Coalition for Cybersecurity Policy and Law

Coalition for Cybersecurity Policy and Law
575 Seventh Street, NW, Washington, DC 20004

September 7, 2016

VIA EMAIL: cybercommission@nist.gov

Nakia Grayson
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

Re: Comment of the Coalition for Cybersecurity Policy & Law

The Coalition for Cybersecurity Policy & Law ("Coalition") submits this comment in response to the request for information ("RFI") that the Commission on Enhancing National Cybersecurity ("Commission") issued on August 10, 2016 regarding the current and future state of cybersecurity in the digital economy.[1] The Coalition is appreciative of this opportunity to contribute to the Commission's important work, as it seeks to identify, develop, and promote the implementation of best practices with respect to cybersecurity.

The Coalition is comprised of leading companies with a specialty in cybersecurity products and services dedicated to finding and advancing consensus policy solutions that promote the development and adoption of cybersecurity technologies.[2] We seek to ensure a robust marketplace that will encourage companies of all sizes to take steps to improve their cybersecurity, and we are supportive of efforts to identify and promote the adoption of cybersecurity best practices throughout the global community.

I. Executive Summary

The Coalition's comment provides recommendations within each of the topic areas identified in the RFI. These topics include: (1) critical infrastructure cybersecurity; (2) cybersecurity insurance; (3) cybersecurity research and development; (4) the cybersecurity workforce; (5) federal governance; (6) identity and access management; (7) international markets; (8) the Internet of Things; (9) public awareness and education; and (10) state and local government cybersecurity. The Coalition also added several recommendations pertaining to the receipt and handling of reported vulnerabilities and the functioning of the Vulnerabilities

[1] *See* 81 Fed. Reg. 52827 (August 10, 2016).
[2] The views expressed in this comment reflect the consensus view of the Coalition, and do not necessarily reflect the views of any individual Coalition member. For more information on the Coalition, see www.cybersecuritycoalition.org.

Equities Process. The Coalition sets out these recommendations in more detail below; however, for ease of reference, we are providing a list of our recommendations here.

- **General**
    - The Commission should consider the topics in the context of a broader framework. Specifically, the Coalition encourages the Commission to consider these topics within the context of the following goals: (1) promoting the adoption of international norms; (2) improving the state of organizational risk management; and (3) increasing resilience, deterrence, and improved capabilities and awareness. We discuss each of the topics identified in the RFI within the context of this framework.

International Norms

- The Commission should promote the development and use of frameworks created through public private partnerships to effectively manage cybersecurity risk, such as the NIST Cybersecurity Framework ("CSF"). In addition, the Commission should encourage the US government to work through international organizations and standard setting bodies to ensure that resulting frameworks are interoperable across national and regional boundaries.
- The Commission should support efforts to establish an international framework for sharing cyber threat indicators and defensive measures.

Organizational Risk Management

- **Critical Infrastructure**
    - The Commission should promote the adoption of the CSF by owners and operators of critical infrastructure in the US.
    - The Coalition should recommend that NIST incorporate existing supply chain management standards into the informative references.
    - The Commission should recommend that NIST clarify the criteria defining the different Framework Implementation Tiers.
- **Identity and Access Management**
    - The Commission should recommend that NIST incorporate its current authentication standards into the informative references.
- **Cybersecurity Insurance**
    - The Commission should facilitate continued development of the cybersecurity insurance market.
- **Internet of Things**
    - The Commission should emphasize the importance of ensuring that the Department of Commerce promotes voluntary, consensus-based, industry-led standards consistent with OMB Circular A-119 and the National Technology Transfer Act of 1995.
- **Federal Governance**
    - The Commission should promote transparency with respect to any efforts to reorganize cybersecurity responsibilities amongst federal agencies.

Increasing Resilience, Deterrence and Improved Capabilities and Awareness

- **Finding and Responding to Vulnerabilities**
  - **Internal Process for Handling of Vulnerabilities.** The Commission should encourage organizations to implement a process by which they receive and address vulnerability reports.
  - **Government Disclosure of Vulnerabilities.** The Commission should encourage the Administration to formalize the process and provide for greater transparency with respect to the criteria that guides the decision process.
- **Research and Development**
  - The Commission should support the Administration's plan.
- **Cybersecurity Workforce**
  - The Commission should support the government's continued investment in the education and training of cybersecurity professionals.
- **Public Awareness and education**
  - The Commission should recommend that any such campaigns be focused on only the most critical information for consumers to protect themselves.
- **State and Local Governments**
  - The Commission should recommend that the government promote and support broader engagement and information sharing between state and local governments, the private sector, and the federal government.

