BSA®
BUSINESS SOFTWARE ALLIANCE

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

p 202/872.5500
f 202/872.5501

September 20, 2010

Jon Boyens
Associate Director & Standards Coordinator, Manufacturing Industries
International Trade Administration
Office of Technology and E-commerce
U.S. Department of Commerce

Dear Mr. Boyens:

On behalf of the members of the Business Software Alliance (BSA)*, it is my pleasure to send you the attached BSA submission in response to your Notice of Inquiry regarding cybersecurity, innovation and the Internet economy (federal register docket No: 100721305-0305-01.)

We commend the Department's continuing recognition of the importance of the Internet to the American economy and to our way of life in the 21st century. We are delighted that the Department conducted this Inquiry into the nexus between innovation and cybersecurity. We believe the Department's mission – advancing economic growth and jobs and opportunities for the American people by helping make American businesses more innovative at home and more competitive abroad is right on target. The Department's extensive experience through the National Institute of Standards and Technology (NIST), the International Trade Administration (ITA) and the National Telecommunications and Information Administration (NTIA) working with the industry make the Department the natural champion of innovation and the digital economy in cybersecurity policymaking.

We look forward to continuing to work closely with the Department in this endeavor.

Sincerely yours,

Katherine B. McGuire
Vice President of Government Relations

* The Business Software Alliance (www.bsa.org) is the world's foremost advocate for the software industry, working in 80 countries to expand software markets and create conditions for innovation and growth. Governments and industry partners look to BSA for thoughtful approaches to key policy and legal issues, recognizing that software plays a critical role in driving economic and social progress in all nations. BSA's member companies invest billions of dollars a year in local economies, good jobs, and next-generation solutions that will help people around the world be more productive, connected, and secure. BSA members include Adobe, Altium, Apple, Autodesk, AVEVA, AVG, Bentley Systems, CA Technologies, Cadence, Cisco Systems, CNC/Mastercam, Corel, Dassault Systèmes SolidWorks Corporation, Dell, HP, IBM, Intel, Intuit, Kaspersky Lab, McAfee, Microsoft, Minitab, PTC, Progress Software, Quark, Quest Software, Rosetta Stone, Siemens, Sybase, Symantec, Synopsys, and The MathWorks.

Department of Commerce Notice of Inquiry (NOI) regarding Cybersecurity, Innovation and the Internet Economy

Submission of the Business Software Alliance (BSA)

September 20, 2010

The Business Software Alliance (www.bsa.org) appreciates the Department's continuing recognition of the importance of the Internet to the American economy and to our way of life in the 21st century, as most recently evidenced by its formation of the Internet Policy Task Force. We welcome this opportunity to respond to the Department's Notice of Inquiry on Cybersecurity, Innovation and the Internet Economy.

BSA is the world's foremost advocate for the software industry, working in 80 countries to expand software markets and create conditions for innovation and growth. Governments and industry partners look to BSA for thoughtful approaches to key policy and legal issues, recognizing that software plays a critical role in driving economic and social progress in all nations. BSA's member companies[1] invest billions of dollars a year in local economies, good jobs and next-generation solutions that will help people in the United States and around the world be more productive, connected and secure.

We see firsthand the reality of cybercrime around the globe – both the challenges and the opportunities for progress. BSA has been helping to promote and strengthen cybersecurity for almost 20 years.

We led the effort in the 1990's to permit the use and export of encryption products. Early in the new millennium, BSA focused on advancing measures that individuals and businesses should take to protect themselves by convening industry roundtables and developing best practices. BSA has strongly supported efforts to have the government do more to protect its own networks and has spearheaded efforts to find ways for the private sector and government to voluntarily share information. We have worked hard to enact new laws against cybercrime. BSA also recognized early on that given the threat to computer systems in and outside the United States from attackers outside the United States, true cybersecurity required international efforts. We supported adoption of the Council of Europe Convention on Cyber Crime and we have pushed for implementation in countries in Europe and Asia. Earlier this year BSA issued a 12 point roadmap for global cybersecurity.[2]

Innovation is the cornerstone of the software and hardware industry. Our industry sprung from technological innovation, it continues to thrive from it and the security of its products and services depends on it. BSA is pleased that the Department is conducting this Inquiry into the nexus between innovation and cybersecurity. We believe the Department's mission – advancing economic growth and jobs and opportunities for the American people by helping make American businesses more innovative at home and more competitive abroad – as well as its extensive experience through the National Institute of Standards and Technology (NIST), the International Trade Administration

---

[1] BSA members include Adobe, Altium, Apple, Autodesk, AVEVA, AVG, Bentley Systems, CA Technologies, Cadence, Cisco Systems, CNC/Mastercam, Corel, Dassault Systèmes SolidWorks Corporation, Dell, HP, IBM, Intel, Intuit, Kaspersky Lab, McAfee, Microsoft, Minitab, PTC, Progress Software, Quark, Quest Software, Rosetta Stone, Siemens, Sybase, Symantec, Synopsys, and The MathWorks.

