March 11, 2016

Via CNECT-FEEDBACK-CYBERSECURITY-DSM@ec.europa.eu

European Commission
DG Communication Networks, Content & Technology
Unit H4–Trust & Security
25 Avenue Beaulieu
Brussels 1049–Belgium

Dear Commission Members:

Our organizations, which represent nearly every sector of the U.S. economy, appreciate the opportunity to comment on the European Commission's (EC's) request for stakeholders' views on cybersecurity public-private partnerships.[1] We represent many European firms that

[1] https://ec.europa.eu/digital-agenda/en/news/public-consultation-public-private-partnership-cybersecurity-and-possible-accompanying-measures

have investments and operations in the United States and have been a steadfast supporter of the transatlantic relationship. The benefits that flow from our two major economies are deeply integrated and crucial to the health of the global economy.

Some of our associations have previously taken the opportunity to offer their perspectives on the European Union's (EU's) Network and Information Security (NIS) Directive.[2] We do not attempt to answer all eight categories of questions in the consultation. Instead, our groups focus on our experiences with the joint industry-National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* (the Framework), which we think could be very useful to European authorities as they interpret and implement the directive.[3]

Embracing the Framework *approach* could advance the EU's goals for cybersecurity and a Digital Single Market (DSM).

There is broad consensus in U.S. industry that the Framework is a sound baseline for businesses' cybersecurity practices, especially internationally, and has the added benefit of being accessible to nontechnical professionals. Our organizations have recently communicated to NIST that as Framework stakeholders begin the yearlong transition from the Obama administration to the next one, we want to sustain the view held by most businesses and policymakers that the Framework is a cornerstone for managing enterprise cybersecurity risks and threats globally.[4]

Our associations hold that the Framework would improve the cybersecurity capabilities of EU member states, strengthen cybersecurity partnerships among EU stakeholders, and equip operators of essential services with an innovative tool that they would actively use.

In addition, embracing the Framework would support the EU's efforts to establish a DSM. The Framework is flexible, enabling consumers to have swifter and wider access to digital goods and services across borders compared with a traditional, regulatory program.[5] Also, many international businesses embrace the Framework—based on global, industry-driven standards and practices—providing an economical risk management platform for entities to flourish

---

[2] For instance, the U.S. Chamber of Commerce's 2013 views include high-level principles and recommended amendments to the directive. They are available, respectively, at www.uschamber.com/sites/default/files/documents/files/chamber_comments_eu_directive_us_exec_order_framework_apr13.pdf and www.uschamber.com/sites/default/files/documents/files/23sept13-chamber-cyber-directive-amendmentsexplanatory-statement_final.pdf.

[3] www.nist.gov/cyberframework

[4] http://csrc.nist.gov/cyberframework/rfi_comments_02_09_16.html

[5] The U.S. business community complies with multiple information-security rules. Among the regulatory requirements impacting businesses of all sizes are the Chemical Facilities Anti-Terrorism Standards (CFATS), the Federal Energy Regulatory Commission-North American Reliability Corporation Critical Information Protection (FERC-NERC CIP) standards, the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), and the Sarbanes-Oxley (SOX) Act. The Securities and Exchange Commission (SEC) has issued guidance outlining how and when companies should report hacking incidents and cybersecurity risk. Also, corporations comply with many non-U.S. requirements, which only add to myriad regulations.

securely. The nonprescriptive aspects of the Framework should offer the added benefit of stimulating the European cybersecurity market by aligning the demand and supply for cybersecurity products and services.

European and American businesses and political leaders have a mutual interest in bolstering the security of their vital infrastructures and bringing down barriers to energetic cybersecurity markets. Watching global companies both strengthen their enterprise cybersecurity and boost the economic security and resilience of the nations in which they operate represents optimal public-private partnerships.

A clear value of the Framework is that it brings coherence to divergent approaches to cybersecurity by collecting standards, guidelines, and best practices that are working effectively in the public and private sectors today. The Framework is composed of three main parts—the Framework Core, the Framework Implementation Tiers, and the Framework Profile.

