Association for Computing Machinery
US Public Policy Council (USACM)

usacm.acm.org
facebook.com/usacm
twitter.com/usacm

September 9, 2016

Thomas E. Donilon, Chair
Samuel J. Palmisano, Vice Chair
Commission on Enhancing National Cybersecurity
c/o National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Re: Input to the Commission on Enhancing National Cybersecurity – Docket No. 160725650-6650-01

Dear Chair Donilon, Vice Chair Palmisano, and Commissioners:

Thank you for the opportunity to comment on the current and future states of cybersecurity in the digital economy, 81 Fed. Reg. 52827 (Aug. 10, 2016), Docket No. 160725650-6650-01. We provide comments on the topic areas of cybersecurity education and the Internet of Things and responses to specific questions.

With more than 100,000 members, ACM (Association for Computing Machinery) is the world's largest educational and scientific computing society, uniting computing educators, researchers, and professionals to inspire dialogue, share resources, and address the field's challenges. ACM advances cybersecurity through its international activities, special interest groups, conferences, publications, digital library collections, policy statements, and curricula recommendations. These comments were developed by the ACM U.S. Public Policy Council with input from the ACM Education Board and the ACM Joint Task Force on Cybersecurity Education. ACM U.S. Public Policy Council statements represent the views of the Council and do not necessarily represent the views of the Association.

## Topic Area Challenges and Approaches

### Cybersecurity Education

A robust focus on strengthening education, research, and innovation is important to achieving overall cybersecurity policy objectives. Ongoing efforts and investments are needed to expand inclusive access to quality computing and cybersecurity education at all levels (K-12, community colleges, and higher education), support flexible pathways to cybersecurity careers and postsecondary educational opportunities, and grow a strong research community that can realize ambitious ideas to build more resilient, secure, and trustworthy digital ecosystems. Computing knowledge and skills underpin the education, research, and workforce pipelines necessary for achieving leadership in cybersecurity. ACM strongly supports making computer science and computational thinking an educational priority, including at the K-12 level.

ACM is actively undertaking projects and initiatives to improve computing and cybersecurity education and workforce development. Among its activities, ACM produces and keeps current international

curricula recommendations and guidelines in all areas of computing, including cybersecurity.[1] These guidelines are used in the United States and worldwide to standardize and assist in the accreditation of college and university programs.

The ACM Joint Task Force on Cybersecurity Education, launched in September 2015, currently is developing comprehensive curricular guidance in cybersecurity education that will support future program development and associated educational efforts.[2] The Joint Task Force is a collaboration between major international computing societies: ACM, the IEEE Computer Society (IEEE CS), the Association for Information Systems Special Interest Group on Security (AIS SIGSEC), and the International Federation for Information Processing Working Group on Information Security Education (IFIP WG 11.8). The Joint Task Force grew out of the foundational efforts of the Cyber Education Project, funded in part by the National Science Foundation.[3]

**Internet of Things (IoT)**

***1. Current and future trends and challenges in the selected topic area:***

The current and future trends and challenges in the realm of cybersecurity will grow exponentially during the next decade. As the networked environment continues to grow, new paradigms in the Internet of Things, cyber-physical systems, and smart cities will bring new security and privacy concerns. Addressing these unprecedented challenges and opportunities presents opportunities for the public and private sectors, individually and collectively, to strengthen cybersecurity across sectors, while fostering innovation and ensuring public safety. Potential challenges should be recognized early, as it might otherwise be difficult to retrofit and address systemic mistakes related to security, privacy, safety, reliability, and resilience of devices and sensors.