[2] Available at http://www.bsa.org/country/News%20and%20Events/Calendar/2010/~/media/Files/Policy/Security/CyberSecure/Cybersecurity_Framework.ashx

(ITA) and the National Telecommunications and Information Administration (NTIA) working with the industry, make the Department the natural champion of innovation in Administration cybersecurity policymaking.

We believe that we must do everything we can to advance innovation, for two fundamental reasons.

First: innovation is key to greater cybersecurity. Cybersecurity is a fast-paced race, in which we must stay ahead of cybercriminals who adapt constantly. Cybersecurity policy should maximize the ability of organizations to design, develop and deploy the widest possible choice of cutting edge cybersecurity solutions.

Second: innovation is key to U.S. economic growth. The software and related services sector employs 1.7 million people in the U.S.,[3] in jobs that pay twice the national average ($85,600 per year.)[4] We add more than $261 billion in value to the U.S. GDP,[5] and we grow much faster than the rest of the economy (e.g. 14% growth in 2007, vs. 2% for the rest of the economy.)[6] U.S.-based software companies are world leaders: 65% of the PC software units in service worldwide in 2008 were from U.S.-based companies,[7] and the U.S. packaged-software industry contributed a $37 billion surplus to the U.S. trade balance in 2009.[8]

We see the issues of cybersecurity and innovation as complementary and highly interdependent. These comments discuss several of the specific issues raised by the NOI and provide various recommendations to leverage the power of innovation to increase our Nation's cybersecurity. It is important to keep in mind two fundamental characteristics of the networked world as the Department considers ways to improve cybersecurity and encourage innovation: First, cyberspace is global, and no single country or company can succeed alone—all must work together. Second, the networked world is diverse and dynamic. One size solution does not fit all, either at a static moment in time or as threats, vulnerabilities, consequences, or probabilities change.

1. Raising Awareness

Continuous Public education and awareness

BSA believes that efforts can be made in the United States to further educate and raise awareness of the public – home users, school-age children and small businesses in particular – about "cyber hygiene", and "safe" and "ethical" computing. This should be done as part of a national-level program that is sustained over time; a permanent educational effort rather than a temporary campaign. In other words, cybersecurity practices for the general public must become 'second nature" in the digital age.

This includes education about software piracy, because many risks to the public come from the use of pirated software. In fact, the government should tap industry resources for such efforts because industry – and the IT industry in particular – has developed a great deal of educational cybersecurity material, has marketing expertise and has established channels to communicate with the public.

[3] Source: OECD, STAN Database for Structural Analysis, ed. 2008.
[4] Source: OECD, STAN Database for Structural Analysis, ed. 2008.
[5] Source: OECD, STAN Database for Structural Analysis, ed. 2008.
[6] Source: OECD, STAN Database for Structural Analysis, ed. 2008.
[7] Source: IDC.
[8] Source: Nathan Associates.

For example, BSA has a long track record of producing and disseminating educational materials on these topics.

In addition, we need to increase the cybersecurity skills of our IT workforce to a level where they become a competitive advantage for the United States in the global marketplace. Perhaps the most fundamental challenge we face in securing our national ICT infrastructure is the need of both private industry and the public sector for a larger pool of "cybersecurity personnel." An assumption of many attempts to improve cybersecurity is that there are qualified personnel available in the workforce to meet the demand for cybersecurity professionals. For example, a predicate for a government agency to assume a significantly larger cybersecurity responsibility is that the agency will be able to readily find qualified people to execute these new functions. However, qualified cybersecurity professionals are a scarce and valuable human resource. Government agencies that can find such employees often lose them to other agencies or the private sector, which may be able to offer more compensation and other benefits. The private sector similarly has difficulties finding qualified cybersecurity personnel to secure and protect their networks.

