for the disclosure of all threat, vulnerability and incident information, regardless of its utility to the recipient or the risks such disclosure creates for the ecosystem, are ill-advised.

2. **Information sharing has clear benefits, but poses risks that must be mitigated.**

   As we have seen, information sharing can help prevent and respond to attacks, but such sharing poses legal, regulatory, contractual, reputational, security, and privacy risks. Any information sharing regime must attempt to reduce these risks wherever possible.

3. **Privacy is a fundamental value, and must be protected when sharing information to maintain the trust of users – individual consumers, enterprises, and governments – globally**.

   Users and governments around the world may have different views about privacy, but they all want assurances that the information they entrust to others is protected properly. As such, government and industry organizations need to be transparent about the policies and processes in place to protect privacy, particularly when information will be shared with and used by others.

4. **Information sharing forums and processes need not follow a single structure or model, and governments should not be the interface for all sharing.**

   Information forums and processes typically reflect several factors, such as the purpose for their establishment, the players involved, the nature of information shared, and the desired outcomes. Because these factors can differ greatly, there is no single model or template for information sharing efforts. Indeed, significant information sharing occurs within the private sector without any involvement of the government, ensuring that millions of customers are protected quickly.

   In the United States, while the Department of Homeland Security and other U.S. government entities play an important role in cybersecurity, they should not be the sole interface or repository for threat, vulnerability and incident data. This approach would limit the flexibility needed to adapt to a rapidly shifting threat environment, particularly when new entities need to be added to information sharing circles quickly.

5. **Government and industry policies on information sharing should take into account international implications.**

   Cyber threats are often international in scope and an attack may have worldwide implications. The U.S. Government must be mindful that many successful U.S.-based ICT businesses are multi-national companies with foreign customers. Domestic rules can discourage foreign markets from embracing U.S. products and lead to reciprocal requirements that could undermine U.S. security. For example, if the U.S. Government required the mandatory disclosure of all threat, vulnerability, and incident information held by a global company, it is likely that other governments would demand the same information. Broad disclosures in so many parts of the world would not improve computer security; to the contrary, it would increase security risks. Similarly, government policies that unnecessarily constrain the private sector's ability to share cybersecurity information across borders will have a negative impact on cybersecurity outcomes, as cyber defenders will be less equipped to address emerging international threats.

6. **Governments should adhere to legal processes for law enforcement and national security requests, and governments should not subvert information sharing to enable or advance law enforcement and national security objectives.**

   In instances where law enforcement and national security agencies require assistance from the private sector, governments should adhere to appropriate legal processes rather than attempting to leverage information sharing forums and processes. Law enforcement and national security requests

are distinct from information sharing, which centers on the *voluntary* sharing of information that enable stronger cyber defense.

Operationalizing Information Sharing to Solve Problems

These tenets can help address operational considerations, which pose their own challenges. An important starting point is to leverage consistent and repeatable processes for sharing information, processes that maximize the benefits and reduce the risks of information sharing. These processes must not only accommodate today's challenges, but scale to address the increasing connectivity across industries and across the globe.

To understand how this can be achieved – and how legislation might help – it is helpful to understand the basics of information sharing. The process generally has five parts: collection, identification, sharing, use, and data handling.

Collection: Organizations collect data from many sources, in part to detect attacks. For example, they may monitor inbound and outbound traffic, attempts to log onto their networks, and logs generated by security products. If a compromise is found – or if a company is alerted to an attack from an outside source – additional collection may then occur. Of course, there are cost implications to broad collection as a company deploys sensors, stores data, and analyzes it. That said, as sensors and storage becomes cheaper – and machine learning permits more data to be analyzed – more attacks may be detected. This may be controversial, however, since collecting haystacks in the hope of finding needles raises privacy concerns.

Identification: Once an anomaly is detected, further analysis must be done to determine that nature of the event and the scope of any compromise. In some cases, the work can be automated; for example, applications can help identify anomalous behavior on networks or identify traffic being sent to a botnet controller. But even with these tools, determining the scope of an intrusion and the damage caused may remain a complex challenge that relies heavily on the expertise of security professionals. This is because tools cannot detect all malicious activity, and not all anomalous behavior is necessary malicious. When security professionals see something, they have to look closely to determine whether it actually indicates that a cyber-attack has taken place or may be underway. This analysis may require outside help if an organization lacks the right security resources.