1) **Framework Core—**The Core is not a checklist of actions to perform. Rather, it is a set of cybersecurity activities, desired outcomes, and informative references that are common across organizations, including critical infrastructure entities. The Core consists of four elements—Functions, Categories, Subcategories, and Informative References—that offer organizations a means of mapping their approach to appropriate cybersecurity standards and smart practices.[6]

   A complete description of the Core is not necessary, but two of the Core's elements are worth describing briefly. The Functions portion of the Core arranges basic cybersecurity activities at their highest level, and they are Identify, Protect, Detect, Respond, and Recover. The Categories portion further subdivides the five Functions segments into outcomes that are linked to an organization's cybersecurity needs, including Asset Management, Access Control, and Detection Processes.[7]

Joint industry-NIST Framework Core structure

[6] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf, pages 7–9.

[7] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf, e.g., page 19.

2) **Framework Implementation Tiers—**The Implementation Tiers give organizations better context about their cybersecurity practices and the processes that they have in place to manage risks. Tiers progress from Partial (Tier 1) to Adaptive (Tier 4) and characterize an increasing degree of exactness and sophistication in organization's cybersecurity endeavors, which are based on business requirements. NIST notes that Tiers do not represent maturity levels, but progressing to higher Tiers is "encouraged when such a change would reduce cybersecurity risk and be cost effective."[8]

3) **Framework Profile—**The Profile helps organizations align the Functions, Categories, and Subcategories of the Framework Core with business requirements, risk tolerances, and resources. Framework Profiles can be used to describe the current state or the target state of specific cybersecurity initiatives.

   The Current Profile indicates the cybersecurity outcomes that are being achieved. The Target Profile indicates the outcomes needed to achieve an organization's desired cybersecurity risk management goals. Profiles support business requirements and help people communicate within and among several entities. The Framework, by design, does not prescribe Profile templates, enabling flexibility in implementation.

In addition to the Framework itself, the approach behind the Framework is just as significant. Indeed, use of the Framework is voluntary. Many industry and public-sector stakeholders are committed to a bottom-up, collaborative approach to cybersecurity policy.[9] A vigorous cybersecurity program—including against nation-state hackers or their surrogates and criminal syndicates—can be very expensive. Therefore, it is imperative that the Framework processes remain cost-effective. Organizations work mightily to get one dollar of security for every dollar spent.

- **Voluntary—**The 2013 executive order (EO) that gave rise to the Framework called for the development of a voluntary, nonregulatory Framework.[10] The Framework should lead neither to the creation of new regulations nor to the rollback of existing ones. Under the terms of the EO, policymakers are expected to help agencies and departments with streamlining existing regulations with the Framework and maintaining the Framework's independent nature.

  U.S. industry is pleased that the new Italian cybersecurity Framework (Italian Framework) is derived in large measure from the NIST Framework, with its emphasis on critical infrastructure protection, international harmonization, and flexibility. The Italian Framework, its authors say, is aimed at creating a common language to compare business practices to mitigate cybersecurity risks. The Italian Framework may help an enterprise

[8] www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf, page 9.

[9] Scott Shackelford, Scott Russell, and Jeffrey Haut, *Bottoms Up: A Comparison of Voluntary Cybersecurity Frameworks* (December 10, 2015). UC Davis *Business Law Journal*, 2016, forthcoming; Kelley School of Business Research Paper No. 16-2, which is available at http://ssrn.com/abstract=2702039.

[10] www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

plan a cyber risk management strategy, according to its business, size, and other characteristics of the enterprise. Using the Italian Framework is *voluntary*, the writers emphasize.[11] The Italian model is worth studying because it is built on principles that should be common to any domestic or global cybersecurity initiative.

- **Common Language—**The Framework's common language is grounded in consensus best practices and international standards, better equipping organizations to discuss risk management and cybersecurity both internally (e.g., with company executives and boards) and externally (e.g., with business partners and suppliers) across their ecosystems. Still, it is clear that the terminology of the Framework should be increasingly promoted and used more widely to provide a coherent language worldwide. The Italian Framework illustrates how this can be accomplished. Among other benefits, leveraging the Framework model would prevent the duplication of national regulatory efforts.

  The key is that the Framework should not serve as the impetus for creating extra layers of regulation. Indeed, regulatory redundancy won't bolster the cybersecurity of any organization, including regulated entities themselves. Rather, the Framework can be held up as a voluntary risk management tool while serving as an international beacon around which policymakers can orient their cybersecurity improvement efforts.