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 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.

Improved Information sharing among companies and between the private sector and government

The private sector designs, develops, owns and operates the vast majority of computer devices, systems and networks. Of course the government also operates key civilian and defense systems and networks and engages in sophisticated monitoring and analysis. Each often learns of threats and attacks. There are many examples of information sharing frameworks that work. Unfortunately, some are not fully utilized by either business or government. Key examples of information sharing mechanisms in the IT and Communications sectors are the IT-Information Sharing and Analysis Center (IT-ISAC) and the National Coordinating Center for Telecommunications (NCC.) Company members get out of the ISAC what they put into it. The FBI's InfraGard program has also shown value to members for many of its 86 chapters, but not all of them. Some of the over 70 State and Major Metropolitan Area Fusion Centers have broad private-sector membership, but others are limited to law enforcement officers.

To be useful, threat and vulnerability information needs to be specific, timely and actionable. Industry needs threat information that the government possesses that very likely would enhance its situational awareness, incident response and mitigation, and resilience. Government needs industry information on specific vulnerabilities, countermeasures, and workarounds.

The President's Information Sharing Environment (ISE) is attempting to streamline and accelerate the sharing of threat information with critical infrastructure and state and local stakeholders through several programs. ISE led the effort to reduce the over 100 Sensitive But Unclassified (SBU) markings and handling caveats in Federal department documents to a rational, consistent list of only three. DHS is developing a security clearance granting program for critical infrastructure risk managers that is not tied to NISPOM contracts. ISE is working to make a "tear line" process routine and pervasive within the Intelligence Community, so that information can be released to those that need it in a timely manner, without compromising sources and methods. The Protected Critical Infrastructure Information (PCII) program was established within DHS to provide protections for sensitive private-sector critical infrastructure information voluntarily shared with the government. Other agencies that need this kind of information for protective programs purposes must agree to equivalent information protection rules, including consequences for unauthorized disclosure. This has encouraged some valuable sharing from industry to government. The federal government should continue to explore these and other efforts.

The government could also leverage the US-CERT as a central clearinghouse for information sharing to and from industry, through Information Sharing and Analysis Centers (ISACs) and other trusted industry mechanisms.

We understand that working with industry to establish the processes and trust to share information will require overcoming persistent and systemic resistance among certain government agencies. This will not happen without engagement from government's most senior leaders.

The government agencies taking part in this information sharing will need appropriate direction, legal authority, and resources, and be assigned specific roles and responsibilities. Existing structures between government and industry (such as the sector-specific Information Sharing and Analysis Centers – ISACs – and US-CERT) may need to be adapted to conform to new trust policies and practices, but those structures provide a foundation from which to build.

If the threat and vulnerability information that is shared with industry is specific, timely and actionable, it would improve situational awareness and give the companies that receive this information the opportunity to improve the security of their operations and information networks.

Importantly, information sharing must remain voluntary. Any obligation to share data would run against the need for organizations to comply with incompatible legal requirements (such as privacy laws, wherever they are applicable), and protect their confidential information, that of their customers, trade secrets, their intellectual property, etc.

Finally, we note that "data breach" laws are not a substitute for such information sharing procedures and institutions. Such laws requiring notification of consumers about unauthorized disclosures of their personal information are all about mitigation not prevention. They are necessarily after the fact and are designed to enable victims of a breach to take action to minimize the consequences of the possible disclosure of information. Certainly such laws are important and BSA supports the enactment of federal legislation replacing the current patchwork of state laws with a single national framework. But this should be in addition to, not a substitute for, the other measures discussed above.

2. Web Site and Component Security

BSA agrees that the websites and components play a role in the overall security of cyberspace. However, we are concerned with several suggestions in this section of the Inquiry.

First, we do not think that any particular segment of the technology spectrum plays a larger role than others in improving or degrading cybersecurity. There are no "silver bullets" but rather cybersecurity comes from continually pursuing a holistic approach to cyber risk that examines and addresses the adequacy of people, process and technology against existing threats. There need to be policies and practices that incorporate administrative, physical and technological elements. We should not focus on just one of these – e.g. technology – or on one subpart – in this case, websites and components.

