Improving our Nation's Cybersecurity through the Public-Private Partnership

A White Paper

Presented by

March 8, 2011

EXECUTIVE SUMMARY

We live and work in, and are dependent on, a networked world. That is why the Business Software Alliance, the Center for Democracy and Technology, the Internet Security Alliance, TechAmerica, and the U.S. Chamber of Commerce believe that the cybersecurity of our critical infrastructure must be a national priority. However, the complexity and interconnected nature of the Internet, and the ever-evolving and sophisticated threat environment, put cybersecurity beyond the reach of any single entity: to secure our critical infrastructure, companies must work together, government must coordinate its efforts, and industry and government must collaborate.

To that end, many government and industry organizations have made considerable investments over the years to develop a strong public-private partnership. Those investments are paying off: this paper details many of the important cybersecurity achievements that the partnership has delivered.

We think, however, that more can be done. This is why this paper proposes building on this strong track record, by expanding the existing partnership within the framework of the National Infrastructure Protection Plan. Specifically, we make a series of recommendations that build upon the conclusions of President Obama's Cyberspace Policy Review in seven important areas of cybersecurity:

- **Risk Management:**
    - *Standards*: Government and industry should utilize existing international standards and work through consensus bodies to develop and strengthen international standards for cybersecurity.
    - Assessing Risk: Government and industry need to recognize that their risk-management perspectives stem from different roles and responsibilities. Where government demands a higher standard of care, market incentives need to be available to accommodate non-commercial needs for security.
    - Incentives: Government and industry must develop a menu of market incentives to motivate companies to voluntarily upgrade their cybersecurity. The incentives must be powerful enough to affect behavior without being so burdensome as to curtail U.S. investment, innovation, and job creation.
- **Incident Management:** Government should fully establish industry's seat in the integrated watch center and begin evaluation and process for growing industry's presence. Industry should ensure a long-term plan for filling the watch center seats;

and participants should report lessons learned from collaborative exercises as soon as possible and undertake improvement measures on a timely basis.

- **Information Sharing and Privacy:** Government and industry should clearly articulate information needs and how to promote more effective information-sharing to address those needs; information-sharing for cybersecurity purposes should be transparent and should comply with fair information practice principles; government should consider how it can share more classified and sensitive information, particularly the parts of that information that can help the private sector defend its systems; and in consultation with interested parties, including industry and civil liberties organizations, Congress should consider whether narrow adjustments to surveillance laws are needed for cybersecurity purposes.
- **International Engagement**: Industry and government need to engage international organizations and standards - making processes and work together to develop a strategy for engagement, capacity building, and collaboration on issues of global concern.
- **Supply Chain Security**: Government should expand its participation in the international system that develops supply chain security standards and work with industry to identify and disseminate them. Government should then leverage these standards when it acquires technology and take steps to ensure it does not acquire counterfeit technology products.
- **Innovation and Research and Development:** The public-private partnership should be used to create a genuine National Cybersecurity Research and Development Plan with prioritized, national-level objectives and a detailed road map that specifies the respective roles of each partner. The plan and its implementation road map should be regularly reviewed by the partners and adjusted as necessary.
- **Education and Awareness:** The public-private partnership should enhance cybersecurity public awareness and education, and increase the number of cyber-professionals available to both government and business, including through policies that boost the number of science, technology, engineering, and mathematics (STEM) college students graduating each year.

~~~~~~~~~~~~~~

INTRODUCTION: THE PUBLIC-PRIVATE PARTNERSHIP NEEDS TO BE FULLY REALIZED THROUGH MEANINGFUL AND REGULAR COLLABORATION

The security of private-sector and government network infrastructure is a national priority. U.S.-based information networks and critical infrastructures are complex and diverse, and most of them are owned and operated by the private sector. Industry has been working continually to enhance the security and resiliency of these systems and is committed to continuing these efforts through a voluntary partnership with government. Industry players have created and developed new products and services that make up information systems and networks, and they continue to innovate to enhance those products and services for operability, productivity, stability and security.

Given the complexity and interconnected nature of information systems and networks, as well as an ever-evolving and sophisticated threat environment, no one organization or entity can address U.S. national cybersecurity alone. Industry players must work together, government entities must harmonize their approaches to protecting critical infrastructure, and government and industry must work together to address common concerns and build collaborative solutions. The public-private partnership on critical infrastructure protection and cybersecurity has an evolutionary history that has culminated in the partnership structure that government and industry collectively created and utilize today under the National Infrastructure Protection Plan (NIPP).[1]

The current critical infrastructure protection partnership is sound, the framework is widely accepted, and the construct is one in which both government and industry are heavily invested. The current partnership model has accomplished a great deal. However, an effective and sustainable system of cybersecurity requires a fuller implementation of the voluntary industry-government partnership originally described in the NIPP. Abandoning the core tenets of the model in favor of a more government-centric set of mandates would be counterproductive to both our economic and national security. Rather than creating a new mechanism to accommodate the public-private partnership, government and industry need to continue to develop and enhance the existing one. In order to more fully articulate the benefits and continuing needs of the partnership, this report outlines key components of the government-industry interaction in cybersecurity. The key components of the outline derive heavily from the Cyberspace Policy Review (CSPR) and industry priorities, and we examine each for the benefits, successes, and outstanding objectives.