- **Collaboration—**The Framework was created through a series of highly collaborative workshops that involved the government and the private sector. Industry and NIST created a tool reflecting that organizations face unique cybersecurity challenges. The Framework is purposefully not a one-size-fits-all approach to detecting, mitigating, and responding to cyber threats.

  Dynamic public-private partnerships thrive on minimal constraints, learn from errors (without punishment), and collaborate through the evolution of ties between participants. It is our organizations' perspective that this is exactly what healthy cybersecurity partnerships facilitate. We recommend leveraging the Framework and the corresponding public-private partnership approach that underpins it to stimulate organizations' protection and resilience against cyberattacks.[12]

- **Cost-effective—**The Framework is a cost-effective mechanism for many organizations because NIST recommends a suite of informative references, but the agency avoids presuming to tell companies how to use them. The Framework is a living document and will be updated as industry provides feedback to NIST and future governing bodies

[11] *2015 Italian Cybersecurity Report: A National Cyber Security Framework* version 1.0 (English translation, February 2016), www.cybersecurityframework.it/sites/default/files/CSR2015_ENG.pdf, page 2.

[12] In his book, *Yes to the Mess: Surprising Leadership Lessons from Jazz* (Boston, MA: Harvard Business Review Press, 2012), Frank J. Barrett, professor of management and global public policy at the Naval Postgraduate School, writes about the requisites for leadership, innovation, and learning in high-performing organizations. He argues (e.g., chapter four, "Minimal Structure–Maximal Autonomy") that dynamic organizations thrive on minimal constraints, learn from errors without punishment, and collaborate through the evolution of ties between participants. In the Chamber's view, this is exactly what healthy cybersecurity partnerships do best.

regarding implementation. Our industry groups urge countries to converge their cybersecurity programs toward the Framework as a touchstone for security and resilience.

Big picture: The very nonregulatory, cooperative, and efficient qualities that have drawn industries toward the Framework—which can be used regardless of where their operations are situated internationally—accrue to companies regardless of whether they are American, Australian, British, French, German, Korean, or Italian, among others. The Framework is special because it is biased toward a standards- and technology-neutral approach to managing cybersecurity risks, rather than favoring a particular nation's or a region's processes. Virtually all multinational organizations benefit when policymakers align flexible cybersecurity risk management programs at the international level, not just at the national level.

The remainder of these comments convey our associations' view that cybersecurity practices should be driven by voluntary, global, and private-sector developed standards and guidance. Also, we contributed extensively to the Framework's development. The letter shows, too, that the U.S. business community is actively using the Framework and promoting it at home and abroad.

Cybersecurity should be rooted in global, industry-driven standards and practices.

Our groups fundamentally believe that cybersecurity efforts are optimal when they reflect international standards and industry-driven practices. Efforts to improve the cybersecurity of the public and private sectors should reflect the borderless and interconnected nature of our digital environment. Standards, guidance, and best practices relevant to cybersecurity are typically private sector-led and adopted on a voluntary basis. They are most effective when developed and recognized globally. Such an approach would avoid burdening multinational enterprises with the requirements of multiple, and often conflicting, jurisdictions.

Industry organizations contributed significantly to the Framework's development.

U.S. industry organizations believe that the Framework—which was released in February 2014—has been a notable success. Sector-based coordinating councils and associations, companies, and other entities collaborated closely with NIST in creating the Framework since the first workshop was held in April 2013. Critical infrastructure entities are very supportive of the Framework. Indeed, crucial elements of U.S. industry are aware of the Framework and are using it or similar risk management tools.

Our associations value the Obama administration's leadership on the voluntary Framework, as well as the Department of Homeland Security (DHS) C^3 Voluntary Program, and urge the next administration to actively support it. We welcome assessments of current and former White House officials who said that industry's response to the Framework has been "phenomenal" and has "exceeded expectations." Such recognition is positive and helps keep the private sector engaged in using the Framework and promoting it with business partners.[13]

[13] For example, the Chamber noted its appreciation of administration officials' comments in an October 2014 letter (page 3) to the National Institute of Standards and Technology (NIST) concerning a previous RFI. It is available at http://csrc.nist.gov/cyberframework/rfi_comment_october_2014/20141010_uscc_eggers_rev1.pdf.

