BSA®
BUSINESS SOFTWARE ALLIANCE

Robert W. Holleyman, II
President and Chief Executive Officer

1150 18th Street, NW
Suite 700
Washington, DC 20036

p. 202/872.5500
f. 202/872.5501

August 19, 2011

Mr. Jon Boyens
Senior Advisor, Computer Security Division
National Institute of Standards and Technology
US Department of Commerce
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

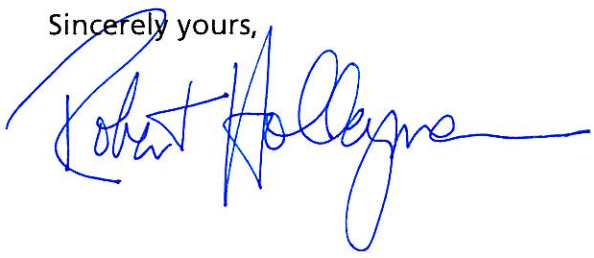
Dear Mr. Boyens:

I am writing on behalf of the members of the Business Software Alliance (BSA)* regarding the Request for Public Comments published in the Federal Register under Docket No. 110527305-1303-02 by the Department of Commerce regarding the Green Paper on Cybersecurity, Innovation and the Internet Economy.

Please find enclosed our full submission in response to the Green Paper. We want to once again express our appreciation for the Department's recognition in the Green Paper of the importance of innovation not only to American prosperity and competitiveness, but also to our Nation's and the world's global cybersecurity.

We look forward to continuing to support your cybersecurity policy efforts.

Sincerely yours,



The Business Software Alliance (www.bsa.org) is the leading global advocate for the software industry. It is an association of nearly 100 world-class companies that invest billions of dollars annually to create software solutions that spark the economy and improve modern life. Through international government relations, intellectual property enforcement and educational activities, BSA expands the horizons of the digital world and builds trust and confidence in the new technologies driving it forward.

Submission of the Business Software Alliance

to the United States Department of Commerce

Regarding the Green Paper on

Cybersecurity, Innovation and the Internet Economy
(Docket No. 110527305-1303-02)

Introduction

BSA commends the Department of Commerce for its recognition of the seriousness of the threat landscape – we face a constantly evolving, technologically sophisticated threat, created by a well-resourced set of actors who are often motivated by significant potential profits.

BSA believes that the Commerce Department has an important role to play in helping our Nation address this threat and improve its cybersecurity, for two reasons: it is the government's agency in charge of promoting innovation, commerce, economic growth and job creation; and these objectives need to be front and center in the cybersecurity debate: we won't have security without prosperity, and vice versa.

BSA believes that the Green Paper's approach is fundamentally the right one. To secure the large portion of the economy that's not critical infrastructure, we need an approach that:

- Is non-regulatory and flexible;
- Is based on incentives;
- Is based on an effective, results-oriented public-private partnership;
- Promotes innovation; and
- Promotes the adoption of global industry standards and generally-accepted industry practices.

BSA wants, in particular, to commend the Department of Commerce for centering its approach on global industry standards and generally-accepted industry practices. The global IT ecosystem depends on industry-led voluntary global standards created in international bodies like the IETF, IEEE, and similar organizations. These standards – and the generally-accepted practices that they often incorporate – permit the use of various solutions and approaches to a variety of process and technology challenges. These standards not only underpin the global IT ecosystem, but they greatly contribute to cybersecurity by spurring the development and use of innovative and secure technologies. The importance of international standards has been underscored by WTO commitments to use them.

Defining the Internet and Information Innovation Sector (I3S)

The Green Paper defines the I3S as a sector that includes functions and services that fall outside the classification of covered critical infrastructure, create or utilize the Internet and have a large potential for growth, entrepreneurship, and vitalization of the economy. More specifically, the following functions and services are included in the I3S:

- provision of information services and content;
- facilitation of the wide variety of transactional services available through the Internet as an intermediary;
- storage and hosting of publicly accessible content; and
- support of users' access to content or transaction activities, including, but not limited to application, browser, social network, and search providers.

How should the Internet and Information Innovation Sector be defined? What kinds of entities should be included or excluded?

First, we appreciate the Green Paper's function-based approach to cyberspace, which is generally much preferable to a system and asset-based approach.