[1] The *National Infrastructure Protection Plan* (NIPP) is available at http://www.dhs.gov/files/programs/editorial_0827.shtm#0

Government and industry sources have documented the substantial progress the current market-oriented process has made. In 2009 President Obama commissioned staff from the National Security Council to conduct an intensive review of our nation's cybersecurity which found that "many technical and network management solutions that would greatly enhance security already exist in the marketplace but are not always used because of cost and complexity."[2]

The marketplace has seen the development of many products and services that provide for greater cybersecurity. Their effectiveness has been affirmed by both government and industry studies that note that a significant number of cyber events could have been prevented or had their effects mitigated by using the standards practices and technologies the marketplace has already created.[3]

The CSPR's finding that cost and complexity, not lack of ability or commitment, are the largest problems in implementing effective cyber solutions has also been confirmed by multiple independent studies. This research shows that although many enterprises are investing heavily in cybersecurity, many others, largely due to the economic downturn, are reducing their cybersecurity investments.[4] As President Obama has noted, "Due to the interconnected nature of the system this lack of uniform implementation of sound security practices both undermines critical infrastructure and makes using traditional regulatory mechanisms difficult to achieve security."[5]

A number of policy and operational accomplishments have already been achieved through the current industry-government partnership. These accomplishments include the development of cybersecurity standards and best practices through the global, multi-stakeholder ecosystem of standard-setting organizations, creation of the Sector Coordinating Councils, Critical Infrastructure Partnership Advisory Council (CIPAC) legal structure, the completion of a National Cyber Incident Response Plan (NCIRP), the successful execution of the Cyber Storm exercises, and several sector risk assessments. There have also been

---

[2] Obama Administration, *Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure* at 31.

[3] Aerospace Industries Association Annual Conference, *Robert Bigman comments on Cyber Security*, Washington, DC in October 2008; U.S. Senate, hearing before the Committee on Judiciary, Subcommittee on Terrorism and Homeland Security, *Testimony of Richard C. Schaffer, Jr. Information Assurance Director of the National Security Agency,* November 17, 2009, http://judiciary.senate.gov/pdf/11-17-09%20Schaeffer%20Testimony.pdf, Verizon, *2010 Data Breach Investigations Report,* http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf; PricewaterhouseCoopers, *The Global State of Information Security*, 2005; Verizon, *2008 Data Breach Investigations Report, http://www.verizonbusiness.com/resources/security/databreachreport.pdf.*

[4] PricewaterhouseCoopers*, The Global State of Information Security*, 2008.
Center for Strategic & International Studies, *In the Crossfire: Critical Infrastructure in the Age of Cyber War*, 2010.

[5] White House, *Remarks by President Obama at White House Meeting on Cyber Security*, July, 2010.

improvements in information-sharing mechanisms, such as Information Sharing and Analysis Centers (ISACs), the National Council of ISACs and other successful sector-specific information-sharing mechanisms, and the launch of the National Cybersecurity and Communications Integration Center (NCCIC), with seats designated for government and industry enabling ongoing coordination, planning and response.

While all these efforts and others make government and industry more coordinated and secure, the partnership has not yet been utilized to implement the economic, technical and operational issues the NIPP calls for. The CSPR confirms this observation:

"The public-private partnership for cybersecurity must evolve to define clearly the nature of the relationship including the roles and responsibilities of each of the partners."[6]

The partnership structure that industry and government collectively created under the NIPP clearly articulates what is required to build this system. Government and industry have the opportunity to work more collaboratively to implement the following agreed upon activities:

"The success of the [public-private] partnership depends on articulating the mutual benefits to government and private sector partners. While articulating the value proposition to the government typically is clear, it is often more difficult to articulate the direct benefits of participation for the private sector…. In assessing the value proposition for the private sector, there is a clear national security and homeland security interest in ensuring the collective protection of the Nation's [critical infrastructure and key resources] (CI/KR). Government can encourage industry to go beyond efforts already justified by their corporate business needs to assist in broad-scale CI/KR protection through activities such as:

- Providing owners and operators timely, analytical, accurate, and useful information…
- Ensuring industry is engaged as early as possible in the development of initiatives and policies related to [the NIPP]
- Articulating to corporate leaders …both the business and national security benefits of investing in security measures that exceed their business case
- Creating an environment that encourages and supports incentives for companies to voluntarily adopt widely accepted, sound security practices
- Providing support for research needed to enhance future CI/KR protection efforts."[7]

[6] Obama Administration, *Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure*, May 2009 at 33.
[7] *National Infrastructure Protection Plan*, 2006 at 9.

In addition to these key activities of the partnership, the following key elements characterize an optimal partnership:

- *Inclusion* – both public and private parties endeavor to include all pertinent participants (providers and users) in the partnership framework;
- *Equality* – both public and private parties have an equal voice and the ability to participate in all phases of the partnership and its component projects from conceptualization to development to implementation;
- *Trust* – the partnership provides for institutional and relationship-based trust mechanisms to foster collaboration and information exchange;
- *Operational Outcomes* – the partnership provides for an on-going collaboration mechanism that fulfills its strategic and planning objectives as well as its operational cooperation goals;
- *Greatest Good* – the partnership strives to develop and meet the strategic and planning objectives that have the most benefit for all parties involved in the partnership and their respective constituents.

Properly constructed and augmented, the public-private partnership model for cybersecurity also has significant privacy and civil liberties advantages over other, more government-directed models. The partnership leaves network monitoring responsibilities for private networks where they belong – with the private sector operators – rather than having governmental agencies monitor those networks. This also promotes transparency so that civil liberties issues that may arise can be more publicly addressed. At the same time, the partnership allows for robust coordination and information sharing between the government and private sector network operators within carefully defined limits, which comports with both legal and constitutional obligations.

There is concern however that new policy initiatives may consider replacing the current model with an alternate system more reliant on government mandates directed at the private sector. This change of direction would both undermine the progress that has been made and hinder efforts to achieve lasting success. Rather, building on the promise and progress articulated by the NIPP and the CSPR would more fully implement the core principles identified above. The following sections of this paper outline how this can be accomplished while also fulfilling the pledge President Obama made upon the release of the Administration's CSPR:

"Let me be very clear: My Administration will not dictate security standards for private companies. On the contrary we will collaborate with industry to find technology solutions that ensure our security and promote prosperity."