The products of this phase are typically IOCs, evidence that reveals an intrusion has occurred (e.g., a piece of malware, a log showing that data has been sent to an unexpected IP address). Ultimately, IOCs are the most common type of information that is shared amongst security professionals.

Sharing: In addition to IOCs, parties may also share information on threats, product vulnerabilities, defensive mitigations, best practices, and strategic analysis. In many cases, this sharing begins as an ad hoc collaboration between affected or knowledgeable parties. This may cause individuals to work together even if they have otherwise competitive relationships or little else in common (e.g., they are in different sectors). These collaborative undertakings build trust and, over time, each party expects that the other will work in a consistent and repeatable way that maximizes protection and minimizes harm. Sustaining these ad hoc efforts in a more structured way requires careful consideration of the what, when, how, and why of information sharing. Understanding these building blocks can help develop structures that not only build trust, but also actively support collaboration in reducing cybersecurity risks.

Use: Each type of information has a different use. Some information helps government and private sector entities assess the risk to cybersecurity at a national or an organizational level, including the risk to critical infrastructure. Some information contributes to analyzing cybersecurity in the long term and to creating incentives for better security. Other types of information can be used to detect attacks, identify incidents, and observe those incidents to determine the objectives of the attackers. Some information, such as best practice information, is more directly actionable for improving hardware, software, and services or for making immediate improvements to network defense. Additionally, security information concerning fraud and abuse can be used to protect the identities, defend account compromises, and for general ecosystem hygiene.

Increasingly, vulnerability and mitigation information is seen as useful in helping actors across the different sectors decide how best to assess and manage risk. This trend reflects a growing understanding of the need to develop better analytical capabilities to understand strategic threats and to better anticipate new risks to ICT and the capabilities ICT enables. High-quality strategic information can help to project where the next classes of cyber-threats may come from, identify the motivations of future attackers, and suggest what technologies they may target. Additionally, strategic analysis can help put incidents into a broader context and can drive internal changes, enhancing the ability of any public or private organization to update risk management practices that reduce its exposure to risk.

At the same time, however, those sharing information often remained concerned about unintended or secondary uses of such information. For example, a party sharing vulnerability information with others would not want to see that security weakness serve as the basis of a future marketing campaign. Similarly, if information shared with the government in the name of computer security was then used for regulatory enforcement purposes, the risk associated with sharing increases, which is a disincentive to do so.

Data Handling: Once cybersecurity information is obtained, organizations have to properly manage its classification, handling, and destruction, among other concerns. Data handling is an important consideration for cyber defenders. For many private sector companies, data management may be informed by rules drawn from multiple jurisdictions, which are often not harmonized.

Defining Approaches That Will Work Today and Tomorrow

While the basic steps of information sharing are the same, how the process is and should be used to manage risks naturally varies. Different players have different capabilities to understand and act on cyber threats. The scale and scope of impacts based on those actions also differs. These differences are important because they affect what information industry players want or need from their peers and governments, and how they can use information to protect themselves and others.

Approximately 18 years ago in the U.S., Presidential Decision Directive 63: Protecting America's Critical Infrastructure[3] encouraged the formation of sector-based ISACs with U.S.-based members to improve information security. Microsoft was a founding member of the Information Technology ISAC in 1999. In 2002, the Homeland Security Act created a new category of information protection called Protected

[3] The White House, Fact Sheet: Protecting America's Critical Infrastructures: PDD 63 (May 22, 1998), *available at* http://fas.org/irp/offdocs/pdd-63.htm

Critical Infrastructure Information,[4] or PCII, in an attempt to address industry concerns about sharing with the government and information disclosure (e.g., Freedom of Information Act requests). While both policies sought to encourage voluntary sharing, results have been mixed for a variety of reasons that have been previously discussed, including the fact that not all members of the same community have an equal ability to act on cyber threat information.