The multifaceted nature of IoT brings with it a new set of trends and challenges. Specific concerns raised by IoT are marked by the pervasiveness and diversity of IoT devices and sensors. IoT crosses virtual boundaries as devices and sensors are now intertwined with consumers' lives in the physical world. Security threats with IoT have broader implications of physical security and safety risks. We see the following two distinctive categories of technical, security-related properties that IoT systems introduce:

- **Pervasiveness.** Many IoT systems are already ubiquitous and invisible and may continue this trend as they mature, reducing opportunities for humans to control such systems due to their ubiquity and transparency of operation.
- **Heterogeneity.** IoT systems incorporate a wide variety of interconnected devices that create interoperability challenges. IoT interconnectivity naturally leads to interaction of systems and components that are built by different vendors, according to different standards, and using different protocols. The magnitude of the diversity in IoT environments is extensive and introduces interoperability challenges that can lead to substantial system vulnerability.

[1] ACM Curricula Recommendations and Guidelines, http://www.acm.org/education/curricula-recommendations.
[2] ACM Joint Task Force on Cybersecurity Education, http://www.csec2017.org.
[3] Cyber Education Project, http://www.cybereducationproject.org.

Security threats are critical in the evolving context of the IoT ecosystem. IoT systems have network, device, and data levels that will require unique and tailored security. The limited configuration of certain technologies embedded within IoT may prevent necessary updates. The vulnerability of these legacy items can have potentially devastating consequences for users. The ubiquitous, heterogeneous nature of IoT raises concerns involving the trustworthiness of the devices and sensors. The trustworthiness includes security, privacy, safety, reliability, and resilience. Trustworthiness poses a greater concern in IoT as devices and sensors continue to proliferate with high interconnectedness and integration.

In relation to challenges related to IoT terminology, the different interpretations of IoT and what it encompasses reflect the continuing development and evolution of IoT systems and technologies. At least three government agencies – the FTC, FBI, and NIST – agree that interconnectedness is a primary characteristic of IoT and related systems. The agencies' definitions involve a level of interaction among the "things" that they respectively consider part of IoT or related concepts. The agencies also incorporate networked connectivity as part of this interconnectedness. Differences lie, however, with the nature of the connectivity and networked systems and whether connectivity needs to be automatic. They also differ in their interpretations of the scope of IoT and overlapping concepts.

A review of the definition of IoT and related concepts has shown a lack of consensus associated with a proliferation of terms.[4] Most recently, a NIST publication titled *Networks of 'Things*,' stated that "there is no formal, analytic or even descriptive set of building blocks that govern the operation, trustworthiness and lifecycle of IoT components."[5] The report recommended that a composability model and vocabulary that defines principles common to most, if not all networks of things, is needed to address the etymology of IoT.

Given the current and expected technology, we encourage further discussion among government and stakeholders, including businesses, academia, professional societies, consumer advocates, nonprofits, and other civil society organizations on what encompasses the IoT landscape and how it relates to or differs from other related systems.

***2. Progress being made to address the challenges:***

Recognizing the importance of IoT, USACM formed a working group to identify and formulate a foundation for explaining the unique issues that IoT brings to policy. Other entities within ACM also see IoT as an important topic. Some of the ACM Special Interest Groups addressing IoT include the Special Interest Group on Computer Human Interaction (SIGCHI), the Special Interest Group on Applied Computing (SIGAPP), the Special Interest Group on Spatial Information (SIGSPATIAL), the Special Interest Group on Management of Data (SIGMOD), the Special Interest Group on Mobility of Systems, Users, Data and Computing (SIGMOBILE), the Special Interest Group on Security, Audit and Control (SIGSAC), the Special Interest Group on Software Engineering (SIGSOFT), and the Special Interest Group on Embedded Systems (SIGBED), among others.

[4] USACM Comments to the National Telecommunications and Information Administration on the Internet of Things (June 2, 2016), http://usacm.acm.org/images/documents/2016_USACM_Comments_NTIAIoT.pdf.
[5] NIST Special Publication 800-183, Networks of 'Things' (July 2016), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-183.pdf.