A May 2014 White House blog, *Assessing Cybersecurity Regulations*, set a meaningful tone for how the administration would view its role vis-à-vis the Framework and industry. The blog sent businesses and other stakeholders an important message that the Framework should remain collaborative, voluntary, and innovative over the long term.[14] In June 2014, nearly two dozen U.S. organizations sent a letter to Mr. Michael Daniel, special assistant to the president and cybersecurity coordinator, agreeing with him that businesses and government "must build equally agile and responsive capabilities not bound by outdated and inflexible rules and procedures."[15]

Industry is enthusiastically using and promoting the Framework in partnership with the U.S. government.

Much of industry's favorable reaction to the Framework is owed in large part to NIST, which tackled the Framework's development in ways that ought to serve as a model for other agencies and departments. Interestingly, increasing public attention on the Framework has created visibility into industry's long-standing efforts to address cyber risks and threats—constant, dedicated, and mostly silent efforts that preceded the creation of the Framework.[16]

Since the Framework's release, industry has demonstrated its commitment to using it. Many associations are creating resources for their members and holding events across the country and taking other initiatives to promote cybersecurity education and awareness of the Framework. Some examples are listed here. Associations are planning and exploring additional activities as well.

- The members of the Alliance of Automobile Manufacturers and the Association of Global Automakers established an automobile industry sector information-sharing and analysis center (Auto-ISAC) to facilitate the sharing of existing or potential threats to motor vehicle cybersecurity among members of the industry. In addition, members of the two associations have recently released a *Framework for Automotive Cybersecurity Best Practices* (the auto Framework). The auto Framework was developed in consultation with NIST. Building on the auto Framework, the industry is developing automotive cybersecurity best practices and will continue to collaborate with external stakeholders and cybersecurity experts as appropriate.

- The American Chemistry Council (ACC) is developing sector-specific guidance based on the NIST cyber Framework to further enhance and administer the council's Responsible Care® Security Code. ACC's Chemical Information Technology Center (ChemITC) is completing a pilot program to implement an ISAC for the chemical sector.

[14] www.whitehouse.gov/blog/2014/05/22/assessing-cybersecurity-regulations

[15] www.uschamber.com/sites/default/files/documents/files/11June14GroupLetterT-YReplytoDanielCyberBlog_Final_0.pdf

[16] The online publication *Inside Cybersecurity* provides an excellent catalog of U.S. industry initiatives to implement data- and network-security best practices. See http://insidecybersecurity.com/sector-initiatives.

- The American Gas Association (AGA) hosted a series of webinars on control system cybersecurity, is collaborating with small utilities to develop robust cybersecurity programs, and is working with companies to review and enhance their cybersecurity posture using the Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG-C2M2) from the Department of Energy (DOE). Among other activities, AGA stood up the Downstream Natural Gas Information and Analysis Center (DNG–ISAC), an ISAC designed to help support the information-sharing interests of downstream natural gas utilities.

- The American Hotel & Lodging Association (AH&LA) conducted a series of widely attended cyber and data security webinars to assist small, medium, and large hotel and lodging businesses with implementing key information security measures and risk assessments.

- The American Petroleum Institute (API) fielded a survey of its members in 2015 on the uptake of the Framework. The survey showed that oil and natural gas companies use the Framework to (1) evaluate and prioritize cybersecurity capabilities and programs, (2) facilitate cybersecurity communications via a common language and taxonomy, (3) benchmark cybersecurity performance vis-à-vis industry peers, and (4) evaluate external suppliers/contractors. The oil and natural gas sector's efforts on cybersecurity also include participation in the Oil and Natural Gas Information Sharing and Analysis Center (ONG–ISAC) through which companies share intelligence on cyber incidents, threats, vulnerabilities, and responses.

- The American Water Works Association (AWWA) created cybersecurity guidance and a use-case tool to aid water and wastewater utilities' implementation of the Framework. The guidance is cross-referenced to the Framework. This tool serves as guidance for using the Framework in the water and wastewater systems sector.