Second, BSA supports an expansive scope of application for the cybersecurity efforts of the Department of Commerce. Few if any aspects of modern life and economic activity take place outside of, or do not depend on, cyberspace. Therefore, the government should promote cybersecurity to as many business sectors as possible.

Additionally, while regulation has a role to play in specific and genuinely critical circumstances, the Department of Commerce's voluntary and flexible approach, based on cybersecurity standards and generally-accepted industry practices, is preferable in the vast majority of circumstances to a regulatory approach that is more suited to a narrowly defined, highly critical set of systems and assets (the "covered critical infrastructure".)[1]

This is why we recommend that the proposed scope of the I3S be used as a starting point by the Department, rather than as a limit. *The I3S should include any economic function that is dependent on, or takes place in, cyberspace*. In particular, we believe it should expand its reach to cover the full spectrum of functions and sub-functions performed by the IT Sector. These functions have been detailed as follows in the IT Sector Baseline Risk Assessment[2]:

- Produce and provide IT products and services;
- Provide incident management capabilities;
- Provide domain name resolution services;

[1] This is not to say, though, that the principles that should guide cybersecurity policy development in the I3S – in particular industry-led development of standards and generally-accepted practices, and promotion of innovation – are not also relevant to CCI: we have consistently cautioned against regulatory approaches that would be based on government-developed, country-specific standards, and that would impose inflexible or burdensome obligations that hamper innovation and thus cybersecurity.

[2] See http://www.it-scc.org/documents/itscc/IT_Sector_Risk_Assessment_Report_Final.pdf

- Provide identity management and associated trust support services;
- Provide Internet-based content, information, and communications services; and
- Provide Internet routing, access, and connection services.

Working from this definition of the IT Sector would also have the effect of ensuring that there is coherence between the efforts of the Department of Commerce (resulting from this Green Paper) and those of the Department of Homeland Security (under the National Infrastructure Protection Plan – NIPP.)

Conversely, as stated below, we believe that the scope of CCI should be appropriately narrowed so that it does not lead to the regulation of a broad class of systems and assets that are not genuinely critical, to avoid straining or misusing limited government resources.

How can the I3S' functions and services be clearly distinguished from critical infrastructure?

The proposed I3S would exist alongside two other concepts: "covered critical infrastructure"[3] and "critical infrastructure."[4] We strongly urge the Department of Commerce, and the Administration at large, to be clear about what I3S, CI and CCI cover, where they may overlap and where they should not overlap. In particular, we urge that the terms "covered critical infrastructure" and "critical infrastructure" not be used interchangeably, as they represent different concepts, despite what their names might suggest.

The scope we propose above for the I3S – any economic function that is dependent on, or takes place in, cyberspace – would cover functions that are not within CCI, and include all of CI, as well as non-CI functions.

The I3S and "covered critical infrastructure" (CCI)—The Green Paper states there should not be overlap between the I3S and CCI. However, the scope of CCI proposed by the Administration is vague and therefore unfortunately potentially broad. This creates a risk of overlap between I3S and CCI, which should be averted: the I3S should have a broad scope, and the systems and assets performing I3S functions should be excluded from CCI.

BSA believes that the scope of CCI should be appropriately narrowed so that it does not lead to the regulation of a broad class of systems and assets that are not genuinely critical, to avoid straining or misusing limited government resources.

This should be done in 3 ways:

a. by tightening the CCI legislative criteria;
b. through the regulatory process that will be set up to further spell out this CCI criteria and apply it to designate CCI entities. We recommend that the Department of Commerce be closely involved in this process, given the reliance of CCI systems, assets and functions on the I3S, and to ensure that CCI coverage is narrow enough to preserve innovation in a broad I3S; and

[3] As defined in section 3 of the Administration's proposed Cybersecurity Regulatory Framework for Covered Critical Infrastructure.
[4] As identified by Homeland Security Presidential Directive 7 (HSPD-7).

c. by adopting the broad definition of I3S that we offered above, which by contrast would contribute to an appropriately narrow definition of CCI.

The narrowing of the CCI should ensure that there is no overlap between CCI and I3S. However, we believe it should be expected, and would be appropriate, that a company could have CCI systems or assets as well as systems or assets performing I3S functions (for its more critical and less critical operations, respectively.) This raises another concern we have about CCI: it should not apply to entire entities, but rather to specific systems and assets.