Second, to improve the cybersecurity of technology – whether websites, components or any other technologies – governments should maintain a policy of technology neutrality when they develop cybersecurity policies and laws. A technology neutral approach is fundamental to effective cybersecurity protection because they ensure that individuals and organizations can deploy the security measures that are necessary to mitigate the specific risks they face. Governments should not certify or designate "good" technologies, nor should they prohibit or require the acquisition or deployment of specific products or technologies, including specific hardware or software. This is the direction given to NIST set forth in the E-Government and Homeland Security Acts and there is no reason to change now (15 USC 278g-3). NIST must ensure that standards and guidelines provide for sufficient flexibility to permit alternative solutions and must use flexible, performance-based standards.

As President Obama said when he released his Administration's Cyberspace Policy Review: "*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.*" Assurance of the security of technology must be addressed through industry processes, standards and best practices. We suggest leveraging the public-private partnership under the Critical Infrastructure Partnership Advisory Council (CIPAC) to explore specific vulnerabilities or areas of concern that have multi-sector or national impact.

3. Authentication/Identity (ID) Management

BSA believes that improved use of reliable and risk-based online identity management, authentication and access control solutions that offer levels of protection commensurate with risk would make a critical contribution to greater privacy and cybersecurity.

We believe the final draft of the National Strategy for Trusted Identities in Cyberspace (NSTIC) provides a strong framework to improve the use of reliable and risk-based online identity management, authentication and access control solutions. Its success will depend on its sustained implementation over the next few years. We must ensure that the government and the private sector both play their part in this process.

Government implementations of identity management systems for online applications should leverage the significant work underway by industry-led coalitions to establish standards-based federated identity and access control standards, certification regimes, and test beds for ensuring online trusted identity systems.

4. Global Engagement

The American software and hardware industry leads the world in IT. American industry has thrived under a "build once sell globally" business model – and IT users in the United States and around the world have significantly benefited from having an open and globally interoperable Internet.

The same holds true for cybersecurity products and services. The industry has been built around industry-led voluntary global standards created in international bodies like the IETF, IEEE, and similar organizations. These standards 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.

The imposition of country-specific cybersecurity standards and market access requirements– whether they address technology development or require specific features and performance from technology products and services – breaks up the global technology marketplace into national markets. This is particularly true when these standards and requirements are developed by government agencies, rather than being industry-led. For example, governments should not require or mandate proprietary cryptographic algorithms or artificially limit the strength of encryption, but should accept publicly available, peer-reviewed algorithms.

This breakup has serious negative consequences. First, it hurts innovation by limiting the incentives for technology providers to differentiate themselves through the development of cutting edge technologies. Second, it impedes competition between vendors, which leads to less choice and higher costs. Third, it hurts cybersecurity by requiring compliance with standards that become inadequate in the face of rapidly evolving global cyber threats. Fourth, it inhibits global interoperability between systems built by different vendors. If the U.S. pushed toward creating and mandating country-specific standards, other countries would be encouraged to follow suit, with deleterious consequences in both innovation and security. The U.S. can continue to show leadership by its own adherence and promotion of international standards.

Several examples of such policies can be found in the People's Republic of China. China is aggressively pursuing policies under the banner of promoting "indigenous innovation" that are

aimed at developing national champions by restricting foreign company participation in the market and seeking to compel foreign companies to transfer technology to Chinese entities. These policies take many forms, including government procurement preferences, R&D funding, preferential tax treatment, government financing, standard-setting, certification requirements and others. Some of the measures specifically impact cybersecurity, including the following:

- **China Compulsory Certification (CCC)**—in August 2007, the China National Certification and Accreditation Administration (CNCA) announced mandatory testing and certification for 13 categories of security-enhanced technology hardware and software. The CCC is based on Chinese security standards, not on international standards such as the Common Criteria for Information Technology Security Evaluation ("Common Criteria"), ISO/IEC 15408, developed by the International Organization for Standardization (ISO). In March 2008, the CNCA announced which specific products in these 13 categories would be required to obtain the CCC mark. In April 2009, China announced it would require compliance "only" for government procurement, rather than for commercial sales to "strategic sectors." These requirements took effect in May 2010 and we are currently assessing their impact on market access.
- **Multi-Level Protection Scheme (MLPS)**— In 2007, the Chinese government announced MLPS, which applies mandatory security requirements to the development, deployment, management and use of information technology. It applies to a broad spectrum of sectors, including finance, transportation, energy, telecom and Internet, etc. While it is originally based on the "Orange Book" – a 1980's standard for the assessment of computer security controls that has been replaced by the more modern Common Criteria – MLPS includes additional requirements that are specific to China and at variance with international standards and requirements. Among the most problematic requirements of the MLPS, for products rated at level 3 and above, are: the developer and manufacturer must be Chinese companies owned by Chinese citizens; the core technology and key components of products must be based on Chinese intellectual property rights; and any product incorporating cryptographic functionality must receive approval from the Office of Security Commercial Code Administration (OSCCA), and cannot be an imported product, except with approval of the State Encryption Management Bureau (SEMB). The SEMB enforces the implementation of Chinese cryptographic algorithms, and imposes import and export licenses and requires the escrow of source code for software implementing cryptographic functionality.
- **Trusted Cryptography Modules**—China has decided to disallow the use of Trusted Platform Modules (TPMs) – chips that perform specific security tasks, such as verifying that only authorized code runs on a system – which comply with the internationally-accepted ISO standard (ISO/IEC 11889.) Instead, China is developing its own standards that will build upon, and enforce the use of, Chinese cryptographic algorithms (see above reference to SEMB).