II. The Commission RFI

The Commission was created to study the current state of cybersecurity and to make detailed recommendations to strengthen cybersecurity in both the public and private sectors while protecting privacy, ensuring public safety, fostering discovery and development of new technical solutions, bolstering partnerships between the government and the private sector, and promoting the adoption of cybersecurity best practices. Executive Order 13718 identified a number of topics that the Commission must consider and provide recommendations on. The Coalition recommends that the Commission approach these topics, identified above, within the context of a broader framework to provide structure to the Commission's consideration of these issues.

The Coalition also encourages the Commission to consider the topics identified in the Executive Order within the context of the following goals that the Coalition believes will promote improved cybersecurity both in the near-term and over the next ten years: (1) improving cooperation between the public and private sectors; (2) increasing information sharing between the government and the private sector regarding cybersecurity threats and vulnerabilities; (3) providing greater transparency with respect to government actions that impact cybersecurity; (4) advancing the maturity of organizational risk management; and (5) ensuring the interoperability of policies adopted across national and regional boundaries. The Coalition believes that the Commission's work will benefit significantly from focusing on these goals within the above stated framework.

III. International Norms

The Coalition considers the adoption of interoperable international cybersecurity standards to be critically important to the continued development of and innovation in the Internet economy, both in the near-term and over the next ten years. As organizations increasingly operate on a global scale, interoperable standards are essential to an organization's ability to efficiently use and protect its systems and networks. Organizations are also increasingly becoming dependent on service providers located all over the world and need workable, interoperable standards by which they can measure their service providers' cybersecurity practices and establish uniform cybersecurity protections for their own systems and information. Organizations face a global threat landscape and must have the tools they need to defend against cybersecurity threats arising anywhere in the world.

The Coalition believes that the Commission can promote the adoption of compatible international standards by encouraging countries to develop cybersecurity frameworks using the Public Private Partnership model that NIST used in the development of the CSF. The Coalition believes that broader adoption of risk management approaches that are interoperable with the CSF will greatly improve organizational cybersecurity across the global marketplace. With many organizations operating internationally and interacting with customers and service providers all over the world, the development of interoperable cybersecurity frameworks is vitally important for organizations to maintain the security of their entire network.

The Coalition also encourages the Commission to promote broad sharing of cyber threat information. Sharing cyber threat indicators is an important element in a proactive approach to organizational cybersecurity. Further, the Coalition believes that broad sharing of threat information by organizations in countries all over the world is needed to maintain the security of the global networks that many organizations use to conduct their business.

A. NIST Framework: Promoting Risk Management as a Norm

The Coalition believes that adoption of a risk management framework is an important element in protecting an organization's systems and information. The Coalition supports the adoption of a risk management framework as an international norm but believes that such frameworks must be interoperable with frameworks adopted in other countries.. The Coalition members provide security products and services on a global scale, and can attest to the importance of coordinated standards and interoperability across jurisdictions. The implementation of diverse or specialized requirements in particular countries or regions could impede interoperability, create inefficiencies, hinder innovation, and make organizations less secure. Therefore, the Coalition encourages the Commission to recommend that the government promote the CSF as a global approach to organizational risk management and encourage international standards setting bodies and other countries to adopt risk-oriented approaches that are capable of interoperability with the CSF to facilitate their own efforts to improve organizational risk management.

The Commission can promote the adoption of interoperable frameworks in other countries by recommending that NIST further engage the international community in the ongoing development of the CSF. For example, the Commission could recommend that NIST solicit feedback on the CSF from international organizations. Engaging the international community through the continued development of the CSF could encourage other countries to develop their own frameworks using the same public private partnership model that NIST used in developing the CSF. Engaging the international community will also help in future efforts to align the CSF with frameworks developed by other countries, which will facilitate the adoption of cybersecurity best practices by organizations that operate on a global scale.