President Barack Obama, Release of the Cyberspace Policy Review*, May 29, 2009*

I. RISK MANAGEMENT

Standards

Many cybersecurity standards have been and are continually being established and updated through the transparent consensus processes of standards development organizations (SDO). Many of these processes are international in design and scope, and they routinely include active engagement by multinational corporations and various government entities that participate as developers or users of the technology. The multitude of continually evolving standards is essential because of the widely disparate configurations that are in use, and these configurations are constantly evolving and being updated to support rapid innovation in a dynamic industry. Both industry and government organizations voluntarily adopt the resulting best practices and standards that best fit their unique requirements, based on their roles, business plans, and cultural or regulatory environments. This historic process of standards development is widely embraced is, highly participatory, and maintains high credibility in the global community. Not only does the standards regime facilitate interoperability between systems built by different vendors, it also facilitates competition between vendors that leads to greater choice and lower cost. Moreover, it spurs the development and use of innovative and secure technologies. Implementation of these resulting standards and best practices can also be highly effective in improving cybersecurity.

An effective approach to cybersecurity policy needs to leverage the existing system of standards development rather than replace it with one that has a distinct bias in favor of national or participant interests. We have already seen that attempts to impose nation-specific requirements under the auspices of security are not embraced by the private sector or the civil liberties and human rights communities for both public policy and powerful economic reasons. A government-controlled system of standards development that resides outside the existing global regime will not be accepted. If imposed, it would quickly become a second-tier system without widespread user or technology community adoption, thereby fracturing the global network of networks and weakening its security.

Governments, either through national or international bodies, can serve an important security function by funding independent evaluations of the existing and emerging standards for their security effectiveness and applicability, and by working with industry to develop profiles of existing standards[8], as opposed to creating new standards. Naturally, varying standards formulas will provide differing levels of security and likely at different cost levels.

Recommendation: Government and industry should utilize existing standards and work through consensus bodies to develop and strengthen international standards for cybersecurity.

Assessing Risk

A general consensus has emerged that the most effective path to cybersecurity is a risk-based approach that encompasses an assessment of threats, vulnerabilities, and consequences. As suggested in the NIPP, government partners and industry players often assess risk differently, based on their differing missions and objectives. Typically, private sector entities assess risk in terms of the economic consequences. Because the economic consequences of some cybersecurity failures can be quite high, including the loss of intellectual property that is expensive to develop, the damage inflicted to the brand of the affected company, or the erosion of trust in an unstable system that is critical to its success, cybersecurity expenditures that are made to avoid these failures are also quite high.

The risk analysis drives relatively high investment in cybersecurity measures by many, but not all, enterprises. A comparatively higher tolerance for risk may exist if the cost of security is more than the perceived or anticipated loss.

Risks to the nation vary widely, and neither government nor the private sector can afford to protect everything against all risks, be they physical or cyber. Managing these risks is particularly difficult in an environment of limited resources and security interdependence. When evaluating risk, the interests of both industry and government need to be considered, including decisions that require trade-offs.[9]

Corporate and governmental risk management calculations can often lead to different decisions for various reasons, including differences in perception and tolerance of risk or differences in motivations. Government can act as an enabler to align these risk management expectations. If targeted regulatory action to bridge these differences is considered, it should

[8] Profiles are used to define how a standard will be deployed, and against which interoperability testing can be used to demonstrate compliance.

[9] U.S. Government Accountability Office, *Strengthening the Use of Risk Management Principles in Homeland Security* (GAO-08-627 SP), April 2008, http://www.gao.gov/new.items/d08627sp.pdf.

be undertaken with caution and in consultation with affected companies to avoid unintended consequences. Alternatively policymakers should first consider providing market incentives to the private sector to meet shared national security and public safety requirements.

Recommendation: Government and industry need to recognize that their risk-management perspectives stem from different roles and responsibilities. Where the government demands a higher standard of care, market incentives need to be available to accommodate non-commercial needs for security.

Incentives

Currently, the most effective way to stimulate innovation and development of infrastructure is through economic incentives. In the last century, the incentive-based approach, in contrast to the government-centric regulatory model seen in other parts of the world, resulted in the creation of information infrastructures in the United States that provided the engine for America's economic competitiveness in the 20th century. A similar and modernized version of this market-incentive model needs to be developed to meet our nation's present cybersecurity needs. Such a system will likely enhance not only our security but also our economy. Public and private studies indicate that this model will work for cybersecurity. The CSPR found that policymakers should consider, in consultation with affected parties, a mix of tailored incentives to achieve the nation's cybersecurity objectives.

Central to this finding is the realization that cybersecurity is not simply a technical or operational issue but a strategic and economic one. A 2010 study conducted by the Center for Strategic and International Studies (CSIS) states that a primary obstacle to ensuring the security of critical networks is cost.[10] Similarly, a survey by PricewaterhouseCoopers of business executives responsible for their organization's information security reported that roughly half of them pointed to the recession as a cause for restraint in funding cybersecurity.