- The Automation Federation (the federation) is a nonprofit association made up of 16 member organizations and 7 working groups representing more than 500,000 automation and technology professionals worldwide. In 2013, the federation committed to working with the White House and NIST to help them develop the Framework. With the launch of the Framework in 2014, the federation conducted eight Framework seminars throughout the United States and in London.

  These informational programs provided manufacturing and business leaders with the opportunity to learn more about the Framework and the role it plays in addressing the cybersecurity threat against critical infrastructure.

  In 2015, the federation continued its commitment to instruct business professionals on how to implement the Framework, and the organization recommended that certain automation security standards be incorporated as essential Framework components. The federation is continuing its outreach efforts in 2016.

- The Communications Sector Coordinating Council (CSCC) is the primary venue for collaborative cybersecurity activities with the council's government partners and is made up of the broadcast, cable, satellite, wireless, and wireline industries. Council members have participated in multiple NIST and National Telecommunications and Information Administration (NTIA) engagements, have supported DHS' C^3 Voluntary Program to promote the Framework, and, through their industry associations, have sponsored Framework-related educational programs, webinars, and panels.

  The sector is implementing the recommendations and guidance set forth in the Federal Communication Commission's (FCC's) Communications Security Reliability and Interoperability Council's (CSRIC's) landmark adaptation of the Framework—the *Cybersecurity Risk Management and Best Practices (Working Group 4)* report. Producing this report consumed the time of more than 100 cybersecurity professionals over the course of 12 months. As part of the current CSRIC V effort, the sector is leading three major working groups focused on key cybersecurity topics—information sharing; secure hardware and software–security by design; and the workforce

- CSRIC V's new Working Group 6, which is co-chaired by ACT | The App Association and CBS, recognizes the advantages of building security into hardware and software from the start rather than adding it later. Working Group 6 has developed a report that offers best practices to service providers seeking to manage cybersecurity risks associated with technology obtained from third-party vendors, suppliers, and integrators for use in providers' core networks. Working Group 6 leveraged the Framework to offer sound recommendations that can be adopted by stakeholders of communications sector to improve security-by-design practices.

- The Electricity Subsector Coordinating Council worked with DOE to develop sector-specific guidance for using the Framework. The guidance leverages existing subsector-specific approaches to cybersecurity, including DOE's *Electricity Subsector Cybersecurity Risk Management Process Guideline*, the *Electricity Subsector Cybersecurity Capability Maturity Model*, NIST's *Guidelines for Smart Grid Cyber Security*, and the North American Electric Reliability Corporation's (NERC's) Critical Infrastructure Protection Cybersecurity Standards.

- The financial services sector incorporated the Framework as the basis for its sector-wide *All-Hazards Crisis Response Playbook* (the playbook). Developed and maintained by the Financial Services Information Sharing and Analysis Center (FS-ISAC), the playbook was trimmed from more than 70 pages to 10 pages and redesigned for cyber and business resiliency executives and crisis response teams. Industry exercises, such as the Quantum Dawn series and the Hamilton series, have repeatedly pointed to the need for a unified, useable playbook. Similar to the Framework, the playbook was developed over a six-month period relying heavily on public and private feedback and recommendations.

  The playbook puts into operation the Framework's response and recovery controls at a critical sector level. It also provides a means for businesses to develop their cybersecurity programs over time. The language of the Framework controls is identifiable in the five

main playbook components: (1) Financial Sector (FS) crisis communication; (2) FS Crisis Response Coordination; (3) Government Crisis Response Coordination; (4) Associations, Regional, and Multi-Sector Crisis Coordination; and (5) Sector Contingency Plans and Event Closure.

The succinct structure of the playbook ensures ease of use when responding to crises. The response and recovery activities of both public and private groups are defined throughout the playbook so that crucial sector teams and individuals will know their roles, as well as the roles of government entities, other sectors, and third parties.

Supplementing the playbook is a library that features crisis resource guides, event-specific plans, and templates for use during exercises. For example, playbook templates provide a method for the sector to incorporate lessons learned and identify improvements for future incidents and exercises. The FS-ISAC maintains the library and makes updates based on exercises and real-world experiences. Financial sector leadership is expanding the 2016 sector exercise program to promote and make broader use of the playbook throughout industry.