B. International Standards for Sharing of Cyber Threat Information

While the sharing of cyber threat indicators has recently taken a step forward in the United States with the enactment of the Cybersecurity Information Sharing Act of 2015 ("CISA"), the Coalition believes that the development of international standards for sharing cyber threat indicators is essential to facilitate broader sharing of such information. Broad sharing of cyber threat information is important because it enables organizations to move from a reactive posture, seeking to identify and remove intruders from their systems, to a proactive posture where the organization is able to identify and address likely threats before its systems have been compromised. While localized sharing of cyber threat information is a good starting point, it is not sufficient. The Coalition's members and many of their customers operate globally and rely on vendors located all over the world. With such expansive operations, broad sharing of cyber threat information is particularly important to protecting the security of their systems and networks. The ability to efficiently share cyber threat information on a global scale could also have a deterrent effect by increasing the cost of executing an attack and decreasing the potential opportunity for financial gain. The Coalition believes that the Commission can play an important role in facilitating this conversation.

IV. Risk Management

The second goal that the Coalition encourages the Commission to focus on when considering the topics identified in the RFI is improving organizational risk management. The Coalition recommends that the Commission consider the following topics under the broader framework of organizational risk management: (1) Critical Infrastructure; (2) Identity and Access Management; (3) Cybersecurity Insurance; (4) the Internet of Things; (5) Federal Governance; and (6) the Handling of Vulnerabilities. The Coalition views each of these topics as an important component of an effective organizational risk management program. The Coalition will address each topic in turn; however, we will focus particular attention on the Internet of Things and the handling of vulnerabilities, which the Coalition views as being particularly important in both the near-term and in the future.

A. Critical Infrastructure

The Coalition applauds the work that has already been done to develop the CSF, and notes that it has achieved a substantial degree of acceptance and adoption while remaining entirely voluntary. The number of organizations that have adopted the CSF is growing; however, more work is needed to facilitate adoption by small and medium-sized businesses. In particular, the notions contained in the CSF need to be distilled into a form and using language that is understandable to and actionable by small and medium-sized businesses.

For the CSF to remain a valuable resource for organizations to assess their level of cybersecurity preparedness, it must be continuously developed and updated. In particular, the Coalition encourages the Commission to recommend that NIST incorporate existing supply chain management standards into the informative references and that NIST clarify the Implementation Tiers.[3] The CSF Core incorporates consideration of an entity's position in the overall supply chain when identifying cyber assets to be protected, but, in its current state, does not address the security of the supply chain through which such an entity acquires its IT infrastructure. Like other security risks, supply chain vulnerabilities present security risks to critical infrastructure owners, operators, users, and suppliers, and should be addressed, at least at a high level, and with maximum flexibility through the CSF.

Since the adoption of the CSF, important new work has been done on addressing supply chain vulnerabilities, including Supply Chain Management Practices for Federal Information Systems and Organizations, SP 800-161.[4] This work has been informed and supplemented by more recent NIST efforts, particularly its October 2015 workshop on Best Practices in Cyber Supply Chain Risk Management. This work addresses myriad areas, including vendor selection and controls, detection and prevention of vulnerabilities in hardware and software, and implementation of controls on software design, loading, and testing processes. The Coalition also believes that the incorporation of the relevant standards into the informative references will help companies use the CSF to demonstrate their ability to manage supply chain risks. Broader adoption and use of these standards and other recent commercial best practices can serve to inform the discussion of how to better protect the cyber supply chain.

The Coalition also encourages the Commission to recommend that NIST clarify the criteria defining the different CSF Implementation Tiers.[5] The Coalition believes that additional rigor around what each Tier represents would facilitate the adoption of the CSF, and make it more effective in improving cybersecurity practices among critical infrastructure owner and operators. The Tiers are meant to reflect an organization's cyber risk management achievement or risk target level. The Tiers are used in different parts of the CSF evaluation process. The first is in the creation of a Target profile. This is the profile which describes the organization's agreed-to level of acceptable risk in each of the categories/subcategories. The second is in the assessment process. Organizations are able to identify the appropriate tier reflecting their cyber risk management posture after conducting an assessment using the CSF. This dual use needs to be better clarified in the Framework. Indeed, in the experience of the Coalition members, the Framework Implementation Tiers have caused substantial uncertainty because the criteria for designation at each of the given Tiers are fairly amorphous and imprecise.

[3] The Coalition filed comments addressing this issue with NIST on February 17, 2016. The Coalition's comment addresses the incorporation of existing supply chain management standards into the informative references on pages 5 and 6 of the comment.

[4] NIST, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, NIST SP 800-161 (April 2015), available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf.