One of the most immediate, pragmatic, and effective steps that the government could take to improve our nation's cybersecurity would be to implement the recommendations made in the CSPR to explore incentives, such as liability considerations, indemnification, and tax incentives. For example:

- Tax incentives that encourage establishing additional cybersecurity investments, such as the R&D tax credit;

[10] Center for Strategic and International Studies, *In the Crossfire: Critical Infrastructure in the Age of Cyber War*, 2010, http://csis.org/event/crossfire-critical-infrastructure-age-cyber-war

- Grant funding using effectively in other homeland security areas such as emergency preparedness and response. Critical infrastructure industries can use grant funds for research and development, to purchase equipment, and to train personnel;
- Streamlining regulatory procedures, which would cut both government and industry costs;
- Updating the SAFETY Act to better appreciate the cyber threat that has become more evident since its enactment. This Act, which provides a mix of marketing, insurance and liability benefits for technologies designated or certified by DHS, can be expanded to standards and practices as well as technologies that protect against commercial as well as terrorist threats;
- Liability protections or regulatory obligations (e.g., for utilities) adjusting in numerous ways to provide incentives for enhanced security practices, such as adoption of standards and practices beyond what is required to meet commercial risks, or enhanced information sharing. Liability benefits do not need to be elevated to immunity to be attractive. Categories of liability (e.g., punitive vs. actual damages) or burden of proof levels (preponderance rather than clear and convincing evidence) can be adjusted to motivate pro-security behavior without costing taxpayer dollars; and
- Stimulating the growth of a private cyber insurance industry that can both provide private economic incentives to spur greater cybersecurity efforts while also creating a private market mechanism that fosters adoption and compliance. The government should give consideration to implementing reinsurance programs to help underwrite the development of cybersecurity insurance programs. Over time, these reinsurance programs could be phased out as insurance markets gain experience with cybersecurity coverage.

To accommodate the needs of a wide variety of critical infrastructures with different economic models, the public-private partnership should develop a menu of incentives that can be tied to voluntary adoption of widely-accepted and proven-successful security best practices, standards, and technologies. The R&D tax credit may be the most attractive option for an IT security vendor, while a defense firm may be more interested in procurement options, an electric utility in a streamlined regulatory environment, or an IT-user enterprise in an insurance discount and risk transfer. Many of these incentives are deployed successfully in other areas of the economy, but not yet to cybersecurity.

Recommendation: Working through the NIPP framework, government and industry must develop a menu of market incentives that government can put in place to motivate companies to voluntarily adopt additional security practices and technology investments. The incentives must be powerful enough to affect behavior without being so burdensome as to curtail US investment, innovation, and job creation.

II. INCIDENT MANAGEMENT

Companies and government entities regularly and successfully respond to cyber attacks and other intrusions on their networks. In many organizations, there are processes and procedures for incident response and reporting that are used to protect their networks and information assets on a regular basis. It is when an incident becomes too big or complex for one organization to handle alone that collaborative incident management – and partnership – is important in order to prevent, defend against, and recover from the attack. Many attacks have called for collaborative action, and public and private partners learn from each incident how to communicate, share information, and remediate the problem. In addition, they engage in exercises that are designed to test processes and plan for incident response from which they continue to learn what the most effect measures are in any given circumstance.

The Cyber Storm exercise series has been an excellent tool for understanding the possible course of any particular incident – or combination of attacks – and for assessing existing response measures and determining gaps. Industry has been a partner in the planning and play of the exercises, which have spanned the critical infrastructure sectors and incorporated many aspects of attacks on that infrastructure. In each of the three Cyber Storm exercises, the participants have used the lessons learned to make corresponding changes in their internal procedures and in the procedures used to collaborate among the participants.

In the most recent Cyber Storm III exercise, the scenarios tested the preparation and processes laid out in the National Cyber Incident Response Plan (NCIRP) completed prior to the exercise. The development of the NCIRP was a collaborative process between industry and government. It resulted in a plan that was meant to be instructive for both groups, but flexible enough to accommodate the varying types of scenarios that could occur. The official results and lessons learned from Cyber Storm III are still being assessed and reported, but the immediate observations from the exercise are already being evaluated and integrated into organizations' planning procedures.

Rigid response protocols and procedures are not effective in managing each possible type of incident, and it has been important to recognize and acknowledge that there is no one-size-fits-all in cyber incident response. Cyber incidents do not occur in one moment; they can evolve and grow in nature and impact over time. These attributes require flexibility and an iterative evaluation mechanism that includes impacted parties – those that are the victim(s), and those that can provide assistance. In that vein, it is important to have an ongoing, sustained collaboration mechanism to continuously assess the problem as it occurs over time and to determine the most effective response tools.

Through the National Cyber Coordination and Integration Center (NCCIC), government and industry are in the early stages of implementing a long-standing recommendation that industry responders from the IT and communications sectors should work together with their government counterparts in an integrated operations center so that their respective expertise, analysis, and response capabilities can be shared and leveraged on a sustained basis – not just in times of crisis. The NCCIC is a very positive development in the public-private partnership and should be strengthened by the full participation of industry.

Recommendation: Government should fully establish industry's seat in the integrated watch center and begin evaluation and process for growing industry's presence; industry should ensure a long-term plan for filling the watch center seats; and participants should report lessons learned from collaborative exercises as soon as possible and undertake improvement measures on a timely basis.

III. INFORMATION SHARING AND PRIVACY

Effective information sharing is crucial to any collective effort to prevent cyber attacks and to respond to cyber incidents.

Information sharing, as practiced today, is not sufficient or effective enough to address cybersecurity threats. Government and industry partners should first articulate the types and sources of information and analysis that need to be shared in order to achieve our nation's cybersecurity goals and identify the types of information that are not being sufficiently shared. Various proposals have been put forward to impose mandates on industry to share information with a new government "clearinghouse" that would process the information it received, achieve situational awareness with respect to the health of major public and private networks, and disseminate information to owners and operators of those networks to prevent and respond to cyber incidents.

However, the objective should be to improve the quality, not necessarily the quantity, of the information shared. Rather, the scope of the information exchange should be driven by an analysis of the respective roles of the private sector and the government and by a better understanding of the collective or collaborative action needed to combat current or future attacks. Based on such a framework, more nimble approaches can be developed to muster the kind of information sharing necessary to meet cybersecurity challenges. Also, such a framework will more likely produce information-sharing procedures that do not involve the routine sharing of data about traffic over private networks, which poses acute concerns for civil liberties and the protection of financial and proprietary information or intellectual property.