- HITRUST, in collaboration with healthcare, business, technology, and information security leaders, established the HITRUST CSF, a certifiable framework that can be used by organizations that create, access, store, and exchange personal health and financial data.

  In February 2016, HITRUST, the Healthcare and Public Health (HPH) Sector Coordinating Council (SCC), and the Government Coordinating Council (GCC) announced a new guide to assist healthcare organizations in using the Framework. This document was developed to help HPH-sector organizations implement the Framework and carry out the HITRUST Risk Management Framework (RMF)—consisting of the HITRUST CSF, the CSF Assurance Program, and supporting methodologies.

  HITRUST also leads the development of the healthcare industry's largest information sharing and analysis organization (ISAO) and has taken a holistic approach to threat intelligence sharing and cybersecurity. Key HITRUST initiatives include the Cyber Threat Intelligence and Incident Coordination Center (C3), the Cyber Threat XChange (CTX), monthly threat briefings, and the CyberRX attack simulation exercises.

- The Information Technology Industry Council (ITI) visited Korea and Japan and shared with these countries' governments and business leaders the benefits of a public-private partnership-based approach to developing globally workable cybersecurity policies. ITI highlighted the Framework as an example of an effective policy developed in this manner, reflecting global standards and industry-driven practices.

  ITI principals also spoke at a U.S.-EU workshop in Brussels, comparing U.S. and EU policy approaches on cybersecurity and emphasizing the positive attributes of the Framework and its development. In addition, ITI conducted outreach regarding the Framework in Germany, India, and China.

- The mutual fund industry, represented by the Investment Company Institute (ICI), regularly shares information on threats and mitigation strategies via meetings of its Chief Information Security Officer Advisory Committee. ICI hosts one-day Cybersecurity Forums involving ICI members, security vendors, consultants, and law enforcement entities in the United States and London. In addition, ICI developed a detailed cybersecurity survey for its members, which showed that many firms' cybersecurity programs are consistent with the Framework and that most companies use an amalgam of standards and guidelines in developing and maintaining their information security programs.

  Moreover, the survey results enable a firm to see how it compares with its peers and direct resources according to security priorities. Finally, the ICI hosted an open house in Washington, D.C., featuring the FBI and the Secret Service so that ICI members could discuss the threat environment and personally engage law enforcement agents who have direct responsibility for cyber investigations in 40 field offices across the country.

- The National Restaurant Association (NRA) created and widely distributed last year the *Cybersecurity 101: A Toolkit for Restaurant Operators* guide that details the five functions of the Framework in order to assist restaurant operators and executives in adopting an enterprisewide cybersecurity program. Further, the NRA has convened a working group of member companies to develop a cybersecurity Framework for the restaurant industry, a sector-specific guidance based on the NIST Framework for use by single-unit restaurant operators. More than 7 in 10 restaurants are single-unit operations. The NRA hosted NIST for presentations on the cyber Framework during association events, including webinars and executive study groups.

- The National Association of Manufacturers (NAM) spearheaded the D.A.T.A. (Driving the Agenda for Technology Advancement) Policy Center, providing manufacturers with a forum to understand the latest cybersecurity policy trends, threats, and best practices. The D.A.T.A. Center focuses on working with small and medium-size manufacturers to help them secure their assets.

- The Retail Industry Leaders Association (RILA), in partnership with the National Retail Federation (NRF), created the Retail Cyber Intelligence Sharing Center (R–CISC), featuring information sharing, research, and education and training. This ISAC enables retailers to share threat data among themselves and receive threat information from government and law enforcement partners.

- The Security Industry Association (SIA) created a Cybersecurity Advisory Board composed of member company representatives to recommend safeguards to protect physical security products, systems, and services against malicious cyberattacks and educate the industry on cybersecurity best practices. SIA staff will be implementing a Technology Resource Center for SIA members. The center is set to include a cybersecurity section that will serve as an information-sharing portal for SIA members seeking to communicate among themselves, discuss best cyber practices, employ robust

cyber hygiene, explore network auditing software, and assist businesses with governmental compliance.

- The transportation sector conducted a joint government-industry initiative to offer guidance to businesses on using the Framework as a risk management tool. The Transportation Systems Sector Cybersecurity Working Group (TSSCWG)—made up of officials with the Transportation Security Administration (TSA), the Department of Transportation (DOT), the Coast Guard, and representatives of each of the transportation modes—provided the forum for this cooperative effort. The working group's guidance contributed substantially to common understandings of the Framework and to a broader use of the Framework by entities in each mode of the transportation sector.