If there are benefits to participating in the I3S (e.g. incentives), a CCI company should be allowed to receive them (in particular but not only because a company can have part of its operations in CCI and part in the I3S.) Therefore, we believe it is of the utmost importance that the voluntary codes of conduct that will be developed for the I3S and the mandatory regulatory regime that will be imposed on CCI be compatible.

Furthermore, the relationship between CCI and I3S is not just one of overlap to be avoided. It is also an issue of:

- interconnection: CCI systems and assets may interconnect with systems and assets that provide I3S functions; and/or
- integration: while some elements of CCI systems and assets may have been custom developed, others may have been commercial-off-the-shelf (COTS) products and services designed and developed within the I3S.

To demonstrate compliance with their CCI obligations, owners and operators of CCI systems and assets should be allowed to take advantage of the cybersecurity commitments taken by the owners and operators of I3S systems and assets with which they interconnect and upon which they rely. However, we strongly caution against "regulatory creep": CCI regulatory obligations should not be imposed upon I3S technologies because they interconnect with, or are integrated into, certain CCI systems and assets. The CCI owner or operator is best positioned to understand its operational needs and assess its risk profile, and thus decide which technology and technology provider would best correspond to these operational needs and risk profile and enable it to meet its own regulatory obligations. This does not require that CCI regulatory obligations be extended to an I3S provider, whose products and services are intended to be used in a much broader array of environments.

I3S and the current "critical infrastructure" (CI)—CI, as its definition in the USA PATRIOT Act was implemented under the NIPP, covers a wide array of systems, assets and functions. The Green Paper does not address this, but there is clear overlap between CI and I3S. For example, every function of the IT Sector is currently considered CI, but the I3S also encompasses many functions of the IT Sector (and we recommend that it actually cover them all).

The risk management activities that industry and government conduct in partnership under the NIPP are not regulatory and mandatory, but voluntary and based on the same objectives of promotion of generally-accepted practices and information sharing that underpin this Green Paper. Therefore, this overlap may not be problematic if the activities proposed by the Department of Commerce for the I3S, and those conducted by the appropriate Sector-Specific Agency under the NIPP (e.g. the Department of Homeland Security for the IT Sector), are compatible and coordinated. Such compatibility and coordination could be ensured for example through the involvement of the Department of Homeland

Security in the Department of Commerce's I3S activities, and conversely through Department of Commerce participation in the IT Government Coordinating Council led by the Department of Homeland Security.

Recommendation A1—Developing and Promoting I3S-Specific Voluntary Codes of Conduct

"*The Department of Commerce should convene and facilitate members of the I3S to develop voluntary codes of conduct. Where subsectors (such as those with a large number of small businesses) lack the resources to establish their own codes of conduct, NIST may develop guidelines to help aid in bridging that gap. Additionally, the U.S. government should work internationally to advance codes of conduct in ways that are consistent with and/or influence and improve global norms and practices.*"

BSA supports the Green Paper's recommendation that NIST convene and facilitate members of the I3S to develop voluntary codes of conduct. NIST has a good track record of cooperating with industry in an open and transparent manner to leverage generally-accepted industry practices. It is clear, however, that NIST's role should be one of support, rather than control: NIST should not be setting standards and its contribution should not become a standard or code of conduct without sufficient industry validation.

BSA also supports the Green Paper's recommendation that the U.S. government work internationally to advance codes of conduct in ways that are consistent with and/or influence and improve global norms and practices.

Additionally, we would like to make an important clarification about the implementation and legal effect of voluntary codes of conduct, in reaction to the Green Paper's language on pp.12-13. Once these codes of conduct have been adopted, the Federal Trade Commission (FTC) could use its authority to police "deceptive" practices: it would enforce them against companies that committed to complying with them but are not actually living up to these commitments. This is a straightforward approach.

However, the Green Paper is ambiguous about the use by the FTC of its authority to act against "unfair" practices, which allows it to act against companies that have not taken any commitments but whose practices: cause substantial injury to consumers; violate public policy; and are unethical or unscrupulous. If the FTC were to strike down non-compliance with these codes of conduct as unfair, they would cease to be voluntary commitments and become mandatory requirements. BSA recommends that the FTC regard the codes of conduct as voluntary commitments to implement generally accepted industry practices, enforced through its deception authority.