Sector-designated information-sharing mechanisms, such as the ISACs, are now integrated into the public-private partnership framework. Some sectors, such as finance, information technology and communications, are well known to have strong and proven information-sharing capabilities. An approach to information-sharing that focuses on identifying information requirements for sectors, and organizations within sectors, and building the capacity of these existing information sharing mechanisms and on building the capacity of the U.S. Computer Emergency Readiness Team (U.S.-CERT) in DHS is more likely to have immediate results. In contrast, a top-down, government-centric approach is unlikely to be able to react with the agility necessary to deal with rapidly evolving threats and attacks.

Enhanced self-interest and a flexible approach are more likely than government mandates to result in the sharing of the most useful cybersecurity information. As with any other partnership function, information sharing is founded upon and enabled by trust. That trust is weakened when government information-sharing mandates are imposed. Therefore, they are far less effective than a private sector-driven, well–incentivized program of collaboration. However, government does have an important role in fostering the effectiveness of information-sharing mechanisms. For example, government can increase market-based incentives for sharing information through mechanisms such as creating safe harbors, so that information that is shared about an incident, and that belongs to carefully defined categories of cybersecurity information, is not used to establish liability about the incident.

Information sharing also needs to evolve with modern threat patterns. For example, the information sharing model referenced in the CSPR[11] shifts the focus from sharing inbound attacks and technical vulnerabilities to unauthorized outbound traffic and needs to be developed. Since many modern attacks such as advanced persistent threats (APT) are not successful until data is exported from the system, managing unauthorized URLs and websites

[11] Obama Administration, *Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure*, May 2009 at A-4, citing Internet Security alliance, paper by Jeff Brown, Raytheon Company, entitled *A National Model for Cyber Protection Through Disrupting Attacker Command and Control Channels*, March 2009.

can be an effective defense. Sharing this information side-steps some of the current barriers to sharing since no proprietary or source data is required. Moreover, simply blocking unauthorized command and control sites is much easier; hence, this actionable information can be shared broadly using something similar to the current anti-virus model, which may even allow for the development of a market-based system with incentives for both the sharing and distributing parties.

The government can also play a role by more effectively sharing the cybersecurity information that industry would find valuable to identify and remove the most sophisticated attacks. There should be an assessment of the extent to which attack signatures and other information encountered by intelligence agencies can be shared with industry. The current policy against sharing that data can be detrimental to security if information is not shared with those that need it to meet their security missions. If additional cleared private sector personnel would be beneficial, then there should be a focused effort on filling that gap. Actionable threat information sharing and effective response requires trusted sharing at the controlled unclassified information (CUI) level with ISACs and equivalent information sharing mechanisms appropriate for each sector.

Protection of personal privacy is essential to the operation of any cybersecurity information-sharing or collection activity. It furthers an important societal value – personal privacy – and will promote public acceptance of necessary cybersecurity measures. Cybersecurity measures should honor the promise of the Obama Administration and ensure that the monitoring of private sector networks for malware or other malicious activity is conducted by the private sector entities that operate them, not by the government.

> "Our pursuit of cybersecurity will not – I repeat, will not – include [governmental] monitoring of private sector networks or Internet traffic. We will preserve and protect the personal privacy and civil liberties that we cherish as Americans."
>
> *President Barack Obama, Release of the* Cyberspace Policy Review*, May 29, 2009*

Building on the premise that system operators should be responsible for monitoring their own systems, the analysis, collection and sharing of communications containing personally identifiable information (PII) for cybersecurity purposes should comport generally with the Fair Information Practice Principles. DHS adopted an articulation of these principles in its 2008

Privacy Policy Guide.[12] In the cybersecurity context, application of these principles would mean that:

- Users are given notice of the cybersecurity monitoring and information sharing program and that it may involve collection and use of PII;
- The cybersecurity purpose for which the PII would be collected is carefully articulated;
- Only the PII necessary to accomplish the purpose is collected and shared, and it is used only for cybersecurity matters;
- PII collected for cybersecurity purposes should be retained only as long as it takes to fulfill the specified purpose, and then should be deleted by all parties;
- To the maximum extent feasible, information is sanitized of information identifying innocent parties before it is shared;
- The PII collected is accurate, relevant, and timely, and it is properly safeguarded against unauthorized access or improper disclosure; and
- Actual use of the PII is audited to ensure compliance with these principles.

Moreover, the collection and sharing of communications information for cybersecurity purposes must comport with surveillance statues, including the Wiretap Act, 18 U.S.C. 2510 et seq., the Stored Communications Act, 18 U.S.C. 2701 et seq., the Foreign Intelligence Surveillance Act, 50 U.S.C. 1801 et seq., and the pen register and trap and trace statute, 18 U.S.C. 3121 et seq. These laws already give substantial authority to providers and other system operators to monitor their own networks for cybersecurity. For example, the Wiretap Act permits electronic communication service providers to intercept, use, and disclose communications passing over their networks while they are engaged in any activity that is a "necessary incident" to the protection of their rights and property.[13] In addition, the computer trespasser exception to the Wiretap Act permits a service provider to authorize the government to intercept the communications of a person who accesses a computer without authorization if there are reasonable grounds to believe that the communication is relevant to an investigation of the trespass.[14] Transparency about the extent of disclosures now being made under these exceptions would enhance the ability of Congress and the public to assess their effectiveness and impact on privacy.

While current law provides substantial authority to collect, use, and disclose communications, including content for self-defense purposes, it does not provide explicit

[12] U.S. Department of Homeland Security, Privacy Policy Guidance Memorandum, December 29, 2008, http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf
[13] 18 U.S.C. 2511(2)(a)(i).
[14] 18 U.S.C. 2511(2)(i).

authority to do the same for the defense of others. As noted above, further inquiry is needed to determine exactly what information needs to be shared, but where there are legal barriers to necessary information sharing, it may be necessary for Congress to create a very narrow exception to the surveillance laws to permit such disclosures. Under any such exception, disclosures should be permissive and not mandatory and should be made only for cybersecurity purposes and only when a reasonableness standard is met.

