The Software Alliance

BSA

April 8, 2013

VIA EMAIL
cyberframework@nist.gov

The Honorable Patrick D. Gallagher
Under Secretary of Commerce for Standards and Technology
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Re: Developing a Framework to Improve Critical Infrastructure Cybersecurity

Dear Mr. Gallagher,

BSA | The Software Alliance (BSA) appreciates this opportunity to provide comments to the National Institute of Standards and Technology (NIST) on the development of a Framework to improve critical infrastructure cybersecurity. BSA is the leading advocate for the global software industry before governments and in the international marketplace.[1] It is an association of world-class companies that invest billions of dollars annually to create software solutions that spark the economy and improve modern life.

BSA commends NIST on its efforts to date regarding the Framework, including its outreach to stakeholders, as well as the April 3rd conference it held relating to the development of the Framework. NIST's recognition of existing private sector efforts, both within and across sectors, is key to a successful cybersecurity strategy. Cybersecurity is a shared responsibility: no company, country, or government can go it alone if we are to successfully combat the increasing threats and risks in the area. Addressing risks in isolation, forcing a "one size fits all" approach, or bypassing industry leadership and progress in the current cyber environment would cause irreparable harm and hamper innovation. Consequently, NIST's proposed approach of focusing on voluntary consensus standards and industry best practices, as well as assuring consistency with voluntary international consensus-based standards, is reassuring.

In the Request for Information (RFI), NIST has stated that the Framework will not "prescribe particular technological solutions or specifications." BSA supports a technology-neutral approach: we strongly believe that the Framework should not call for the regulation of technology or other policies that favor one technology, system architecture, or business model over another. The Framework should not require the acquisition or deployment of specific products or technologies, including specific hardware or software.

[1] BSA's members include: Adobe, Apple, Autodesk, Bentley Systems, CA Technologies, CNC/Mastercam, Dell, IBM, Intel, Intuit, McAfee, Microsoft, Minitab, Oracle, PTC, Rosetta Stone, Siemens PLM, Symantec, and The MathWorks.

Maintaining technology neutrality also requires, as the introduction to the RFI recognizes, that the Framework should include only “technology-independent standards, guidelines and best practices.” This will ensure that no specific technology is imposed as a requirement. Instead, technology providers and users can focus on managing risk and selecting specific security measures – including specific technologies – from competing and evolving solutions tailored to their specific needs. While we understand that some RFI respondents may advocate for a technology-specific approach, we appreciate NIST’s commitment to technology-neutrality.

We also agree with the statements by Under Secretary for Standards and Technology and NIST Director Patrick D. Gallagher in his remarks opening the April 3rd conference that NIST “will not be seeking to tell industry how to develop your products.” Ensuring that the government does not interfere with the design, development, manufacture, and supply chain management processes of the private sector is the best way of ensuring that public policy strengthens innovation by leveraging the private sector’s investment in security innovation.

Such technology-neutral policies are critical to effective cyber protection as they preserve the ability of organizations to develop and deploy security measures that mitigate the specific cyber risks they face. BSA supports NIST’s and this Administration’s commitment to identify norms and goals that give guidance but do not prescribe particular tools and technologies that could hinder the ability of government and the private sector to utilize the most innovative solutions in the face of a constantly evolving threat landscape.

As the Framework is developed and implemented, BSA believes the government must assess how it will fulfill its cybersecurity responsibilities so as to assist the various sectors in their efforts to secure their systems and networks. Specifically, the government should evaluate the following:

- The government’s capability to build trust with the private sector to assure that whatever recommendations come out of the Framework and related processes add value to ongoing efforts;
- The government’s efforts to promote innovation, both on cybersecurity and in the broader technology sphere;
- The government’s ability to enable critical infrastructure owners and operators to implement the security measures that are most appropriate to mitigating the specific risks they face; and
- The government’s recognition of the borderless nature of the Internet, the global economy and cyber threats.