Recently, India has also been pursuing cybersecurity-focused policies that erect market access barriers. In December 2009, the Indian Department of Telecommunications started issuing new Equipment Security Approval Regulations. The purported aim of the regulations is to address national security concerns regarding the confidentiality, integrity and availability of the Indian telecommunications infrastructure. They impose a security approval process for the acquisition of telecommunications equipment and software. The regulations also require that the technology and intellectual property of the equipment and software be transferred to Indian companies, and that source code and other product design specifications be escrowed. Additionally, the process remains unclear because the rules have not been transparently developed with, or widely disseminated to, all interested stakeholders. BSA has joined with a number of other industry groups in calling for the Indian government to suspend these policies and engage in a comprehensive stakeholder process to develop policies that address India's security needs without undermining the development of key technology sectors.

Country specific initiatives and mandates are often presented as based on national security considerations. However, equally often the requirements seem to be motivated by industrial policy and the misperception that the U.S. has similar or even more onerous regimes in place. Further, as we stated above, we firmly believe that mandating compliance with country-specific, government-developed standards, far from enhancing cyber and national security, actually undermine them by preventing technology users – government agencies, critical infrastructure owners or operators, and others – from using the best, most innovative and therefore most secure technologies available.

Importantly, as the U.S. IT industry and the U.S. government have been calling on foreign governments not to impose such country-specific, government-created cybersecurity standards, we have expressed concerned about various legislative attempts in the Congress to impose such standards in the United States. If the U.S. government were to do so, it would make it impossible to urge foreign governments not to do so.

U.S. cybersecurity policymakers must continue to champion, both domestically and internationally, the preservation of the contribution of industry-led, global standards to address cybersecurity challenges.[9]

In addition, BSA supports the government's efforts to exert leadership in international cybersecurity policymaking within legal and diplomatic forums. The ultimate goal must be to produce a globally convergent policy framework. To reach this goal, the U.S. government needs to develop, and provide sufficient resources to implement, a more comprehensive international cybersecurity strategy, and actively involve industry in its development and implementation.

5. Product Assurance

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, best 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

[9] The fact that the U.S. government should not mandate security standards does not mean it should do nothing about standards. First, the government should identify the relevant international industry-led cybersecurity best practices, and recognize and promote their use in federal systems. Second, NIST continues its excellent work to address perceived needs for standards – and does so in the right way. This is also fully consistent with the statement made by President Obama when he released his Administration's Cyberspace Policy Review: "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."

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 security engineering best practices have emerged. These best 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 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.

We strongly believe that it is in the government's interest to ensure that policies preserve and foster industry's continued ability to design, develop, produce and sell COTS technology around the world. Our industry's use of this business model yields many important benefits for agencies across the government. Our globally competitive, commercial technology industry offers to its government customers the most diverse and innovative set of solutions, at the lowest cost possible. That is why existing law requires that performance based standards and guidelines permit to the greatest extent possible the use of off-the-shelf commercially developed information security products (15 USC 278g-3).

Continuing to adopt COTS technology also is fully consistent with fundamental objectives of the Obama Administration:

- Promoting the widespread use of transformative technologies by civilian agencies;
- Maintaining the superiority of U.S. defense and intelligence agencies; and
- Remaining fiscally responsible, by relying on the R&D investments of the private sector, and thus freeing up scarce dollars for government-specific R&D.