Granting enforcement authority to the FTC should also take into account the scope of its technical expertise. In the field of cybersecurity and privacy, the FTC enforces consumer protection laws. Its technical expertise is thus limited to how businesses collect, retain, store, transfer, use and dispose of consumers' personal information. We recommend that the FTC enforce codes of conduct inasmuch as their subject matter falls within the scope of consumer privacy and cybersecurity.

Furthermore, we do not think that the FTC has adequate expertise to evaluate the more complex requirements of enterprise cybersecurity risk management and the cybersecurity implications of business-to-business (B2B) interdependencies and interconnections. Therefore, it should not be tasked with enforcing them.

Finally, it is not clear what the relationship would be between these codes of conduct and the information security requirements that Congress is considering under data security legislation.[5] They would have largely the same objectives of securing personal data, would similarly instruct companies on how to secure such data, and would both be enforced by the FTC. If such legislation were enacted, what would be the effect of these codes of conduct? BSA recommends that the FTC recognize them as safe harbors under the legislation, i.e. that a company complying with an applicable code be considered in compliance with the statute.

Are there existing codes of conduct that the I3S can utilize that adequately address these issues? Are there existing overarching security principles on which to base codes of conduct?

BSA recommends that the creation of codes of conduct leverage the principles and approach that underpin recognized industry standards for information security risk management, such as ISO/IEC 27001, the Standard of Good Practice of the Information Security Forum, or the COBIT framework created by the Information Systems Audit and Control Association (ISACA.) It is important to note, however, that broad enterprise risk management standards such as ISO/IEC 27001 encompass a large number of security controls. We should avoid any approach that leads to creating codes of conduct or standards that require implementation of the entire set of controls, but rather preserve the flexibility of each company to select the controls appropriate to its operational needs and risk profile.

Recommendation A2—Promoting Existing Keystone Standards and Practices

"*The Department of Commerce should work with other government, private sector, and non-government organizations to proactively promote keystone standards and practices.*"

"*The government should not be in the business of picking technology winners and losers; however, where consensus emerges that a particular standard or practice will markedly improve the Nation's collective security, the government should consider more proactively promoting industry-led efforts and widely accepted standards and practices and calling on entities to implement them.*"

BSA agrees with these recommendations.

We would like to make two semantic clarifications:

- "Global" and "international" standards: "international" standards could be understood by some to refer only to standards developed by organizations, such as the International Organization for Standardization (ISO), whose members are government or quasi-government organizations, such as national standards organizations. "Global" standards, on the other hand, might not have that limitative connotation and would include global industry standards. This submission will refer to "global" standards to clarify that both have value and neither should be excluded, and we recommend that the Department of Commerce embrace both models.
- "Best" vs. "generally-accepted" industry practices: we believe it is more appropriate to seek increased adoption of "generally-accepted" security practices, rather than "best" practices, which might set the bar too high and as a result receive little adoption.

[5] See for example section 2 of S 1207, the ''Data Security and Breach Notification Act of 2011'' of Sens. Pryor and Rockefeller: http://www.gpo.gov/fdsys/pkg/BILLS-112s1207is/pdf/BILLS-112s1207is.pdf

Are the standards, practices, and guidelines detailed in Appendix B[6] appropriate to consider as keystone efforts? Are there others not listed here that should be included?

The standards, practices, and guidelines detailed in Appendix B are generally good, but we would make the following comments.

Overall, we believe it is preferable that the government promote the implementation of outcome-based standards that stimulate innovation by not prescribing the use of specific technologies or methods.

PCI DSS—The PCI DSS is generally found to be overly prescriptive, expensive to implement, confusing to comply with and fairly burdensome. The prospect of some sort of government endorsement of the PCI DSS also raises concern because the standard is very specific in what technological measures it prescribes. Finally, we must be clear that it is only meant to apply to the retail payment operations of organizations that handle payment cardholder information.