One area that is of concern to BSA is how the RFI process and resulting Framework will relate to the Department of Homeland Security’s (DHS) announced working groups on cybersecurity. In particular, it is imperative that the two processes are coordinated to avoid divergent and conflicting outcomes and recommendations. Given the number of critical infrastructure sectors already working with DHS, it is essential that the guidance and recommendations of DHS and NIST are coordinated and consistent with each other and with ongoing private sector efforts. BSA appreciates the explanation that NIST and DHS provided at the April 3rd event regarding the relationship between the two agencies: we understand that a Memorandum of Understanding (MOU) is in place to assure a cohesive and comprehensive effort between the two agencies.

We recommend that NIST and DHS, as they continue to implement the Executive Order on cybersecurity, clarify their cooperative efforts and how such efforts will impact critical infrastructure sectors, owners, and operators. In particular, we would recommend that NIST and DHS ensure that the DHS working group processes and timing are conducted in such a fashion that they can be effectively informed by the NIST process. Should the working groups conduct their work without sufficient information on what organizations have recommended to NIST as part of the RFI, the agencies risk having disparate and potentially conflicting products that do not adequately represent industry views and experiences.

Below, please find BSA's specific answers to each of the question posed in the RFI.

Current Risk Management Practices

The first set of questions in the RFI requests information on how organizations assess risks and what frameworks, standards, guidelines, and best practices are used by particular entities in their risk management practices.

1. What do organizations see as the greatest challenges in improving cybersecurity practices across critical infrastructure?

The private sector faces several challenges in improving cybersecurity practices across critical infrastructure.

First, cost and complexity complicate efforts to implement effective cyber practices and technologies. Bad actors come in a variety of forms – from organized crime to nation-states to rogue actors to hacktivists – creating new security risks every day for companies. As companies use innovative technologies (*e.g.*, smart phones, cloud) and practices (*e.g.*, bring your own device), their security needs become more complex and require great sophistication. Consequently, it is not a lack of commitment or ability that prevents companies from improving cybersecurity but rather the dynamic and changing nature of technologies and business models and needs. There is little question that critical infrastructure systems will be attacked and subverted. As critical infrastructures rely on a resilient IT backbone to function, and that managers understand the systemic risks associated with networked systems.

Second, critical infrastructure owners and operators are often insufficiently aware of the specific threats they face. As a result, they are unable to appropriately defend themselves against these threats. That is why we recommend that the government share more actionable cyber threat information with the private sector.

Third, there is a significant need for a larger cybersecurity workforce. Improved cybersecurity is not possible without a qualified and trained workforce. Without one, the US will be at competitive disadvantage in the global marketplace. In order to meet this challenge, the US must invest increased funding in cybersecurity education programs. BSA advocates for policies to produce and retain highly skilled workers by strengthening enrollment in advanced science, technology, engineering, and math (STEM) programs and by advancing common-sense reforms that allow high-skilled immigrants to meet technology workforce needs and have a path to obtain permanent residency status.

2. What do organizations see as the greatest challenges in developing a cross sector standards-based Framework for critical infrastructure?

It is important to recognize that not all targets are equal and not all threats present the same risk. Security protections do not necessarily transfer between sectors. Businesses must be able to implement the security measures, including using appropriate best practices, technologies, and standards that are most appropriate for mitigating the specific risk that they face.

At its core, the Framework should avoid including flawed requirements that would adversely affect those sectors that have strong policies, procedures, and standards in place. At the same time, it must be careful to not make the mistake of transferring sector-specific policies, practices, and standards to other sectors that may not be similarly situated. A holistic Framework that promotes security but remains flexible is key to any successful cybersecurity approach. If the Framework formulates baseline approaches that are appropriate within specific sectors, then NIST should strive to ensure that its recommendations are not too prescriptive and do not implicitly or explicitly require specific technologies or tools that can easily become outdated or may have problems replicating success across sectors.

3. **Describe your organization's policies and procedures governing risk generally and cybersecurity risk specifically. How does senior management communicate and oversee these policies and procedures?**

The IT industry is constantly evaluating the policies and procedures that govern risk, including cybersecurity risks. Executives in companies are increasingly holding their organizations accountable for implementing practicable and effective practices and controls. BSA supports a comprehensive approach to cyber risk that is constantly evaluating, examining, and addressing 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 elements.

Many of BSA's members are filing specific comments detailing the specific policies and practices that their companies use in their day-to-day business operations

4. **Where do organizations locate their cybersecurity risk management program/office?**

BSA member companies understand that cybersecurity risk management must occur at all levels of their business operations. Cybersecurity is woven into the fabric of all our companies' operations. Filings by individual BSA member companies provide specific examples of how risk management is addressed on a company-by-company basis.