[5] The Coalition filed comments addressing this issue with NIST on February 17, 2016. The Coalition's comment addresses clarifying the criteria defining the different Framework Implementation Tiers on pages 6 and 7 of the comment.

Additionally, the Coalition recommends that the Commission encourage NIST to identify and catalogue tools relevant to implementation of the CSF. For example, NIST could initiate a dialogue about what meaningful use of the tools in the CSF looks like (i.e., maturity assessment, identification of risks, and decisions around identification, implementation, and use of relevant standards). Currently, the CSF does not address how organizations can measure their progress towards implementing the CSF. The CSF also does not provide organizations with the tools they need to measure another organization's maturity or implementation of the CSF. The Coalition believes that NIST can play an important role in fostering discussion about how organizations' risk management maturity should be measured.

The Coalition further believes that increased sharing of cyber threat information is an essential component in moving from a reactionary defense posture to a proactive approach to protecting the security of our critical infrastructure. Currently, the CSF is silent with respect to an organization's participation in the cyber threat identification and information sharing ecosystem. The Coalition encourages the Commission to recommend that NIST consider cybersecurity information sharing when reviewing the CSF Implementation Tiers. There are now a number of industry/sector-specific Information Sharing and Analysis Centers ("ISACs"), Cyber Emergency Response Teams ("CERTs"), vendor and industry alliances, public-private partnerships, and other, related initiatives that provide real-time information on, and assistance in resolving, specific cyber threats. The owners and operators of critical infrastructure who have implemented a mature risk management culture have ongoing and productive interactions with the relevant cyber ecosystem, including one or more ISACs, CERTs, or other entities, as well as the government in some instances, to share information about threats that it has identified, and to improve its protective posture against threats identified by other entities and by the government. It is important that NIST's definitions of the Implementation Tiers incorporate the various ways in which an entity fits within, and leverages information from, the broader cyber threat identification and information sharing ecosystem.

B. Identity and Access Management

The Coalition believes that broader adoption of multi-factor authentication is an important element of improved cybersecurity for critical infrastructure. As reflected in the Obama Administration's Cybersecurity National Action Plan ("CNAP"), multi-factor authentication processes reflect best practices and have the potential to significantly improve security. Multi-factor authentication processes have increasingly been used in recent years to protect an entity's most sensitive IT assets. However, there continue to be barriers to the implementation of multi-factor authentication processes, including the continued use of legacy systems that do not support such authentication methods and the lack of standardized approaches to multi-factor authentication.

The Coalition encourages the Commission to recommend that NIST incorporate its current authentication standards into the informative references in the CSF's Core. Since the issuance of the CSF, important work has been done to advance the development of authentication standards, including the work on Identity Ecosystems by the National Strategy for Trusted Identities in Cyberspace, and NIST's Electronic Authentication Guidelines, SP 800-63-

2.[6] Incorporating these standards into the informative references would facilitate users' adoption of the appropriate standard to strengthen their authentication practices.

The Coalition also recommends that the Commission leverage aspects of the CNAP to help address barriers to adoption of multi-factor authentication processes, including the high cost of retiring and replacing legacy systems that have security shortcomings. Specifically, the Coalition supports the objectives of the President's proposal to establish an Information Technology Modernization Fund to be used to retire, replace, and modernize the federal government's information technology systems.[7] Federal agencies currently spend 71% of their Information Technology budgets on maintaining legacy information technology that is hard to secure.[8] Transitioning to modern systems will facilitate efforts to secure those systems, and will allow for increased investment in modern security features using the money saved by retiring inefficient legacy systems.

C. Cybersecurity Insurance

The Coalition supports the use of cybersecurity insurance to manage organizational risk arising from a data security incident. In recent years, cybersecurity insurance has become more prevalent in the marketplace, and is frequently a requirement in contracts between an organization and its service providers if such service providers will receive or collect personally identifiable information about the organization's customers or members. Insurance clearly plays a critical role in building risk management strategies. The Coalition supports efforts by the federal government to encourage the continued use of cyber liability insurance without imposing burdensome regulations.

