



July 29, 2011

The Honorable Dennis Hightower
Deputy Secretary
United States Department of Commerce
1401 Constitution Avenue, NW
Washington, DC 20230

Via e-mail to: SecurityGreenPaper@nist.gov

Re: United States Department of Commerce, Notice and Request for Public Comments
Cybersecurity, Innovation and the Internet Economy
Docket No. 110527305-1303-02

Dear Deputy Secretary Hightower:

The Bay Area Council thanks the Commerce Department for its well thought-out Green Paper on cybersecurity. The paper demonstrates both a pragmatic and a nuanced approach to some of the greatest challenges confronting American businesses. As breaches, violations, and cyberattacks increase in frequency and sophistication, it has become essential to swiftly develop and implement strong solutions that can be driven by private industry, with the assistance of government and law enforcement where appropriate. To ensure the best strategy is followed in this critical time, the Bay Area Council has formed a multi-sector, dynamic Cybersecurity Committee to offer its feedback and help shape cybersecurity policy to ensure a thriving economy. The Cybersecurity Committee represents a wide range of industries, including banking, finance, technology, security, health care, energy, food, and retail, among others.

The Bay Area Council is a business-sponsored, public-policy advocacy organization comprised of private employers in the Silicon Valley-San Francisco-Oakland Bay Area. Founded in 1945, the Bay Area Council is widely respected by elected officials, policy makers and other civic leaders as the voice of Bay Area business. Today, approximately 275 of the largest employers in the region support the Bay Area Council and offer their CEO or top executive as a member. Our members employ more than 4.43 million workers and have revenues of \$1.94 trillion, worldwide. The Council proactively advocates for a strong economy, a vital business environment, and a better quality of life.

We thank you again for inviting comments to your Green Paper and hope you will take into consideration our views and concerns, which are respectfully elucidated below.

Critical infrastructure needs to be explicitly defined

A clear delineation of the organizations which fall into the category of critical infrastructure from those in the Internet and Information Innovation Sector (IIS) is needed, as the organizations that might fall into

either category grapple with the uncertain prospect of differing regulatory oversight. As regulations are implemented for critical infrastructure, it is important to note that the additional costs involved in implementing stricter security measures may introduce a cost disadvantage for covered entities and create an unlevel playing field with regard to new or smaller competitors that are not covered. To mitigate this inequality, and to ensure that technology and business develops in a way that includes appropriate cybersecurity practices, codes of conduct should be determined by equal criteria for both covered and non-covered entities, and scaled to match the size, significance, and capacity of each enterprise. The Bay Area Council would welcome the opportunity to be a part of the effort in determining these criteria and developing these codes of conduct.

International security policies should be globally uniform

As the U.S. government works to promote voluntary codes of conduct internationally, it should pursue globally uniform standards and best practices. Because many countries use their own product assurance criteria, encryption code policies, and other security procedures, there is disharmony in the international market that introduces unnecessary costs and complexities that do not further a more secure environment. And as long as there are significant differences in the stringency of security policies, competitive disadvantages will continue to hinder the market. International trade needs to flow freely, minimizing trade barriers that limit commerce, and the needs of trade and security need to be optimized by promoting equal standards and policies for all entities across country lines. In this endeavor, the United States should strive to be an international leader in security policy, avoiding a reactionary strategy in the global marketplace.

Threat priorities should be clarified

It is critical to clarify the roles that private industry, state agencies, and the federal government should play in cybersecurity. To do this, we need to make distinctions among the different kinds of threats in the cybersecurity world. Not all dangers are within the capacity of private industry to prevent or remedy, and not all dangers mandate the same response strategy. Standards and best practices need to reflect these differences, and to take into account that private industry should be focused on mitigating cybercrime against both the institution and the consumer, protecting against attacks like intellectual property theft, identity theft, and financial fraud. Similarly, it is primarily the role of states to protect consumers by enforcing state laws, and the role of the federal government is to combat international criminals, foreign government intrusions, and other national security threats. In light of the Department of Defense's recent designation of a cyberattack as a potential "act of war," emphasizing the need to fight crime, protect the country's national security, and to foster measures that deter external agents from aggression, we recognize that cyber attacks will differ in origin, nature, and impact, and therefore caution against an insufficient discussion of the roles that private entities and public agencies should play.

Priorities: codes of conduct development, data collection, awareness building, and consumer confidence

We put forth the following four priorities for improving the nation's internet security:

a) Security compliance-safe harbor program - The potentially central role of incentives in effectively driving widespread compliance with best practices requires that the incentives be chosen wisely, with a realistic appreciation of business interests. Liability protections are an important such incentive. Offering tangible benefits, predictable outcomes, and a level-playing field for the business community, they have substantial motivational power with private enterprises. Safe harbors, even of a qualified nature, in exchange for adoption of effective standards and best practices offer important financial safeguards. This possibility should not be discounted because of fears of misdirected resources, the stifling of security innovation, or inducing a false sense of security. In our experience, safe harbors are an effective means by which codes of conduct can remain voluntary while being established, monitored, and adapted when necessary by a respected independent body. In such an environment, compliance with codes is just as likely as it is when codes are imposed coercively, and the voluntary codes will prove more effective.