5. **How do organizations define and assess risk generally and cybersecurity risk specifically?**

The IT industry has been on the forefront of defining and assessing cybersecurity risks. Our companies have long understood the need to protect cyberspace and the networks and systems that underlie so much of US critical infrastructure. Our sector uses a top-down and functions-based approach to assess and manage risks to promote the IT infrastructure‘s assurance and resiliency, and to protect against cascading consequences based on the sector‘s interconnectedness and the critical functions' interdependencies.

6. **To what extent is cybersecurity risk incorporated into organizations' overarching enterprise risk management?**

Cybersecurity risks, given the nature of the sector, inherently are incorporated into BSA member companies' enterprise risk management efforts. Security risk related to the operation and use of information systems is just one of many components of organizational risk that senior leaders/executives address as part of their ongoing risk management responsibilities. As NIST has recognized, "effective risk management requires that organizations operate in highly complex, interconnected environments using state-of-the-art and legacy information systems—systems that organizations depend on to accomplish their missions and to conduct important business-related functions."[2] We agree with NIST that managing information security risk is not an exact science. Companies are focused, however, on assuring that cyber risks are addressed across organization, mission/business process and information systems.

7. What standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational, and technical levels?

As noted previously, BSA firmly believes that the Framework must be "technology neutral" and agree with NIST's assertion in the RFI that it is taking such an approach. It is critical that the US government not certify or designate technologies as "good" or "bad." Nor should the Framework require the acquisition or deployment of specific products or technologies, including specific hardware or software.

BSA firmly supports the RFI's assertion that the Framework should include only "technology-independent standards, guidelines and best practices." By focusing on outcomes, the government can best recognize that critical infrastructure owners and operators must have the flexibility to manage their unique risks in a manner that allows for the implementation and, when necessary, changing of best practices and controls. We urge NIST to remain committed to a technology-neutral approach as it develops the Framework.

In understanding best practices, standards, and tools, the software industry has worked closely with DHS to assess the risks to the sector. The NIPP and IT-SCC have been vital in this effort. While many of BSA's members are filing specific comments detailing their individual practices, there are a number of enterprise controls that some of our companies have indicated that they employ for enterprise compliance and risk management. Among these are the following:

- SANS 20 Critical Security Controls
- IIA & AICPA IT General Computing Controls
- COBIT
- ISO 27000 series
- ISO 15408

Frameworks such as ISO, COBIT, SANS & ITIL are useful because they do the following:

- Organize security and control objectives into logical groupings;
- Provide sample security and control objective language;
- Provide sample security and control implementation guidance;
- Place emphasis on risk management, governance and good IT service management; and
- Allow us to adjust and refine the security and control objectives and implementations based on our business methods, technology architectures, and risk management approach.

8. What are the current regulatory and regulatory reporting requirements in the United States (e.g. local, state, national, and other) for organizations relating to cybersecurity?

[2] *Managing Information Security Risk: Organization, Mission, and Information System View* (NIST Special Publication 800-39, March 2011), http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

Many BSA member companies are public companies that are required under the disclosure guidelines issued by the staff of the Securities and Exchange Commission's Division of Corporation Finance to disclose risks related to cybersecurity, including past incidents, future risks, and any foreseeable effects that cybersecurity breaches might have on a company's financial condition.[3]

To the degree that our member companies maintain personally identifiable information of customers, we are very cognizant of the Federal Trade Commission's enforcement actions relating to data breach and data security. The FTC's assessments on whether companies' assertions relating to security and privacy are "unfair or deceptive" are followed closely by our industry.

9. What organizational critical assets are interdependent upon other critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors?

As IT companies, BSA member companies are dependent on the power generation, transmission, and distribution elements of the energy sector.

10. What performance goals do organizations adopt to ensure their ability to provide essential services while managing cybersecurity risk?

BSA members focus on operations – risk mitigation, incident response, and information sharing – to ensure their ability to provide essential services while managing cybersecurity risks. Many BSA members are filing specific comments detailing their unique performance goals.