Regulations or procurement rules would run counter to this objective and harm the global COTS model if they:

- Imposed technology-specific requirements about the integrity, reliability and trustworthiness of technology;
- Favored specific technology development models or processes;
- Were not based on transparent criteria developed in coordination with industry;

- Did not provide vendors fair opportunities to address concerns; or
- Drove divergent requirements from country to country.

6. Research and Development

First, BSA believes that we can enhance our nation's cybersecurity research and development (R&D) by strengthening incentives for the private sector to conduct R&D. In particular, we have been calling for many years for a permanent and seamless – i.e. retroactive – extension of the R&D tax credit, which expired at the end of 2009. We also have urged the alternative simplified credit be increased from 14 to 20%. This is of great importance to our entire industry and to the preservation of America's leadership position in global IT innovation.

Second, BSA strongly supports cybersecurity innovation through U.S. government-funded R&D grants and initiatives. Government support of cybersecurity R&D helps meet the country's future technological needs, helps train individuals in cybersecurity, and further develops the IT industry. The work of the Cybersecurity and Information Assurance (CSIA) Interagency Working Group (IWG) under the National IT Research and Development (NITRD) program has had good success, and offers great potential.

Third, 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.

Fourth, BSA offers the following recommendations in order to make the nation's cybersecurity R&D effort more effective:

Identify and prioritize objectives with input from the private sector: The 1961 declaration by President Kennedy that the United States would land a man on the moon by the end of the decade illustrates the usefulness of identifying and prioritizing national goals. R&D activities that contribute to reaching the national objectives should be prioritized, while others receive less support. Had individual agencies been left to create their own R&D plans outside of such a national framework, President Kennedy's goal might not have been met—certainly not so swiftly. Similarly, because the goals of the national plan should reflect the cybersecurity needs of the nation, this necessarily requires that a wide community of stakeholders play an integral role. We support NITRD's efforts to prioritize "leap-ahead" research projects to improve cybersecurity.

Ensure R&D results are disseminated within the government and with the private sector: We recognize that certain governmental R&D activities need to remain classified. However, we have seen in this field, as in other aspects of national and homeland security, a tendency to over-classify. In cybersecurity R&D, over classification has had the negative effect of preventing other agencies from benefiting from the technological advances produced by classified R&D projects. We also recommend that the federal government improve its sharing with the private sector of the innovations generated by cybersecurity R&D conducted by federal agencies. Too often, those innovations are not shared with industry, where they could benefit the Nation as a whole through productization, even with licensing conditions that appropriately reward the agency in question.

Harness the creativity of the private sector: Companies often receive federal funding because they submitted proposals in response to a competitive federal solicitation. We believe this mechanism should continue to represent a large part of the federal R&D funding. Sometimes, however, companies are awarded funding as a "sole source" grantee because they had pro-actively suggested to the agency the research topic or project. We believe it would be appropriate to facilitate this type of support: we believe a mechanism should be found that would make it easier for agencies to act upon such suggestions, while not running afoul of legitimate concerns regarding the fairness of the award process. This would encourage more companies to suggest promising avenues for cybersecurity innovation to the federal government.

Improve IP protection to encourage greater participation: An obstacle to greater industry participation in federally funded cybersecurity R&D is the status of the intellectual property (IP) it generates. We recommend that the Administration work with Congress to explore ways to make such industry participation more appealing through improved IP ownership or licensing, similar to what Congress did for small businesses, non-profits and universities through the Bayh-Dole Act in 1980.

7. Incentives for Evolving Cyber-Risk Options and Cybersecurity Best Practices

Every business has strong incentives to protect its high value assets and those of its customers. This includes the value of its brand, and supply chains. These incentives are affected by the particular product or service they offer, geographic markets, competition, innovation, regulatory structure, and other influences. There is no single answer to a question on incentives.

The greatest incentive the government can provide is to share specific, actionable threat information with affected businesses and sectors, and its view regarding cascading or national-level consequences of incidents. When business owners and operators are aware of risks to their businesses and customers, they will act to protect the operation, product, or service at risk.

For small and medium-sized businesses outside the scope of "critical infrastructure and key resources," best practices available at sites like www.staysafeonline.org, www.onguardonline.gov, and www.sba.gov/beawareandprepare/cyber.html are useful. Government could continue raising awareness and thereby changing behavior by supporting these ongoing public-private efforts.

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.