In particular, the Coalition supports efforts to convene stakeholders in the cybersecurity insurance market to facilitate a consensus understanding of what products are available, how much they cost, how they work, and what they protect against. The Coalition believes a broad discussion of the benefits of cybersecurity insurance will lead to broader adoption in the marketplace, which, in turn, will lead to improved security practices as organizations take steps to secure their systems to reduce their insurance premiums. As this process is beginning to occur organically in the marketplace, the Coalition encourages the Commission to recommend that the government facilitate the continued development of the cybersecurity insurance market while, at the same time, providing room for innovation and growth.

D. Internet of Things

The Coalition believes that the Internet of Things ("IoT") market holds great promise for both consumers and businesses over the coming years; however, this promise will be fully realized only if IoT products and services are engineered with privacy and security by design. Appropriate steps must be taken throughout the design, development and use of IoT technologies to manage risks associated with an increasingly connected world. Strong security is also

[6] NIST, Electronic Authentication Guideline, NIST SP 800-63-2 (August 2013), available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf.

[7] *See* Scott, Tony, *Improving and Modernizing Federal Cybersecurity*, White House Blog Post (April 8, 2016), available at https://www.whitehouse.gov/blog/2016/04/08/improving-and-modernizing-federal-cybersecurity.

[8] *Id.*

important to the development of consumer trust in these products and services. The Coalition supports the continued reliance on voluntary consensus-based, industry-led standards setting processes to set cybersecurity standards for the IoT market. Such an approach would be consistent with the requirements of the National Technology Transfer and Advancement Act and OMB Circular A-119.[9] Further, reliance on a voluntary, consensus-based, industry-led approach to setting cybersecurity standards in the IoT market is appropriate due to the diverse nature of the IoT market. The IoT market crosses multiple industries and covers a wide array of devices with varying functionalities and capabilities, and varying degrees of security risk. Additionally, the businesses that are involved in the IoT market vary significantly with respect to their size, resources, and the sophistication of their products. A voluntary, consensus-based, industry-led approach to setting cybersecurity standards for the IoT market would be able to account for this level of diversity in the market, while a prescriptive government-led approach is far more likely to set standards that may be overly burdensome and may restrict innovation in the market. The Coalition believes that the U.S. Department of Commerce plays an important role in promoting and fostering the development of robust standards in new markets and should pro-actively do so in the IoT case.

In particular, the Coalition further encourages the Commission to recommend that the industry-led approach to setting cybersecurity standards seek to create a common understanding about definitions in the following topic areas: (1) security by design; (2) vulnerability disclosure; and (3) updating and patching software. The Coalition believes that each of these areas are of particular importance for the security of the IoT market. First, the standards setting process for IoT devices should address security by design because IoT devices may provide consumers with limited, if any, opportunity to layer security features over what is included with the product when provided to the consumer within the device itself. Therefore, it is particularly important that manufacturers of IoT devices are transparent about the security of their devices throughout the intended lifecycles of the technology they design, develop, and sell. Armed with this information, the market can make effective decisions about what risks are associated with particular technologies and whether or not effective, efficient strategies exist to manage or mitigate those risks during the period the technology will be in use.

Second, the Coalition believes that the standards setting body should consider the development of a taxonomy around the disclosure of vulnerabilities within the IoT market because the possibility of consumer harm arising from un-remedied vulnerabilities in IoT devices poses a substantial threat to consumer trust in the IoT market, which is essential to its continued development and expansion. Finally, the Coalition believes that the standards setting process should address the identification of and patching of security vulnerabilities because certain features of the IoT market present unique challenges to maintaining support for IoT devices over the life of the device. For example, IoT devices that are designed to be inexpensive and disposable are more difficult to update; consumers are often unaware of available security patches; and companies may lack economic incentives to provide ongoing support and security updates. Additionally, having clear patch management guidelines is particularly important in the

[9] OMB, Revision of OMB Circular A-119, Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities, 81 Fed. Reg. 4673, 4673 (January 27, 2016).

IoT market as a significant number of participants in this market may be new to the technology industry and may not know how to implement an effective patch management program or understand the importance of such a program.

E. Federal Governance

The Coalition supports the Administration's efforts to improve federal governance of cybersecurity matters through the creation of a federal chief information security officer and the centralization of cybersecurity authority in DHS; however, the Coalition believes that it is important that this process be transparent. In particular, when creating new positions or transferring responsibilities from one agency to another, it is critically important that the government clearly identify what responsibilities were transferred and what responsibilities remain with the same person or agency as before. This transparency is necessary so that the private sector knows who to interact with when seeking to offer products or services to the government, and so that the agencies with responsibility for various aspects of cybersecurity understand the scope of their own responsibilities. Without this level of transparency, transferring responsibilities to a new individual or agency is likely to result in duplication of effort and wasted resources as both the public and private sectors sort through who has what responsibilities. The Coalition encourages the Commission to address this concern by recommending that the government provide public notice before transferring cybersecurity responsibilities, it allow the private sector an opportunity to provide feedback, and it issue a report identifying the responsibilities that were transferred to a new agency or individual.