11. If your organization is required to report to more than one regulatory body, what information does your organization report and what has been your organization's reporting experience?

Many BSA members are filing specific comments addressing how their individual companies are affected by any reporting requirements relevant to their organizations.

12. What role(s) do or should national/international standards and organizations that develop national/international standards play in critical infrastructure cybersecurity conformity assessment?

ISO and IEC, and ANSI as the US representative to ISO and IEC, have been active in critical infrastructure cybersecurity conformity assessments. In general, national/international standards and organizations that develop national/international standards could play an important role in conformity assessments. As NIST looks at conformity assessments in the cybersecurity space, BSA urges it to not employ overly stringent conformity assessment and testing mechanisms that could hamper innovation or affect the United States' global positioning. Rigid conformity assessments are not effective in managing the risks associated with cybersecurity and badly implemented third-party certification systems can inadvertently limit the flexibility and evaluative mechanisms needed to have a truly strong cybersecurity framework.

A useful example of industry-supported, international, standard-based conformity assessment is the Common Criteria. Under the Common Criteria, a product evaluation conducted by an

[3] *See CF Disclosure Guidance: Topic No. 2: Cybersecurity (October 13, 2011), http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.*

independent laboratory in one participating country is recognized by any other country that is a member of the Common Criteria Recognition Arrangement (CCRA.)

Use of Frameworks, Standards, Guidelines, and Best Practices

1. What additional approaches already exist?

As directed by the Executive Order, the Framework should first and foremost be based upon industry-led, internationally acceptable standards. These standards not only underpin the global IT ecosystem, but contribute to cybersecurity by spurring development and use of innovative and secure technologies. Governments should never mandate compliance with country-specific cybersecurity standards, especially standards developed by government agencies. Such mandates cut off a country's access to innovative, cost-effective, secure, and interoperable security technologies. Imposition of country-specific cyber standards and market access requirements breaks up the global technology marketplace. This is particularly true when standards and requirements are developed by government agencies, rather than industry.

The IT software 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. In addition, as noted above, a number of BSA members use documents produced by ISO, SANS, COBIT, and ITIL, among others.

In addition, many BSA members comply with ISO 15408, more widely known as the Common Criteria. In its current form, the Common Criteria has been mostly applied to critical products that perform security functions. Its value comes from the fact that it is the only international, industry-supported, standard-based conformity assessment for product assurance. Under the Common Criteria, a product evaluation conducted by an independent laboratory in one participating country is recognized by any other country that is a member of the Common Criteria Recognition Arrangement (CCRA.)

2. Which of these approaches apply across sectors?

This approach of industry-led, internationally acceptable standards applies across sectors. In addition, any Framework, standards, guidelines, and best practices, as noted earlier, that are technology-neutral and recognize that a one-size-fits-all approach is not practicable for cybersecurity applies well across sectors. In addition, built-in safeguards must exist to ensure flexibility across and within sectors with regard to specific cybersecurity solutions, processes, and procedures.

3. Which organizations use these approaches?

A number of organizations use the controls and standards described above. It is worth noting how each of the documents identified above assist companies in their cybersecurity efforts:

- **ISO 27000 Series** provides an internationally recognized set of control objectives and control statements with supporting guidelines and risk management framework.

- **Common Criteria** is applied through a robust network of independent evaluation labs that are accredited under the criteria to conduct product reviews that are accepted in more than two dozen countries.

- **SANS 20 Critical Security Controls** provides guidance on security & control objectives and implementations that have been demonstrated to be effective in both private industry and the public sector.

- **COBIT** provides an internationally recognized set of control objectives and control statements with supporting guidelines and risk management framework. In addition, COBIT is well recognized and respected in the IT Audit community.

- **General Computing Controls** are well aligned with Risk Management, Governance and good IT Service Management and provide for a risk management approach that include flexibility to design controls appropriate to the business, technology architecture and business risk tolerance.

- **ITIL** (Information Technology Infrastructure Library) is a very good framework for IT service governance developed by the British government and well recognized internationally. While ITIL is not specifically focused on information security, good IT governance and service operation is a critical underpinning to information security. Note, ITIL is also closely related to the General Computing Controls, but ITIL has more of a business focus whereas the General Computing Controls are more audit focused.