Recommendation: Government and industry should clearly articulate information needs and how to promote more effective information sharing to address those needs; information sharing for cybersecurity purposes should be transparent and should comply with fair information practice principles; government should consider how it can share more classified and sensitive information, particularly the parts of that information that can help the private sector defend its systems; and in consultation with interested parties, including industry and civil liberties organizations, Congress should consider whether narrow adjustments to surveillance laws are needed for cybersecurity purposes.

IV. INTERNATIONAL ENGAGEMENT

The cyber networks and infrastructure constitute a global system where traditional borders do not apply. Not only are our companies and networks global, but so are our adversaries'. This global attribute must be taken into consideration for any policy or operational aspect of cybersecurity.

Any public policy deliberation must consider the impact of that policy on global competitiveness, interoperability, and compliance obligations. The companies that fuel our nation's economic growth are operating globally in one way or another. They either have business operations in many other countries, source their products and services globally, or rely on just-in-time delivery of components or products to meet their domestic customers' needs. Therefore, we cannot deliberate public policy with merely a national lens. Our nation's policy impacts the ability of its companies to do business globally, either directly through prescriptive restrictions or indirectly as a result of reciprocity or copycat policies in other countries.

Further, if U.S. policies raise concern about the level of government engagement in corporate networks or data, it will raise skepticism by global customers regarding the U.S. government's access to their corporate or consumer data and the implications of that access. Customers will simply go elsewhere to find providers that do not pose the same concern. These potential consequences may not be apparent in any particular policy, but that makes it even more important that U.S. policy making consider the global impact of any proposed measure.

The partnership, which includes companies whose very existence demands a global perspective, needs to be more fully utilized to ensure that global impacts are considered from the beginning of a policy development process, whether in Congress or the Administration.

The partnership can also contribute to the international aspects of cybersecurity. It is important to build and foster global relationships that enable harmonization of appropriate policy mechanisms where they are needed and allow cross-border coordinated action on preparation and incident response on a sustained basis. The interaction of US-CERT with its counterpart computer security incident response teams (CSIRTs) helps foster that international coordination. We need to explore ways to integrate industry into those mechanisms as appropriate to further collaborative action.

As part of an international strategy, the U.S. government needs to find ways to leverage engagements with key allies and the global community (at varying degrees, as appropriate) to collaborate on improving situational awareness, analysis, and response, containment, and recovery measures. Current government-to-government efforts could be bolstered by new institutional arrangements or reduction of barriers to international coordination. In addition, such a strategy should articulate where in the international community the government should engage and with what position(s), and the role or efforts of the agencies engaged to ensure a consistent and coordinated approach. Because of its international engagement, the private sector has much to offer to these inter-government processes.

Given the importance of the global community in improving cybersecurity and critical infrastructure protection, the international component should be part of our national strategy. The CSPR specifically addresses this aspect and refers to the need to incorporate cybersecurity in our global diplomatic efforts. Not only can the U.S. reach out to global partners, but it can also provide capacity building that enables those countries to take measurable steps to improve their cybersecurity capabilities and become partners in the global effort to combat cyber attacks and cybercrime.

In order to develop and implement a cybersecurity diplomacy strategy, government needs to coordinate among its various components. In that regard, we applaud recent interagency coordination efforts and the establishment of a Coordinator for Cyber Issues to lead the Department of State's engagement on cybersecurity. There needs to be an early and ongoing partnership in order for both government and industry to leverage expertise, experience, insight, and relationships toward greater collaboration and success in the international environment. The global approach should include ways to foster even greater cooperation among law enforcement to more effectively pursue and prosecute cyber criminals.

Recommendation: Industry and government need to engage in international organizations and standards-making processes and work together to develop a strategy for engagement, capacity building, and collaboration on issues of global concern.

V. SUPPLY CHAIN SECURITY

Supply chain security is critical to cybersecurity. Without appropriate assurance that technology products and services are not counterfeits, are reasonably free from intentional and unintentional vulnerabilities, are appropriate to the level of threats they face once deployed, and are correctly configured and maintained, there can be little confidence that the information and communications they process and store are safe and secure.

Supply chain security is another area of cybersecurity policymaking and operations that requires that both government and industry leverage international industry best practices and standards, as well as work in a close public-private partnership. We believe such a partnership is needed to assure appropriate levels of security in the supply chain while transcending national boundaries, being economically practical, and including appropriate market incentives. As information technology is developed on a global basis, our approach to supply chain security must also be global.

Potential risks differ across sectors and throughout the development life cycle. Therefore, each actor in the life cycle has different risk management responsibilities. The public-private partnership can help them better discharge their responsibilities.

Technology suppliers have a responsibility to develop and deliver solutions that meet the needs of their global customer base and are worthy of its trust. To this end, the providers have contributed to the development of a wide spectrum of best practices and standards, as well as their own company-specific practices and controls. Assurance and inspection processes should be in place to verify product trustworthiness. The partnership has two important roles in that regard:

- Standards for assurance are developed through a multi-stakeholder international partnership framework rather than setting country-specific assurance standards, the government should expand its participation in the international standards-setting process;
- The public-private partnership should also facilitate the identification and dissemination of effective international assurance standards and best practices.

The principal international standard for product assurance is ISO 15408, also known as the Common Criteria. There is a robust network of independent evaluation labs that are accredited under the standard to conduct product reviews that are mutually recognized under the Common Criteria Recognition Arrangement (CCRA), and product evaluations are accepted in more than twenty countries.

In its current form, the Common Criteria has been mostly applied to critical products that perform security functions. The difficulty with deploying the certification more widely comes from the fact that the process is costly, while the expected risks may not warrant such expense. In addition, the timeframes associated with achieving the certification are often not compatible with current market demands for product development.