NIST SP 800-53—We caution against pushing for compliance by private sector entities with standards created by and for government agencies. As we stated in our September 2010 submission in response to the Department's Notice of Inquiry[7], doing so can limit access to "the best, most innovative and therefore most secure technologies available", as well as create precedents for other governments to similarly push for private sector compliance with their own national standards. We believe it is much preferable for innovation, market access and security that globally-accepted standards – such as ISO/IEC 27001 – be leveraged. It is important to note, however, that broad enterprise risk management standards such as ISO/IEC 27001 encompass a large number of security controls. We should avoid any approach that leads to creating codes of conduct or standards that require implementation of the entire set of controls, but rather preserve the flexibility of each company to select the controls appropriate to its operational needs and risk profile.

Finally, we would add that the government should promote the adoption of security standards, practices, and guidelines that offer or fit into a layered security approach, which is generally-accepted by information security experts. Security in depth minimizes the chances that any single point of failure will result in the leak of information or the compromise of a system. Elements of layered security include protection at the data/document level, the application/operating system levels, and finally at the network/perimeter level. Government should adopt layered security for its own use and encourage its adoption by the private sector through voluntary means.

Is there a level of consensus today around all or any of these guidelines, practices and standards as having the ability to improve security? If not, is it possible to achieve consensus? If so, how?

The increased implementation of cybersecurity practices and technologies remains hampered by the lack of reliable metrics of their effectiveness. In other words, organizations are reluctant to invest in

[6] Note to BSA members: the Green Paper lists PCI DSS; NIST SP 800-53; the codes of conduct and standards that will be developed or recognized under NSTIC; IPSEC; DNSSEC; Internet routing security; web security (SSL and https); and email security (SPF and DKIM.)

[7] See pp. 6, 8, 10 of the submission.

cybersecurity because they cannot measure the return on that security investment.[8] We recommend that the National Institute of Standards and Technology (NIST) work with the private sector to develop measurements that can inform organizations' cybersecurity risk management. Another driver of the implementation of cybersecurity standards and generally-accepted practices would be to ensure that the government is among the first adopters: using the purchasing power of the government would have a very positive critical mass effect on the marketplace.

What process should the Department of Commerce use to work with industry and other stakeholders to identify best practices, guidelines, and standards in the future?

BSA recommends that NIST annually convene a dialogue open to all interested public and private sector experts, to:

a. identify security needs;
b. identify international and global industry standards and generally-accepted industry practices that meet these needs;
c. identify appropriate forums for developing needed standards and practices (when none currently exist to sufficiently meet the identified needs); and
d. review the progress made in the development of these standards and practices.

In what way should these standards, practices, and guidelines be promoted and through what mechanisms?

The Department of Commerce should use the tools it already has to promote the adoption of generally-accepted industry practices by American businesses. For example, the Hollings Manufacturing Extension Partnership (MEP) is a network of field offices in every state that advise small and medium-sized manufacturers, on a voluntary basis, on how they can expand and be more competitive. The Department of Commerce should consider how it can add cybersecurity experts to the MEP network and services. Another example is the Department of Commerce's Economic Development Administration (EDA), which also runs a network of field offices providing services to American businesses in economically distressed regions, to help them expand and be more competitive.

The Department of Commerce should also use the existing social networks of the business community, such as local Chambers of Commerce, to promote these recognized standards and generally-accepted practices.

Recommendation A4—Improving and modernizing security assurance

"*The Department of Commerce, in concert with other agencies and the private sector, should work to improve and augment conformance-based assurance models for their IT systems.*"

[8] This is a point discussed in Alan Friedman's *Economics and Policy Frameworks for Cybersecurity Risks* paper, published by the Brookings Institution and available at http://www.brookings.edu/~/media/Files/rc/papers/2011/0721_cybersecurity_friedman/0721_cybersecurity_friedman.pdf

BSA agrees with this recommendation. A key element to building trust in ICTs and securing the critical infrastructure is driving assurance into the products that make up the infrastructure. While various mechanisms exist today (standards, generally-accepted practices etc.), many of them can be expanded and improved to greatly further the goal of robust product assurance. Effective security assurance mechanisms can usefully address questions of what threats need to be considered and the degree of confidence that the product actually addresses these threats (e.g., confidence being established via an accredited third party validation of software). It may also include verifying that a product not only does what it was designed to do, but also does not do what it was not designed to do, (e.g., via insertion of malicious code or corruption of the software in some way). Security assurance typically also addresses lifecycle issues such as the security of the software development environment.