Among ACM's existing publications providing technical and policy information about IoT are articles submitted for an ACM Ubiquity symposium on the topic. The symposium articles explore the complex issues of IoT from multiple perspectives, including on privacy and security. A forthcoming Special Issue of the ACM Transactions on Computer-Human Interaction (ACM TOCHI) magazine will address end user development for IoT. Further, upcoming ACM conferences and workshops will address topics such as the rapid advancement and pervasiveness of IoT systems,[6] new horizons for IoT,[7] IoT security and privacy challenges and solutions,[8] and the trustworthiness of embedded devices and sensors within IoT.[9]

***3. The most promising approaches to addressing the challenges:***

In order to address technical challenges and improve cybersecurity awareness, we support approaches that aim to foster invention and innovation while ensuring a secure and private digital ecosystem. Risk management and adoption of best practices across the public and private sectors will help advance cybersecurity policy objectives. Promising approaches to addressing challenges will recognize the multidisciplinary nature of IoT.

In the case of IoT, important technical aspects to consider for the future include:

- **Interoperability** allows the different components of the IoT ecosystem to function in harmony. Interoperable systems have impacts on privacy and security. The ability for devices and sensors to interact allows vulnerable legacy items to be phased out and replaced with updated components. Conversely, selective non-interoperability can enhance privacy by preventing information flow into certain contexts where privacy might be in peril. There may be contexts in which lack of interoperability should actually be seen as a goal or mitigation rather than an obstacle.
- **Composability** will be a technical issue to consider, particularly given the large number of IoT devices and sensors that interact with each other. As a unit, a device, or a sensor may meet security, privacy, and safety requirements. However, when combined or integrated with other devices and sensors, as expected in IoT, there is no certainty in that these properties will remain. In a composable infrastructure, systems can assemble in variety of combinations based on user needs. The integration of all these properties and behaviors brings opportunity but also can have unintended consequences on the IoT ecosystem.
- **Data ownership, data maintenance, and data attribution** are also important to consider in the development of IoT. These issues raise concerns about data quality, networked storage, and

[6] Sixth International Conference on the Internet of Things (IoT 2016), November 7-9, 2016, Stuttgart, Germany, http://www.iot-conference.org/iot2016/.
[7] UbiComp '16 Workshop on New Horizons for the IoT in Everyday Life, 12 September, 2016, Heidelberg, Germany (co-located with 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing), https://iothorizons.wordpress.com.
[8] Tutorial on IoT Security and Privacy Challenges and Solutions, Embedded Systems Week, October 2-7, 2016, Pittsburgh, PA, http://www.esweek.org/events/2016/tutorials/iot-security-and-privacy-challenges-and-solutions.
[9] Sixth International Workshop on Trustworthy Embedded Devices, October 24-28, 2016, Vienna, Austria (co-located with the 23rd ACM Conference on Computer and Communications Security), http://th.informatik.uni-mannheim.de/trusted-workshop/2016/.

legacy file formats. Moreover, the large scale of data creation and storage can overwhelm available infrastructure. A challenge that is inherently tied to these considerations is the maintenance of metadata, especially as it concerns data integrity and data ownership.

- **Metadata**, referred to as "data about data," provide context on data. Some of the attributes that may be displayed by metadata are location, owner, domain, or manufacturer. A function of metadata is to provide context that can later be used for applications or analysis. If there are multiple data points for the same item, one may be materially older. Failure to maintain the metadata prevents usage of the most current data, which can have negative effects on later applications of the same data. Similar metadata concerns are associated with permissible use.

***4. What can or should be done now or within the next 1-2 years to better address the challenges? 5. What should be done over the next decade to better address the challenges?***

As IoT devices and sensors become more ubiquitous, policy approaches should be informed by technical experts and stakeholders who can provide guidance and insights on related technical aspects. We urge the government to pursue federally funded research initiatives in computing and approaches to ensure a secure, resilient, and trustworthy digital ecosystems.

As IoT continues to capture unprecedented amounts of data at a fast rate, the private sector and users will need privacy guidance. It is important that users are aware of the privacy and security ramifications of the data collected. They should be encouraged to play an active role in determining and managing what data is collected, its accuracy, and the retention of that data. This will allow users to make choices that align with their personal privacy and security expectations.