The public-private partnership should play a critical role to reform Common Criteria and address these issues, as well as advance Common Criteria's utility in the global marketplace. Additionally, the partnership should examine industry engineering best practices to see how they may be applicable in any additional framework for products that are not as critical as to warrant the use of Common Criteria. NIST should work with industry and other agencies to undertake this examination. Any other framework developed should be consistent with and complementary to the Common Criteria.

Finally, as recommended by the CSPR, the government can make another contribution to the supply chain security efforts of technology providers by sharing specific and actionable threat information with them, to help them address such threats and improve their supply chain and technology design and development processes.[15]

Acquirers of technology also have an important role to play. The selection of specific supply chain risk management practices varies depending on the role of the IT system and how critical the IT element is within the system. Technology acquirers need to evaluate their suppliers' practices on the basis of recognized industry standards and best practices. They also have a responsibility to follow recognized best practices as they configure, integrate, deploy, and maintain technology solutions.

Acquirers of technology should actively leverage tools and resources available to ensure that they do not acquire counterfeit technology products. IT suppliers, especially commercial–off-the-shelf (COTS) vendors, have been fighting a sustained and costly battle against counterfeit products for decades. The government should work in close partnership with industry to establish best practices that ensure the acquisition, integration, implementation, and use of genuine and legitimate products throughout the life cycle of systems. This includes

[15] Obama Administration, *Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure*, May 2009 at 35.

leveraging commercial anti-piracy and anti-counterfeiting technologies and processes and putting in place more rigorous requirements for the government to purchase only from authorized dealers and resellers.

Providers of technology products and services implement a wide spectrum of international standards and best practices, as well as company-specific practices and controls so that their technology solutions deliver appropriate levels of security. Mandating country-specific, government-created risk management practices limits the user's access to cutting-edge technologies, causing several negative effects:

- A lack of measurable increases in security. For example, government has made attempts to require technology providers to share information that contains intellectual property and other trade secrets. Few if any acquirers have the appropriate level of technical expertise to make decisions based on such information, while suppliers would experience significant harm if that information's confidentiality was compromised.
- Government mandates evolve at a slower pace than technology; therefore, they compromise innovation by freezing design, development, and supply chain risk management practices in time and hampering related economic growth.
- Disparate and redundant government requirements regarding supply chain security would weaken security, because resources that would otherwise go to improving security would be assigned instead to complying with multiple standards.
- Mandates that are fundamentally at odds with recognized industry best practices and international standards restrict companies that build solutions for a global marketplace. As a result, such mandates greatly hinder competition between vendors, leading to fewer choices and higher costs. They would also open the door to imposition of other, divergent requirements by foreign governments. These effects would harm America's competitive position in the global marketplace.

Recommendation: The government should expand its participation in the international system that develops supply chain security standards and work with industry to identify and disseminate them. Government should then leverage those standards when it acquires technology and take steps to prevent its acquisition of counterfeit technology products.

VI. INNOVATION AND RESEARCH AND DEVELOPMENT

Cybersecurity is a fast-paced race in which malicious cyber actors constantly adapt their tactics and tools. To prevail, we must also constantly adapt our defenses. Cybersecurity policy

should therefore maximize the ability of organizations to develop and adopt the widest possible choice of cutting edge cybersecurity solutions. An effective way to do this is through the creation and implementation of a National Cybersecurity R&D Plan.

Currently, federal cybersecurity R&D efforts are conducted under the Federal Plan for Cybersecurity and Information Assurance Research and Development (CSIA), which was established under the Networking and Information Technology Research and Development Program. CSIA plan's effectiveness can be improved by using public-private partnership mechanisms to define, as well as pursue, national objectives.[16]

A National Cybersecurity R&D Plan needs to be created and must have the following:

- National-level objectives—The Plan's objectives must be established on the basis of a truly comprehensive and holistic view of the cybersecurity needs of the nation. Unlike the CSIA plan, the National Plan should not be principally based on the needs of the federal agencies that fund or conduct cybersecurity R&D, because their aggregation, although valuable, does not produce a cohesive picture of the nation's overall R&D needs.
- Prioritized objectives—Regrettably, the objectives of the CSIA plan are not prioritized. The National Plan's objectives must be established on the basis of a clear prioritization of what needs protection at the national level, so that greater attention and resources are devoted to the protection of critical and strategic national interests, while others receive less support.
- Objectives set jointly by public and private partners–The CSIA plan has suffered from insufficient input from non-governmental stakeholders. Simply put, the National Plan should not be just a government one: the definition and prioritization of national objectives require that a wide community of public and private partners play an integral role from the earliest stages of the process and throughout the creation of the Plan, as well as when the Plan's objectives and implementation activities are reviewed.
- Balanced long-term and short-term objectives—the Plan should combine long-term, proactive, "game-changing" objectives, with short-term, reactive, tactical objectives. As a general rule, we recommend that the government focus its own cybersecurity R&D efforts – which it would undertake under the Plan – on long-term and basic research. It is appropriate for the government to be involved in applied R&D if the technological solution that is sought is not commercially available, and its absence

[16] Most of these recommendations were made to the Science and Technology Committee of the U.S. House of Representatives, and were incorporated by the Committee in sections 103 and 108 of H.R. 4061, the Cybersecurity Enhancement Act of 2010, which was adopted by the House on February 4, 2010.

creates a measurable security gap. Federal agencies should be required to ascertain, in collaboration with the private sector, whether commercial solutions exist or could be readily adapted, before they invest in an R&D project to develop equivalent capabilities. By leveraging new and existing cybersecurity technologies, in addition to research and development, the government will be able to better utilize its limited resources.

- Regular review by the partners—Innovation in information technology and cybersecurity evolves rapidly. This is why the process for setting the Plan's objectives must be extremely flexible, to allow for a cyclical, comprehensive and genuinely critical review.