4. What, if any, are the limitations of using such approaches?

While not cited above, PCI-DSS and NIST SP-800-53/FISMA standards are often mentioned by other organizations. These prescriptive technical standards are useful as a reference but tend to be cumbersome and inflexible when applied as a direct requirement. This can result in specific technical implementations to apply controls that may not make good business sense based on the business scenario and the risk profile of the business and technology activities. Specifically:

- **PCI-DSS** is highly prescriptive in technology solutions to address control objectives, is costly to implement and verify, and has been widely criticized as ineffective at achieving security objectives. It does have utility as a reference or sample for how to build technical implementations to support desired control objectives.

- **NIST SP-800-53 / FISMA** is prescriptive and has a strong process and procedure orientation that is not easily scalable to diversified businesses of various sizes, business models and risk management approaches. In addition, while the NIST standards and guidelines are well thought out for a veteran security professional, they are difficult to consume for the typical business technology leader or analyst. This results in what could be very good guidance being viewed as a barrier rather than an enabler and causes security teams of businesses that adopt NIST to invest considerable effort to make the NIST guidelines consumable for the rest of the business.

5. What, if any, modifications could make these approaches more useful?

In order to successfully use current approaches, BSA recommends the adoption and consolidation of existing frameworks that meet the following three criteria:

- Are based on a risk management approach;
- Are based on analysis of real world data and experience to identify control objectives and guidelines that have been shown to be effective at addressing risk; and

- Are presented and composed with a business-oriented audience in mind, with notes or appendices to deliver security and technology domain specific details

As NIST develops the Framework, it would be helpful to move toward a single framework that produces alignment and consolidation of many of the standards, guidelines, and practices described above. In addition, it would be useful to have uniform common business-oriented opportunity/risk/solution strategic framing and language.

6. How do these approaches take into account sector-specific needs?

As noted above, the more technical and prescriptive approaches are not as easily transferrable for implementation by specific sectors. The most successful approaches are those that are technology-neutral and do not require specific tools, solutions, or technologies. In addition, they are flexible enough to allow specific sectors and entities within those sectors to develop internal processes that maximize their security efforts while also enhancing their ability to operate and provide necessary services.

7. When using an existing framework, should there be a related sector-specific standards development process or voluntary program?

The IT software industry's current approach to standards development works, in part, because it is voluntary, flexible, and responsive to changing innovative needs. The IT software industry is unique as its products and services are inherently incorporated into other sectors. As such, efforts to develop cross-sector and sector-specific approaches impact our operations and efforts to support other sectors.

8. What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches?

Sector-specific agencies and related sector coordinating councils play a key role in assisting sectors to meet their specific cybersecurity needs. These entities recognize the unique nature of each sector and can provide advice tailored to the threats and vulnerabilities that an individual sector faces. Indeed, ISACs, the National Council of ISACS, sector-specific information sharing mechanisms and the National Cybersecurity and Communications Integration Center all play key roles in developing technical and operational success. In addition, BSA recommends that the Framework explore how the government can better leverage the public-private partnership under the Critical Infrastructure Partnership Advisory Council (CIPAC) to address specific threats, risks or areas of concern to various sectors.

9. What other outreach efforts would be helpful?

The most important outreach effort from the US government that could be undertaken is assuring the increased sharing of cybersecurity threat, vulnerability and risk information. The government should share specific, actionable threat information with affected businesses and sectors, including providing 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. They can utilize the right practices and standards and adjust their efforts accordingly.

Specific Industry Practices

NIST expressed interest in identifying core practices that are broadly applicable across sectors and throughout industry. Specifically, NIST requested information on the adoption of the following practices as they pertain to critical infrastructure components:

- Separation of business from operational systems;
- Use of encryption and key management;
- Identification and authorization of users accessing systems;
- Asset identification and management;
- Monitoring and incident detection tools and capabilities;
- Incident handling policies and procedures;
- Mission/system resiliency practices;
- Security engineering practices;
- Privacy and civil liberties protection.

1. Are these practices widely used throughout critical infrastructure and industry?

These practices are widely used throughout the IT industry. For example, BSA members have long supported robust and reliable risk-based online identity management, authentication and access control solutions. Unreliable identity, authentication and access controls are what often facilitate successful cyber attacks. BSA supported the National Strategy for Trusted Identities in Cyberspace (NSTIC), as it provided a strong, industry-led framework. BSA has also routinely urged the US government to 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.