The body of standards and best practices required to qualify for safe harbor should evolve in line with innovation and new information, and should be more responsive to the most current threats and needs of business than inflexible pre-existing federal minimums. These standards should be risk-based and scalable. Requirements should take into account the size and resources of companies, as well as the quantity and sensitivity of the data which they possess.

b) Data collection - To confidently implement difficult and costly security controls, private enterprises need reliable information about which security strategies and controls are effective. Despite the efforts of government, Information Sharing and Analysis Centers (ISACs), and independent organizations to advance data leveraging and information sharing, there remains a need for a dependable and authoritative voice to determine which codes of conduct, standards, and technologies actually prevent attacks and deter cybercriminals. To this end, a data collection agency is needed to collect and analyze data about threats and intrusions in a voluntary and liability-protected framework. Without this kind of data and analysis, enterprises are forced to assume most practices to be ineffective, thus reducing the value of all vendors in the security sphere.

c) Education and awareness - At present, individual consumers and small businesses are especially attractive targets for attackers, as they are the least educated on cybersecurity and have the fewest resources to combat attackers. For the protection of these entities, and of the larger enterprise networks to which their systems are connected, we encourage education programs to help owners, operators, and consumers become more aware of the risks they face and the technologies available to help them.

d) Consumer confidence - In addition to protecting data and ensuring the integrity of closed systems, codes of conduct should aim to bolster external confidence in security, helping consumers feel secure when utilizing enterprises' services and promoting trust in the internet environment. This can be achieved through plainly visible indicators of best practices compliance and strong investment in security.

The goals of: a) a security compliance-safe harbor program, b) threat and intrusion data collection, c) business owner and consumer awareness building, and d) consumer confidence improvement could be jointly achieved by the establishment of a new managing body charged with researching, building, and disseminating the best controls and standards available. This third-party managing body could be an independent government agency, working in cooperation with other agencies like NIST and the Department of Homeland Security. This independent agency would gather and analyze data and leverage that information to develop and frequently update a robust body of industry-specific codes of conduct and best practices, with which compliance would be rewarded with liability protection. At the same time, this agency would disseminate reports and information to inform business owners and consumers about security risks and technologies, and maximize its visibility to support consumer confidence.

To ensure multi-sector and popular acceptance, such an agency would need to be completely neutral, independent, and agnostic. Its government affiliation would give it the legitimacy needed for a seal or certification to gain traction in the commercial market, and would give the average consumer confidence that security measures are a top priority in the internet eco-system. This model has proven to be successful in other spheres, as evidenced by the widespread adoption of the safety recommendations of the National Transportation Safety Board and the legitimacy of Underwriters Laboratories for general product safety. Even without federally mandated standard compliance, companies would adopt this managing body's cybersecurity control recommendations for market competitiveness reasons.

Federal regulation needs to be balanced with voluntary codes of conduct

As hackers, criminals, and other malicious agents continue to evolve their skills in defeating security systems, defense mechanisms that are correspondingly innovative, sophisticated, and responsive to change are essential. An important factor in accomplishing this goal is an information sharing mechanism that facilitates the exchange of threat information between the government, public agencies, and private industry. We support an information sharing mechanism that is voluntary, ensures liability protection for private actors, and protects the sensitive data of participants in accordance with fair information practice principles. If the government aggressively shares its real-time threat data with private industry, and if all stakeholders work cooperatively to develop mitigation strategies and update security regulations, such a mechanism can bolster the ability of all parties to protect themselves against the newest and most advanced threats.

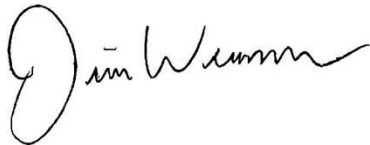
Although federal regulation may be necessary to implement the most essential security protections, especially for federal agencies and the nation's critical infrastructure, we emphasize that industry-specific and risk-based codes of conduct must be a central priority in any strategy for improving internet security. Even with an effective public-private mechanism for information sharing, government-mandated technical standards and regulations may become outdated quickly and inhibit the adaptation necessary to combat attackers. A strategy that relies on industry players to constantly develop, update, and implement new practices that reflect new technologies and new threats is integral to a secure cyber eco-system and a flourishing internet economy. These practices should depend on standards and shared best practices that are flexible, technology neutral, and goals-based rather than prescriptive. We think this is especially true in the I3S environment.

It is important to note that strong standards and practices - including PCI DSS, NIST Special Publication 800-53, and DNSSEC - already exist which should thwart the majority of cyber attacks. The Green Paper appropriately observes that many of these are applicable beyond their intended target entities and would greatly improve security beyond the baseline currently required by law. However, as the White House's Cyberspace Policy Review has acknowledged, these mechanisms are not deployed as frequently as they should be - generally because of high costs and intra-corporate complexities. The current perceived return on investment for companies does not favor improved standards and best practices compliance. This cost dissonance is the single greatest deterrent to strong security practices in private industry. For government to secure private and federal networks and protect its national infrastructure, it should aim to help reduce this cost dissonance and to incentivize best practices so that enterprises will clearly discern more benefit than cost in new implementations. The cost-benefit gap in cybersecurity must be closed, and it must happen soon.

In addition to a security compliance-safe harbor program, other incentive policies with promise to motivate improved cybersecurity include grant funding for research and development, tax provisions that will promote cybersecurity investments, and other financial measures that will mitigate the costs of security implementation. Furthermore, a more developed cyber insurance industry should promote better practices, but as matters now stand, there are too many unanswered questions to count on the insurance industry to provide near-term assistance to businesses facing substantial cybersecurity risks.

We hope you will consider the foregoing comments and recommendations, and we look forward to continuing communication between our organizations as our nation battles existing and anticipated threats to our cybersecurity.

Sincerely,

A handwritten signature in black ink that reads "Jim Wunderman". The signature is fluid and cursive, with the first name "Jim" being particularly prominent.

Jim Wunderman
President & CEO

For further information please contact:

Linda Galliher, J.D. | Vice President Public Policy | **BAYAREA COUNCIL**
415-946-8708 | LGalliher@bayareacouncil.org | www.BayAreaCouncil.org
201 California St., Suite 1450 | San Francisco, CA 94111