  The TSSCWG produced flexible guidance to facilitate businesses' use of the Framework in ways adaptable to the varying sizes, resource bases, and risk profiles of organizations across the transportation sector. A key element of this approach is the development of cyber threat intelligence priorities, which are submitted to DHS and reflect the needs of TSSCWG members. By pooling public-private intelligence requirements, the goal is to produce an up-to-date cyber threat picture, which should better instruct organizations' use of the Framework in mitigating cyber risks. The TSSCWG is cooperating with DHS to hone the transportation sector's intelligence priorities.

- The U.S. Chamber of Commerce launched its cybersecurity roundtable series in 2014. This national initiative recommends that businesses of all sizes and sectors adopt fundamental Internet security practices, including using the Framework and similar risk management tools, engaging cybersecurity providers, and partnering with law enforcement before cyber incidents occur.

  The Chamber is in the third year of its cybersecurity campaign. Eight regional roundtables and two summits in Washington, D.C., have been held since 2014. More events are planned in 2016. Each roundtable typically features cybersecurity principals from the White House, DHS, NIST, and local FBI and Secret Service officials.

Clearly, private sector organizations are using the Framework, creating new resources to help their constituencies reduce risks to their cybersecurity, and sharing best practices through formal and informal means. Industries are also working with government entities to strengthen their information networks and systems against malicious actors.

It is crucial to connect consistent, sound regulatory practices with the EU's Better Regulation agenda.[17]

Finally, but no less importantly, our organizations note that the EC's questionnaire, similar to other consultations launched in support the DSM initiative, may lend itself to generating responses that can be translated into mandates for biased policies and actions. We believe that it would be more productive for the EC to use the questionnaire as a fact-finding exercise to more accurately capture a full picture of what is happening in the marketplace.

[17] http://ec.europa.eu/smart-regulation/index_en.htm

In particular, several questions in the consultation suggest that European officials may take a decidedly discriminatory approach to addressing cybersecurity in an effort to cultivate a domestic cybersecurity industry in the EU. While adopting policies to help grow domestic industries may be appealing from a political perspective, our associations urge the EC not to lose sight of the fact that the challenges posed by cybersecurity threats are inherently global in scope. For this reason and many others, there should be greater emphasis placed on public-private partnerships both in Europe and the United States that include industry actors beyond our nations' respective borders.

Our groups also recognize that the EC's consultation is but one of several and represents only the initial stages of its process to develop a DSM. However, as it continues to develop the DSM we urge the EC to focus on utilizing a process surrounding the creation of a unified market that (1) adheres to smart and effective regulatory practices, (2) lives up to the standards of the Regulatory Fitness and Performance Programme (REFIT),[18] and (3) reflects the changes outlined and endorsed in the Timmermans report on Better Regulation.

***

Our organizations applaud the EU's focus on cybersecurity. Digital attacks on critical infrastructure and intrusions to steal business-sensitive information pose a threat to the security of EU member states and countries around the world. Government and the private sector need to collaborate to deflect and defeat sophisticated and persistent adversaries. Further, we would welcome the opportunity to work with the EU to craft policies that would create a powerful sea change in current information-sharing practices between government and the business community and reflect the conditions of an increasingly digital world.

Sincerely,

ACT | The App Association
Alliance of Automobile Manufacturers
American Fuel & Petrochemical Manufacturers (AFPM)
American Gas Association (AGA)
American Petroleum Institute (API)
Association of Global Automakers
Automation Federation
CompTIA–The Computing Technology Industry Association
CTIA
Edison Electric Institute (EEI)
HITRUST–Health Information Trust Alliance
National Association of Manufacturers (NAM)
National Association of Water Companies
The National Business Coalition on E-Commerce & Privacy
Security Industry Association (SIA)

[18] http://ec.europa.eu/smart-regulation/refit/index_en.htm

Software & Information Industry Association (SIIA)
Telecommunications Industry Association (TIA)
United States Telecom Association (USTelecom)
U.S. Chamber of Commerce