Another practice area that NIST should evaluate as part of the framework is the authenticity of software. Specifically, it should evaluate the requirements that entities have in place to procure technology from authorized resellers and distributors to assure the reliability and security of software used in critical infrastructure.

2. How do these practices relate to existing international standards and practices?

Increasingly, international organizations are looking at how companies address the practices described above. Some of these efforts are helpful, as previously discussed, to assuring a comprehensive framework for evaluating sector-specific security measures that are flexible yet strong. Efforts by groups such as IETF, IEEE and similar organizations permit the use of various solutions and approaches to a variety of process and technology challenges. They actually spur the development and use of innovative and secure technologies in the identified practice areas.

Other efforts by specific nations, however, can be counterproductive. The imposition of country-specific cybersecurity standards and market access requirements disrupts global cybersecurity efforts and hurts innovation. It also increases costs, decreases the ability of companies to develop cutting-edge solutions, and inhibits global interoperability of systems and networks. Standards and practices, to truly be effective, should be industry-led, global and technology-neutral.

3. Which of these practices do commenters see as being the most critical for the secure operation of critical infrastructure?

Given the holistic nature of IT security, no single practice plays a central role in the secure operation of critical infrastructure.

4. Are some of these practices not applicable for business or mission needs within particular sectors?

The practices listed are universal in nature and are important across sectors. That said, the implementation of specific practices will vary depending on the operational and technical requirements in each sector and may even vary within a sector.

5. Which of these practices pose the most significant implementation challenge?

Those practices that are user-based present the most significant implementation challenges. Personnel-related issues, both in terms of finding qualified personnel, as well as building in contingencies and redundancies to assure that user error doesn't make systems more vulnerable, can be significant.

6. How are standards or guidelines utilized by organizations in the implementation of these practices?

Organizations regularly use standards and guidelines to implement practices. The filings by individual BSA member companies provide examples of their specific practices.

7. Do organizations have a methodology in place for the proper allocation of business resources to invest in, create, and maintain IT standards?

The filings by individual BSA member companies provide specific examples of their companies' practices.

8. Do organizations have a formal escalation process to address cybersecurity risks that suddenly increase in severity?

Companies regularly and successfully respond to cyber risks and threats. In general, BSA members have processes and procedures for incident response and reporting that are used to protect networks and information assets on a regular basis. As a part of this effort, companies have implemented specific plans to address cybersecurity risks as they arise and escalate.   The industry recognizes the need for flexibility in these plans and processes as well as the multi-dimensional nature of cyber risks that require the involvement of various parts of a company's leadership, operational, and technical teams.

9. What risks to privacy and civil liberties do commenters perceive in the application of these practices?

Privacy and civil liberties are important and should be addressed as part of security efforts. Security should reinforce privacy and civil liberties, not be balanced against them. For example, the NSTIC demonstrates how the protection of privacy can be a fundamental principle guiding the implementation and use of identity, authentication, and access controls.

10. What are the international implications of this framework on your global business or in policymaking in other countries?

The Framework must preserve the contribution of industry-led, internationally acceptable standards to global policy. These standards not only underpin the global IT ecosystem, but contribute to cybersecurity by spurring development and use of innovative and secure technologies.

The US should avoid mandates in this area as mandates can cut off access to innovative, cost-effective and valuable security technologies. As noted earlier, the imposition of country-specific cyber standards and market access requirements breaks up the global technology marketplace. This is particularly true when standards and requirements are developed by government agencies, rather than industry. If done improperly, a US government-specific framework would inhibit global interoperability between systems and encourage other countries to enact their own country-specific standards.

11. How should any risks to privacy and civil liberties be managed?

A public-private partnership for developing a Framework can inherently protect privacy and civil liberties and has advantages over a government-mandated or directed model. Companies can more readily address privacy and civil liberties concerns through transparency and privacy policies, where applicable.

12. In addition to the practices noted above, are there other core practices that should be considered for inclusion in the framework?

The filings by individual BSA member companies provide specific examples of additional practices used by individual companies.

Sincerely,

Robert Holleyman