One effective mechanism to demonstrate assurance is through third party validation mechanisms that are licensed and trustworthy. As noted above (see section 4), ISO 15408, the Common Criteria, is the international standard for security assurance and has a robust construct of evaluation labs that are accredited under an international standard and certified to conduct product reviews and whose reviews are mutually recognized. Furthermore, product evaluations done against the Common Criteria are accepted in more than twenty countries. The U.S. should promote and extend the use of the Common Criteria.

In light of its international recognition, Common Criteria is at this time the hallmark of product assurance. While it is an important tool for certifying the security of information technologies, in its current form Common Criteria has not been generally applied across the marketplace, but mostly to critical products that perform security functions. The difficulty with deploying the certification more widely comes from the fact that the process is costly, and consequently products and services that are certified are significantly more expensive to produce. In some cases, however, the risks associated with the expected uses for a technology would not warrant such expense. In addition, the timeframes associated with achieving the certification are often not compatible with current market demands for product development. While there are differing views about how to reform Common Criteria, including whether or not the focus of the certification should be expanded beyond security functionality to security development processes, these are some of the reasons why Common Criteria stakeholders and government agencies continue to work to evolve it.

The challenge for policymakers and industry is to measurably increase the assurance of information technology without requiring that a certification regime like the current version of Common Criteria be made mandatory for all information technology products and services, while at the same time not drawing government into the design and development of products, or undermining the Common Criteria or international standards. We believe that while such certifications are helpful they may be too heavy handed in some cases and thus a lighter, more agile mechanism should also be available to meet different levels of need or risk. There should not be multiple disparate certification regimes.

Engineering processes used by suppliers to increase product security continue to evolve rapidly and generally-accepted security engineering practices have emerged and been compiled by groups such as SAFECode[9] and the Trusted Technology Forum[10]. These practices should be examined to see how they may be applicable in any additional framework for products that are not as critical as to warrant the use

[9] www.safecode.org
[10] www.opengroup.org/ttf

of the Common Criteria. NIST should work with industry and other agencies to undertake this examination. Any other framework should be consistent with and complementary to the Common Criteria.

Recommendation B1—Develop the right mix of incentives to promote adoption of cybersecurity best practices

"*The Department of Commerce and industry should continue to explore and identify incentives to encourage I3S to adopt voluntary cybersecurity best practices.*"

BSA agrees with this recommendation, with the caveat made on p. 6 regarding "best" vs. "generally-accepted" industry practices.

How can liability structures and insurance be used as incentives to protect the I3S?

We believe that liability limitations can be a very effective tool to incent increased cybersecurity, without requiring the expenditures of scarce fiscal resources. Importantly, liability limitations are a sliding scale of measures: without granting a complete safe harbor from any and all liability, Congress can reduce or remove the threat of certain types of liability without affecting others (e.g. punitive damages, actual damages, compensatory damages, economic or non-economic damages, etc.)

Congress can also limit liability by raising the burden of proof that rests on a plaintiff (e.g. preponderance of the evidence vs. clear and convincing evidence.)

Additionally, Congress can consider restricting standing to bring suit to certain parties, in particular by clarifying that only law enforcement agencies (such as the FTC or State Attorneys General) can bring suit, rather than private parties.

Finally, Congress should consider pre-empting state laws in favor of a unified federal liability regime, where appropriate.

Should federal procurement play any role in creating incentives for the I3S? If so, how? If not, why not?

We believe that federal procurement can play a very effective role in driving the adoption of standards and generally-accepted practices, as long as those standards and practices are industry- rather than government-created, and global rather than national.

Recommendation B2—Using security disclosure as an incentive

"*Recommendation B2a—Congress should enact into law a commercial data security breach framework for electronic records that includes notification provisions, encourages companies to implement strict data security protocols, and allows states to build upon the framework in defined ways. The legislation should track the effective protections that have emerged from state security breach notification laws and policies.*"

BSA supports the enactment of a single national framework for notification of breaches where there is a significant risk of sensitive personally identifiable information being used to cause harm.