There are times, of course, where reporting is mandatory, and Microsoft has long supported a federal breach notification law to eliminate the hodge-podge of state reporting laws that currently exist. But in the dynamic field of computer security, etching in stone what must be reported to whom regardless of whether the information is actionable is the wrong approach. At the same time, however, we need to ensure that those with important information share it with the right party, at the right time, for the right purpose, and with appropriate protections. This can be done both by creating incentives for, and removing disincentives to, such sharing.

As noted above, information sharing has and does work. But it works because the parties see that the benefits (better protection, detection and response) outweigh the risks. History also teaches, however, that information sharing tends to work best when those involved trust each other to respect informal and sometimes formal agreements (e.g., non-disclosure agreements) on information use and disclosure. Occasionally this sharing is ad hoc and unstructured, driven by events that bring participants together in a time of common need. But once that happens, the resulting relationships may form the basis for further, sustained collaboration, collaboration that continues long after the crisis has passed.

In other cases, information sharing arrangements are more formal and based on non-disclosure agreements, legal contracts, or membership agreements. These arrangements establish a clear set of expectations between the participants, including the type of information to be shared, how it can be used, and how the information will be protected – with consequences for those that do not adhere to the agreed upon conditions. As a result, formalized sharing tends to be the most visible form of sharing – including vendor-user relationships one would expect with cybersecurity service providers. Other examples include ISAC and the MAPP program discussed earlier. In a subset of these cases, extremely sensitive information is shared, such as the Department of Homeland Security's Enhanced Cybersecurity Services ("ECS") Program.[5]

Significantly, some of these sharing arrangements are now supported by automated tools with standardized formats, thus allowing machine-to-machine interactions that speed up response times dramatically. For example, malware signatures need not be manually transmitted and entered into detection tools; the entire process can be automated. Microsoft's Interflow is one such tool that allows cybersecurity professionals to exchange threat information using Threat Information eXpression ("STIX") and Trusted Automated eXchange of Indicator Information ("TAXII") to create automated, machine-readable threat and security information that can be shared across industries and groups in near real-time. This approach should help reduce costs and increase the speed of defense by automating processes that are currently performed manually.

[4] 6 U.S.C. § 133 (Section 214 of the Homeland Security Act of 2002).

[5] Department of Homeland Security, Enhanced Security Services, *available at* http://www.dhs.gov/enhanced-cybersecurity-services

How Congress Can Help

The two most important things Congress can do are (1) ensure that the information sharing arrangements that are working effectively are left undisturbed; and (2) encourage additional information sharing by providing protections for shared information and addressing risks posed by information sharing, including privacy risks. As you consider legislating in this area, I would suggest the below key principles to guide you.

1) New legislation should make clear that it is not meant to impact existing information sharing efforts.

2) New legislation should be scoped to cover information that reasonably enables defenders to protect against, detect, or respond to cyber threats (that is, attacks against the confidentiality, integrity and availability of data and systems).

3) New legislation should not impose additional burdens on industry, but rather incentivize sharing by providing greater protections for shared information. More specifically, the legislation should:

   - Not require the mandatory reporting of threat, vulnerability and incident information, except as necessary to provide breach notifications to consumers;
   - Protect threat, vulnerability, and incident information from inappropriate disclosure;
   - Restrict the use of voluntarily shared data, and prohibit secondary uses;
   - Require the data to be anonymized, except in clearly defined cases where such anonymization would undermine the use of that data (e.g., removing the IP addresses of a botnet server would render the data useless);
   - Require the government to seek a court order when seeking to pierce the veil of anonymity;
   - Require the government to share threat, vulnerability, and incident information with a company if that company (1) participates in information sharing and (2) can action the information. To the extent the information is sensitive and/or classified, Congress should direct the government to evaluate whether the information can be declassified or shared in a way that otherwise protects government interests;
   - Grant liability protection for sharing that occurs consistent with the legislation, without undermining contractual obligations between a company sharing information and its customers; and
   - Provide additional liability protections during well-defined government declared emergencies.

Thank you for the opportunity to testify and I look forward to working with the Committee on this effort.