Challenges associated with the terminology of IoT and related concepts, as well as cybersecurity lexicon should be addressed by encouraging interagency discussion and discussion between the public and private sectors. This would allow for the creation of cohesive and consistent policy and regulatory approaches that foster innovation while enhancing cybersecurity and privacy.

***6. Future challenges that may arise and recommended actions that individuals, organizations, and governments can take to best position themselves today to meet those challenges.***

The pervasiveness of IoT devices and sensors and their high interconnectedness will make it very difficult and expensive to retrofit and address issues like security, privacy, and safety. Proactively addressing these issues is important. Appropriately crafted principles to help guide technical development can help enable innovation and can help avoid systemic mistakes.

Meeting the dual imperatives of protecting privacy and security is a challenge for IoT that raises questions on the relationship between cybersecurity and privacy risks. Many privacy risks are interdependent with other types of risks, data actions, and processes. Addressing privacy concerns should entail an understanding of the way privacy risks work in tandem with security risks so as to address risks comprehensively. Five major considerations should be technically addressed within the IoT infrastructure and these include data integrity, identity management, trust management, data protection, and data volume.

- **Data integrity** ensures that data produced and captured in the IoT environment can be trusted and has not been compromised.
- **Identity management** is the administration of identities within an IoT system.
- **Trust management** takes into account the human component of IoT devices and sensors as well as their ubiquity and ensures that the devices and sensors transmitting the data can be trusted. The ubiquity of the devices and sensors may require a multi-value and multi-dimensional approach to trust. Rather than trusted or untrusted, devices and sensors may have varying levels of trust, possibly dynamically.
- **Data protection**, from the technical viewpoint, encompasses the guarantee that sensitive information captured in a variety of environments, including information about physical environments, is protected while maintaining the functionality of IoT.
- **Data volume** refers to the massive amounts of data that IoT components capture that directly relate to human activity. The large volume of sometimes highly personal data can be used in unintended ways, like to create detailed predictive profiles of individuals. Moreover, the availability of IoT data creates new privacy risks when combined with existing data sources such as web and social data that can increase their predictive power by combining online behaviors and behaviors in the physical environment.

As the devices and sensors within the IoT ecosystem become increasingly pervasive, they contribute to the volume of data available, the velocity at which data will be generated, and the variety of devices and sensors capturing data. The massive collection of data and the new type and amount of data will likely reveal new insights. The disparate individual pieces of information when combined can reveal sensitive patterns that were previously not readily identifiable; this is known as mosaic theory. This raises privacy concerns because data collection, storage, and sharing might expose users to unexpected privacy risks. Furthermore, data that is collected for one purpose may allow inference of other information in ways that users and developers may not expect.

**Responses to Specific Questions**

***The Commission also seeks input on the following:***

***1. Emerging technology trends and innovations; the effect these technology trends and innovations will have on the digital economy; and the effect these technology trends and innovations will have on cybersecurity.***

Emerging technology trends and innovations will bring about new challenges and benefits that will require equally innovative policy approaches. These emerging trends will have an effect on the global economy and their ramifications extend beyond the digital realm. New computing paradigms will bring about unprecedented risks as well as opportunities. New identifiers, components, devices, and infrastructure will raise issues of computing capability, privacy, security, usability, accessibility, spectrum availability, standards, networks, and interoperability.

The effects these trends will have on cybersecurity will be exponential, and risk management and best practices should be at the forefront of policy discussions. These emerging trends will be characterized by fast-paced evolution, resulting in rapid change in risk environments. As such, it is important to devise approaches that meet the dynamism of operational systems.

The fast emergence and rapid adoption of new technologies may cause data collection to be in conflict with privacy and security. These concerns are reflected in existing privacy data protection frameworks that provide guidance on how data collected by these newer and emergent technologies is collected, retained, combined, shared, or used. It will be important to establish privacy and security parameters, as large-scale collection may leave data vulnerable to multiple privacy and security threats.