In this regard, BSA believes that exemptions from the obligation to notify can provide powerful incentives for the adoption of stronger security measures. Specifically, we believe that notification need not be required when the information has been rendered unusable, unreadable or indecipherable to an unauthorized third party through the use of practices or methods such as encryption, redaction, access controls and other such mechanisms which are widely accepted as effective industry practices or industry standards. This exemption from the obligation to notify provides an effective incentive for organizations to adopt stronger security measures to avoid the costs associated with notification, including reputational damage and potential liability.

BSA supports the inclusion in such legislation of information security requirements that would help prevent breaches from happening in the first place, by requiring that organizations holding personal data take reasonable and appropriate technological, physical and administrative measures to protect it. It is important that these requirements not mandate the use of specific security measures, in particular specific technologies, to preserve innovation and ensure that these organizations implement the most appropriate measures to mitigate the risk they face.

BSA sharply disagrees, however, with the Green Paper's recommendation that federal legislation should create a "floor" above which states could add requirements. An essential driver for federal legislation has precisely been that 46 states, the District of Columbia, Puerto Rico and the U.S. Virgin Islands had created a patchwork of breach notification laws. This has led to a compliance nightmare for businesses. As businesses may in good faith comply in different ways, this in turn creates confusion for consumers who receive notices from a multiplicity of sources.

For example, most state laws exempt encrypted data from the obligation to notify because they rightly consider that such a breach does not create a risk of harm. However, some jurisdictions including the District of Columbia, Wisconsin and New Hampshire require notification even when the data was encrypted. This jeopardizes the legal benefit for businesses of encrypting data. It also creates the likelihood that residents of other states will get notified even if their data was encrypted, and thus even if they are not at risk.

The various bills under discussion in Congress in the last few years[11] provide an effective and comprehensive framework for securing data and for notifying interested parties when it has been breached. This legislation should establish a single national framework that facilitates interstate and online commerce, rather than impede it by allowing continued divergences in legal requirements.

"*Policy Recommendation B2b—The Department of Commerce should urge the I3S to voluntarily disclose their cybersecurity plans where such disclosure can be used as a means to increase accountability, and where disclosure of those plans are not already required.*"

We are very skeptical of the value of such disclosures, and actually believe they would weaken rather than strengthen cybersecurity.

[11] See in particular in the 111th Congress HR 2221, and in the 112th Congress S 1207 and S 1151.

We believe that companies should not be expected or required to make disclosures that would be so detailed that they would communicate information about their exact security posture, which could be of use to malicious actors. On the other hand, a plan that is summarized at too high a level provides no value to those who will try to assess it.

Rather, any disclosure should be limited to a statement that a company complies with e.g. specific higher level enterprise risk management standards.

Recommendation B3—Facilitating Information Sharing and Other Public/Private Partnerships in the I3S to Improve Cybersecurity

"*The Department of Commerce should work with other agencies, organizations, and other relevant entities of the I3S to build and/or improve upon existing public-private partnerships that can help promote information sharing.*"

Sharing information about threats, vulnerabilities and their consequences greatly contributes to more effective collective risk mitigation, and thus improves cybersecurity. Many private sector companies, in particular in the information technology sector, have invested important resources into information sharing, in particular by dedicating personnel to gathering and analyzing the data and to participating in collaborative information sharing mechanisms such as the IT Information Sharing and Analysis Center (IT ISAC.) in fact, information sharing has largely taken place within the framework of sector-specific information-sharing mechanisms, such as the ISACs. 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.

However, government does have an important role in fostering the effectiveness of information-sharing mechanisms. For example, it can increase market-based incentives for sharing information, 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. One example of such an incentive would be a safe harbor from liability, so that information that is shared about an incident cannot be used to seek damages against the company that experienced the incident. We believe that, with the right privacy protections in place, encouraging companies to share information about threats and vulnerabilities without fear of exposing themselves to liability can significantly contribute to improved cybersecurity.

An important objective of efforts to improve information sharing 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.

Information sharing also needs to evolve with modern threat patterns. For example, valuable information could be shared not just about inbound attacks and technical vulnerabilities, but also about unauthorized outbound traffic: advanced persistent threats (APT) are not successful until data is exported from the system, so preventing outbound connections to unauthorized URLs and websites can be an effective defense. Sharing such information side-steps some of the current legal barriers to sharing, since no proprietary or privacy-protected 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 accomplish 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 comply with the President's unequivocal commitment that "*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.*"[12]

Recommendation C2—Creating and Measuring I3S Cybersecurity Education Efforts

"*The Department of Commerce should support improving online security by working with partners to promote the creation and adoption of formal cybersecurity-oriented curricula in schools. The Department of Commerce should also continue to increase involvement with the private sector to facilitate cybersecurity education and research.*"

BSA supports this recommendation.