V. Increasing Resilience, Deterrence and Improved Capabilities and Awareness

The third goal that the Commission should focus on to provide structure to its consideration of the topics in the RFI is increasing resilience, deterrence and other improved capabilities and awareness. The Coalition recommends that the Commission consider the following topics under the broader framework of promoting deterrence: (1) Research and Development; (2) Cybersecurity Workforce; (3) Public Awareness and Education; and (4) State and Local Government. Each of these topics address areas where improvements will likely increase the investment required to gain access to targeted networks and systems.

A. Vulnerabilities

In addition to the topics that the Commission has identified in the RFI, the Coalition encourages the Commission to urge both private and public sector organizations to implement a process for receiving and addressing reports identifying vulnerabilities in their networks or products. The Coalition further encourages the Commission to provide recommendations regarding the disclosure of vulnerabilities to a product's developer or manufacturer by researchers in both the private sector and the U.S. Government. The Coalition believes that greater transparency is needed with respect to this process.

Vulnerability Handling. The Coalition views the implementation of a process for receiving and addressing reports identifying a vulnerability in an organization's network, applications, or products as a basic requirement of responsible risk management. Whether or not an organization chooses to have a "bug bounty" program to remunerate those who turn over information about vulnerabilities, individual employees within an organization should know who to contact about a reported vulnerability, and organizations should have a repeatable process for investigating the reported vulnerability. The Coalition notes that the Federal Trade Commission ("FTC") identified the maintenance of a process for receiving and addressing reports of security vulnerabilities as an element of maintaining reasonable security procedures in its report entitled "Start with Security."[10] The FTC has also identified a need for organizations to maintain a process for receiving and addressing vulnerability reports in at least four enforcement actions.[11] In each instance, the organization received reports about an existing vulnerability but did not take steps to address the vulnerability. Despite the FTC's statements and actions pertaining to the receipt of vulnerability reports, many organizations still do not have an effective process in place for receiving and addressing vulnerability reports. Therefore, the Coalition urges the Commission to encourage all organizations to implement such programs. The Coalition recognizes that the National Telecommunications & Information Administration ("NTIA") has already begun this work, and it supports NTIA's efforts in this area and looks forward to the NTIA's report. However, the Coalition believes that more should be done to encourage participants in the IoT market to adopt policies that promote the disclosure of vulnerabilities to other market participants.

Vulnerability Equities Process. The Coalition also encourages the Commission to provide recommendations with respect to the government's process for determining when a previously unknown vulnerability should be disclosed to the developer or manufacturer of the product or application. When the federal government learns of a previously unknown vulnerability, it considers whether to retain the vulnerability for future use or to disclose the vulnerability to the developer for remediation. The process for reaching this determination is known as the Vulnerability Equities Process ("VEP"). The VEP, which first became public in 2015, brings together representatives of a number of intelligence, defense, and law enforcement agencies to consider whether to disclose the vulnerability for patching. According to documents released by the federal government, an Equities Review Board ("ERB") considers a number of factors, including the extent of the vulnerable system's use on the Internet, the risks posed by leaving the vulnerable system unpatched, whether the Administration would know if another government or organization was exploiting the vulnerability, whether the vulnerability is needed to obtain intelligence, how likely is it that others will discover the vulnerability, whether the government can use the vulnerability, and whether the vulnerability can be patched or otherwise mitigated. Based on its consideration of these factors, the ERB determines by majority vote whether to disclose a vulnerability with the process being biased in favor of disclosure.