***3. Government-private sector coordination and cooperation on cybersecurity.***

We support coordination and cooperation between governments and the private sector in the development, promotion, and implementation of cybersecurity best practices and policies. Fostering and leveraging cooperation among government, industry, academic institutions, professional societies, and other stakeholders is vital to achieving cybersecurity and resiliency of our infrastructures, continued innovation, and an educated computing and cybersecurity workforce.

In developing approaches and initiatives, we encourage governments and the private sector to engage with computing professionals who will be able to provide technical and scientific expertise. Consultative processes should involve a breadth of technical experts from different sectors in the computing community. The development of these approaches should foster and leverage cooperation among government, industry, academic institutions, professional societies, and consumer advocates. This multistakeholder collaboration is vital to achieving resilience of our infrastructures and continued innovation. Public-private sector coordination also is important to strengthening the computing and cybersecurity education, research, and workforce pipelines.

Structurally, we support effective institutions and regulatory frameworks that foster the development and promotion of innovative cybersecurity technologies. We encourage public-private partnerships that

aim to build solid and sustainable foundations for the future and build public trust in technologies and networks. Decision makers in government and the private sector should coordinate to foster an understanding of the technical underpinnings of the possible effects that these technological innovations will have on cybersecurity. The creation of policy frameworks based on technical understandings, including foresight of technological advances, will help foster innovation, mitigate unwanted risks, and anticipate future security needs, opportunities, and challenges.

***4. The role(s) of the government in enhancing cybersecurity for the private sector.***

Cybersecurity and protection of the digital ecosystem will require the government to encourage innovation. In order to enhance cybersecurity for the private sector and increase awareness, the government can take steps to ensure that cybersecurity technologies are developed, implemented, and promoted.

The government should take actions to develop effective institutions, create regulatory frameworks that foster innovation, enable beneficial computing privacy and security research, fund computing research and development, and foster efforts by the private and public sectors (individually and collectively), to build a more secure and trustworthy global digital system. The government also can encourage and support the cybersecurity education, research, and workforce development pipelines. (See additional comments below on cybersecurity education.)

The government should facilitate multistakeholder discussions on enhancing cybersecurity. These discussions should include diverse stakeholders, including from government, the business sector, academia, nonprofits, technical and other professional associations, consumer advocates, and civil society.

Because the digital environment and its security involves cross-border and global issues, we support involvement of the United States in bilateral and multilateral engagements, international standards processes, and efforts to develop and incentivize voluntary marketplace measures. We encourage U.S. participation in international standards and processes for cybersecurity and privacy.

***5. Performance measures for national-level cybersecurity policies; and related near-term and long-term goals.***

With the continued growth in the number and diverse types of networked devices and sensors, it will be increasingly difficult to establish constructive measures for cybersecurity. The highly dynamic and interactive relationships among existing and emerging technologies pose new challenges. Arriving at an approach that protects privacy and enhances cybersecurity in these new environments will require consideration of emergent privacy and security risks.

We encourage the government to convene dialogues on the long-term interests of cybersecurity in existing and emergent environments. These discussions could help identify potential approaches to addressing evolving threats and future implications of proposed options. Such discussions also could help identify areas where the development of technical standards may be beneficial.

***6. Complexity of cybersecurity terminology and potential approaches to resolve, including common lexicons.***

The complexity of current cybersecurity terminology stems from a proliferation of terms. We have seen how different entities might use the same cybersecurity-related terms with differing definitions and interpretations and how some terms are used casually and interchangeably in technical and non-technical contexts.

Many newer technologies in their developmental stages are not yet ready to be constrained by definitions. Further dialogue among stakeholders could help develop better understandings of terms, their applications, and areas of divergence and consensus.

Thank you again for the opportunity to comment on approaches and challenges of enhancing national cybersecurity. The staff and members of the ACM U.S. Public Policy Council, the ACM Education Board, and the ACM Joint Task Force on Cybersecurity Education are available if you have questions or would like additional information about the issues raised in this public comment.

Sincerely,

Stuart S. Shapiro, Ph.D.
Chair, ACM U.S. Public Policy Council
Association for Computing Machinery