What new or increased efforts should the Department of Commerce undertake to facilitate cybersecurity education?

Efforts to improve U.S. cybersecurity over the long term must include measures that will lead to the education and development of more individuals with such skills. For example, government should

[12] President Barack Obama, Release of the Cyberspace Policy Review, May 29, 2009.

significantly increase funding for cybersecurity college scholarships and should work actively with computer science departments to offer a cybersecurity curriculum. Also, we could use the existing Cyber Corps program to create an Elite Cyber Corps Alumni group (e.g. the top 10% of students who go through the program) and design a specific set of benefits for them (training by venture capitalists on how to create a startup company, training on how to be a CISO, networking with top security professionals). Furthermore, we could enhance the existing Scholarship for Service Program by significantly increasing the number of participating schools and making certain they include the top Computer Science programs (e.g. Berkeley, Purdue, MIT). There are now 122 institutions in the NSA/DHS Center of Academic Excellence in Information Assurance Education (CAE-IAE) program, and the evaluation criteria ensure a consistent level of information assurance education at accredited institutions. We believe this program should be supported and grown, with sufficient follow-on employment opportunities for graduates, in both government and critical infrastructure organizations.

We recognize that merely producing more "cybersecurity professionals" will not be sufficient to address key risks in cyberspace; we must also tackle how the infrastructure is developed and built. It is our concern, that many people who design and build ICT systems are not adequately educated and trained to understand:

- ICT-based systems will be attacked and subverted.
- IT is "infrastructure technology" as much as "information technology" – given the degree to which all critical infrastructure rely on an IT backbone – and must be designed and built accordingly.

Cybersecurity professional training needs be broadened beyond just those individuals who would self-identify as cybersecurity specialists. For example, project managers need to be taught to understand the risks associated with heavily networked environments and how to analyze risk and make smart risk management decisions. Management and senior leadership must also understand how to navigate the new, increasingly complex interconnected system risk environment.

It is our view that cybersecurity initiatives must focus on how to make fundamental changes to the educational system so that anyone in a computer or computer-related disciplines understands that he or she is building infrastructure that will be attacked, and that systems must be designed and built with both proactive security functionality and "defense" in mind. Accordingly, computer-related educational disciplines must include security throughout the entire curricula in much the way companies embed secure development processes through an entire product lifecycle. Similarly, management education needs to include the study of systemic risks associated with networked systems. This is increasingly important as cloud computing accelerates.

Recommendation C3—Facilitating Research & Development for Deployable Technologies

"*In cooperation with other agencies through the Federal Networking and Information Technology Research and Development (NITRD) framework, the Department of Commerce should begin to specifically promote research and development of technologies that help protect I3S from cyber threats.*"

BSA cautions against directing government-funded R&D towards short-term technological and cybersecurity needs. As a general rule, BSA recommends that the government focus its own cybersecurity R&D efforts on long-term and basic research. We believe the government should be

involved in applied R&D only if the technological solution that is sought is not commercially available, and its absence creates a measurable security gap. In most cases, when government agencies seek to develop specific technologies, we are concerned that they do not check beforehand whether commercially available solutions provide the same or an equivalent capability. We recommend requiring federal agencies to ascertain whether or not commercial solutions exist—or could be readily adapted—before they invest in an R&D project to develop equivalent capabilities. This would allow the government to better leverage its limited resources.

Recommendation D1—Ensuring Standards and Practices are Global

"*The U.S. government should continue and increase its international collaboration and cooperation activities to promote cybersecurity policies and standards, research and other efforts that are consistent with and/or influence and improve global norms and practices.*"

BSA supports this recommendation. The International Strategy for Cyberspace published in May 2011 provides a great framework for such international engagement. It is important that the U.S. Government devote sufficient resources to its implementation. In particular, we think that the Department of Commerce has an important role to play through its network of U.S. Commercial Service officers stationed around the world. It is also important that the U.S. Government coordinate closely with industry in the implementation of this strategy.