While the Coalition understands and appreciates that much of the VEP must remain classified and disclosure of individual disclosure or retention decisions would not be beneficial, the Coalition urges the Commission to recommend that the Administration formalize the VEP and make certain high-level and aggregate information publicly available. Specifically, the

[10] FTC, "Start with Security: A Guide for Business" 12 (June 2015), available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[11] *In re: Fandango, LLC*, Docket No. C-4481 3 (August 19, 2014)(Complaint); *In re: TRENDnet, Inc.*, Docket No. C-4426 4 (February 7, 2014)(Complaint); *In re: HTC America*, Inc., Docket No. C-4406 2 (July 2, 2013)(Complaint); *In re: ASUSTek Computer, Inc.*, Docket No. C-4587 7 (July 28, 2016)(Complaint).

Coalition encourages the Commission to recommend that the President issue an Executive Order that formalizes the VEP and requires government-wide compliance with it. The Commission should also recommend that the Administration publicly disclose the high-level criteria that the ERB uses to inform its decisions about whether to disclose or retain vulnerabilities. The Commission should further recommend that the Administration require that any decision to retain a vulnerability be subject to periodic review. Finally, the Commission should recommend that the Administration prohibit agencies from entering into non-disclosure agreements pertaining to a vulnerability, and it should recommend that the Administration make certain aggregate information about the number of vulnerabilities that were discovered, the number that were disclosed, and the average length of time between discovery and disclosure.

B. Research and Development

The Coalition strongly supports increased investment in cybersecurity research and development, particularly in the areas of identity and access management, information sharing, and IoT security. With the increasing risk of an organization being targeted by an advanced persistent threat, improved information sharing amongst organizations and with the government is critical to identifying threats and removing them from an organization's system before the attacker has an opportunity to cause damage. The Coalition also believes that the rapid growth of the IoT market has resulted in an increased risk of devices being brought to market with security vulnerabilities. To improve the level of investment in cybersecurity research and development, the Coalition encourages the Commission to support the Administration's Cybersecurity Research and Development Strategic Plan. In particular, the Coalition supports the Plan's recommendation that the government work closely with the private sector to lower barriers and increase incentives for organizations to participate in cybersecurity research and development, that the government address barriers to the broad adoption of proven technologies, and that it promote increased diversity within the cybersecurity research community and the workplace.

C. Cybersecurity Workforce

The Coalition agrees with the Administration's conclusion that there is a shortage of qualified and experienced cybersecurity professionals to match the increasing demand for individuals with such knowledge and experience in both the public and private sectors. The Coalition believes that properly trained cybersecurity professionals are an essential element of any organization's cybersecurity strategy and that a shortage of such individuals could negatively affect the ability of all organizations to identify and protect themselves against an increasing number of threats. The Coalition supports the Administration's Cybersecurity Workforce Strategy generally, and particularly supports the Administration's commitment to invest in the training and education of the cybersecurity workforce. The Coalition encourages the Commission to recommend that the government continue to invest in the education and training of individuals who are interested in cybersecurity positions in an effort to increase the number of trained professionals to meet the market's demand for individuals with these skills.

D. Public Awareness and Education

The Coalition supports efforts to raise the public's awareness of the cybersecurity threats that they face and the steps that they can take to protect themselves, such as the CNAP, which advances a long-term strategy for increasing cybersecurity awareness, and DHS's Stop Think Connect campaign, which encourages individuals to be safer and more secure on the Internet. However, the Coalition believes that such efforts must be narrowly focused on the most important steps that consumers can take to avoid confusing or intimidating consumers. Specifically, the Coalition believes that such programs should provide consumers with information about appropriately managing their online identity. The Coalition encourages the Commission to recommend that current and future public awareness campaigns are narrowly focused on the most useful information to individuals and clearly identify what steps an individual must take to protect the security of their information on the Internet.

E. State and Local Government

State and local governments collect and maintain large amounts of personal information pertaining to their residents. This information may include social security numbers, payment card information, dates of birth, and tax data, among other types of sensitive information. The Coalition believes that state and local governments will be able to better protect this information if they work closely with their federal counterparts and with the private sector. Both the federal government and the private sector can bring a wealth of expertise that states can leverage to improve the security of their systems. State and local governments can also benefit from sharing cybersecurity threat information and intelligence with other states, with the federal government, and with the private sector. Engagement with the multistate ISAC enables states to share cybersecurity threat information with other state or local governments, with private sector partners, and with DHS. The Coalition believes that this type of engagement is important to maintaining an effective deterrence capability and encourages the Commission to recommend that the government promote and support broader engagement and information sharing between state and local governments, the private sector, and the federal government.

* * *

Thank you again for this opportunity. Please do not hesitate to let us know if you have any questions.