Perhaps one of the key deficiencies of the CSIA plan is that it lacks a road map for its implementation. It sets objectives, but does not detail how to reach them. The National Cybersecurity R&D Plan must have an implementation road map that:

- Is detailed: the Plan's road map must determine which partners, be they federal agencies, academia or industry, are responsible for what R&D projects, along with specific timelines, desired outcomes and assigned resources. This would provide the partners involved with the guidance and coordination necessary to reach the objectives, and would enable assessment and accountability.
- Addresses industry's role and government's role in its implementation: the cybersecurity R&D efforts that industry undertakes, with or without federal support and funding, should be an integral part of the Plan's road map. Congress should explore ways to make industry participation in federally funded cybersecurity R&D more attractive, by improving the ownership or licensing of intellectual property (IP) it generates. This would be similar to what Congress did for small businesses, non-profits and universities through the Bayh-Dole Act in 1980. The federal government should also improve its sharing of the innovations generated by cybersecurity R&D conducted by federal agencies. Too often, those innovations are not shared with industry, even though they could benefit the Nation as a whole through production with licensing conditions that appropriately reward the agency in question.
- Is regularly reviewed by the partners: a review would provide accountability by ensuring that actual progress is made and would verify whether the timeframes initially envisioned are realistic. The threat and technology landscape changes rapidly. An annual review of the objectives and the effectiveness of the related implementation activities is also recommended.

Recommendation: The public-private partnership should be used to create a genuine National Cybersecurity Research and Development Plan with prioritized, national-level objectives and a detailed road map that specifies the respective roles of each partner. The plan and its implementation road map should be regularly reviewed by the partners and adjusted as necessary.

VII. EDUCATION AND AWARENESS

In May 2009, President Obama articulated the need for wider public education about protecting America's cyberspace. He called for a national public awareness and education initiative to promote Internet security. The President said, "It's the great irony of our Information Age—the very technologies that empower us to create and to build also empower those who would disrupt and destroy." However, a May 2010 poll conducted by two leading Internet security education and awareness organizations found that the vast majority of Americans are willing to practice good Internet safety and security habits given the right resources.[17] Americans feel that doing their part to help keep the Internet safe benefits their homes and businesses as well as our national and economic security. The public-private partnership is strengthened through policies that help educate people about cybersecurity risks and countermeasures that they can implement to better protect themselves. The partnership is also strengthened through policies that assist cybersecurity professionals to voluntarily improve their skills.

Importantly, "*Stop. Think. Connect.*" is a new public-private education and awareness campaign to help people stay safer and more secure online. It is an outgrowth of the Administration's CSPR to-do list. "*Stop. Think. Connect.*" seeks to achieve for online safety and security awareness what Smokey Bear does to prevent wildfires and "Click It or Ticket" does for seatbelt safety. And yet, more needs to be done. We recommend heeding the 2009 example of government and industry mobilization to halt the spread of the H1N1 flu. Simple and effective resources were made widely available to individuals and families, businesses, and communities to mitigate the impact of the outbreak. An array of media (TV, the workplace, and social media, among others) was used to provide public education and simple recommendations to control infections. The effort was a success because of sustained national leadership and years of planning and preparedness by the public and private sectors prior to the pandemic. This collaborative effort could serve as a model for cybersecurity education and awareness.

[17] See August 10, 2010, press release by the National Cyber Security Alliance and the Anti-Phishing Working Group, available at: http://staysafeonline.mediaroom.com/index.php?s=43&item=62

This campaign could be strengthened by also emphasizing a holistic "people, process and technology" approach to cybersecurity, rather than focusing solely on the user. This would include education about new cybersecurity technologies and the importance of regularly applying security patches to systems.

While much attention has rightfully focused on educating consumers and youth, an educational effort aimed at building awareness among business owners, managers, and employees that cybersecurity is an enterprise risk management issue needs to be further developed and communicated through the partnership. A view of cybersecurity solely as an IT problem masks the larger financial risks cyber vulnerabilities hold for the entire enterprise and could result in under-investing in cybersecurity. However, businesses can substantially reduce the negative consequences of a successful cyber incident through risk management across the entire organization. Promotion of ongoing employee evaluations regarding cybersecurity awareness and cybersecurity policy compliance is needed.

The interconnectedness of computers and networks in cyberspace means that the public and private sectors share responsibility for promoting security as an enterprise-level objective. The CSPR captures this point succinctly: "It is not enough for the information technology workforce to understand the importance of cybersecurity; leaders at all levels of government and industry need to be able to make business and investment decisions based on knowledge of risks and potential impacts."

A goal of the partnership should be to increase the pool of cyber professionals available to the public and private sectors, including fostering policies that add to the number of U.S. science, technology, engineering, and mathematics (STEM) college students graduating annually, to tackle our major cybersecurity challenge.

***Recommendation*:** The public-private partnership should enhance cybersecurity public awareness and education, and increase the number of cyber professionals available to both government and business, including through policies that boost the number of science, technology, engineering, and mathematics (STEM) college students graduating each year.

CONCLUSION

Regular and meaningful collaboration between the public and private sectors is the essence of a strong partnership. A strong framework for promoting cybersecurity through a public-private partnership is already in place, and industry and government have devoted substantial resources to it. There is no need to create a new one, or to replace the existing partnership model with a system of government mandates that would erode trust, threaten

privacy and undermine voluntary cooperation. This would be a setback for cybersecurity. Rather, industry and government must both do more to implement the existing partnership model and meet the growing threat that cybersecurity represents. This White Paper presents a number of measures carefully targeted at existing problems. Adopting these measures would enhance the effectiveness of the public-private partnership. We look forward to working with the Executive branch and with Congress to implement these recommendations to promote cybersecurity, spur innovation, and protect privacy.