**Written Testimony of**

**Dean C. Garfield**
**President & CEO**
**Information Technology Industry Council (ITI)**

**Before the**

**Committee on Homeland Security and Governmental Affairs**
**U.S. Senate**

***Cybersecurity Regulation Harmonization***

**June 21, 2017**

**Written Testimony of:**
**Dean Garfield**
**President & CEO, Information Technology Industry Council (ITI)**

**Before the:**
**Committee Homeland Security and Governmental Affairs**
**U.S. Senate**

***Cybersecurity Regulation Harmonization***

**June 21, 2017**

Chairman Johnson, Ranking Member McCaskill, and members of the committee, thank you for the opportunity to testify today. I am Dean Garfield, President and CEO of the Information Technology Industry Council (ITI), and I am pleased to testify before the Homeland Security and Governmental Affairs Committee on the important topic of cybersecurity regulation harmonization. We welcome your interest and engagement on this subject.

ITI[1] represents 60[2] of the world's leading information and communications technology (ICT) companies. We are the global voice of the tech sector and the premier advocate and thought leader in the United States and around the world for the ICT industry. ITI's members comprise leading technology and innovation companies from all corners of the ICT sector, including hardware, software, digital services, semiconductor, network equipment, Internet companies, and companies using technology to fundamentally evolve their businesses. Cybersecurity and cybersecurity technology are critical to ITI members. Facilitating the protection of our customers (including governments, businesses, and consumers), securing and protecting the privacy of our customers' and individuals' data, and making our intellectual property, technology, and innovation available to our customers to enable them to improve their businesses are core drivers for our companies. Consequently, ITI has been a leading voice in advocating effective approaches to cybersecurity, both domestically and globally.

Cybersecurity is rightly a priority for governments and our industry, and we share a common goal of improving cybersecurity. Further, our members are global companies, doing business around the world. As both producers and users of cybersecurity products and services, our members have extensive experience working with governments across the globe on cybersecurity policy. This is important for the committee to keep in mind because when it comes to cybersecurity, our connectedness is through an Internet that is truly global and borderless. We acutely understand the

[1] **About ITI.** ITI is the global voice of the tech sector. We advocate for public policies that advance innovation, open markets, and enable the transformational economic, societal, and commercial opportunities that our companies are creating. Our members represent the entire spectrum of technology: from internet companies, to hardware and networking equipment manufacturers, to software developers. ITI's diverse membership and expert staff provide a broad perspective and intelligent insight in confronting the implications and opportunities of policy activities around the world. Visit http://www.itic.org/ to learn more. Follow us on Twitter for the latest ITI news @ITI_TechTweets.
[2] See membership list at http://www.itic.org/about/member-companies.

impact of governments' policies on security innovation and on our customers, and thus the need for U.S. policies to be compatible with – and lead – global norms.

I will focus my testimony on four areas: (1) using public-private partnerships and leveraging existing cybersecurity policies to achieve greater regulatory streamlining; (2) harmonizing federal cybersecurity policies around risk management and international standards, including for the Internet of Things (IoT); (3) prioritizing implementation of existing federal policies on regulatory streamlining through federal agency coordination; and (4) reforming government acquisition procedures to allow use of agile federal procurement processes to acquire cybersecurity products and services.

**Assess & leverage existing cybersecurity policies and build upon public-private partnerships to achieve greater regulatory streamlining at the international, federal, and state levels.**

There has been a flurry of cybersecurity policymaking activity in the U.S. over the past few years. The Obama Administration issued several executive actions dealing with cybersecurity, including Executive Order (EO) 13718 that launched the Commission on Enhancing National Cybersecurity[3] and EO 13636[4] that called for the National Institute of Standards and Technology (NIST) to develop the *Framework for Improving Critical Infrastructure Cybersecurity* (the *Framework*). NIST is now leading an effort to update the *Framework*, soliciting comments from the private sector earlier this year. Last month, the Trump Administration issued EO 13800 on *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*,[5] and Congress has passed prominent cybersecurity laws, particularly cybersecurity threat information sharing legislation.[6]

These new initiatives complement well-established public-private partnership activities, and together, the public and private sectors have begun implementing many of these policy instruments. Congress should consider the public and private sectors' ongoing collaboration and efforts to implement pre-existing regulations before further legislating on cybersecurity so that Members may arrive at a holistic, federal cybersecurity strategy approach.

It is well-known that the private sector owns/operates approximately 85 percent of critical infrastructure in the United States and elsewhere, and that the ICT industry creates nearly the entire cyberspace infrastructure. What is not known are the many ways the ICT industry works cooperatively with federal, state, and local governments to improve cybersecurity and ensure that approaches to cybersecurity are adaptive, flexible, and effective. For well over a decade, ICT companies have provided leadership, subject-matter experts, technical and monetary resources, innovation, and stewardship to help enable all stakeholders to better manage and mitigate

[3] Executive Order 13718, *Commission on Enhancing National Cybersecurity*, February 9, 2016, *available at* https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/executive-order-commission-enhancing-national-cybersecurity.
[4] Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, February 12, 2013, *available at* https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.
[5] Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, May 11, 2017, *available at* https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal.
[6] *Cybersecurity Act of 2015*, passed as Division N of the FY 2016 Omnibus Appropriations Act, P.L. 114-113, December 18, 2015.

cybersecurity risk. Cyberspace would be much less secure in the absence of these partnerships and initiatives. For example, the Information Technology Information Sharing and Analysis Center (IT-ISAC) has been invaluable to help address sector specific and cross-sectoral threats and vulnerabilities. It helped monitor and collaborate with its members on large-scale threats such as Conficker and the DNS Cache Poisoning Vulnerability. The IT-ISAC provided a forum for members to engage in collaborative analysis on those significant issues and share alerts and potential solutions with members, other ISACs, and the public.

Policymakers, as they seek to advance critical infrastructure (CI) protection, stand to gain by leveraging existing work, as appropriate, prior to establishing new policies- particularly by continuing to harness the public-private partnerships that have been in existence for decades. For example, many companies previously shared limited cyber threat information through ISACs and Sector Coordinating Councils (SCCs), but Congress improved upon and bolstered those partnerships through the 2015 cybersecurity threat information sharing legislation by eliminating barriers that precluded the sharing of specific, actionable threat information between public and private sectors.

In addition, Congress should ensure NIST continues to serve as the federal coordinator for cybersecurity best practices and guidelines. One of the best examples of effective public-private collaboration on cybersecurity is NIST's continuing work on the *Framework*, as well as its other efforts such as the *IoT-Enabled Smart City Framework*.[7]

To streamline federal, state, local, as well as international, cybersecurity regulatory efforts, we need a common language or cybersecurity risk management taxonomy that can be effectively used by policymakers globally and at all levels of U.S. government. It is counterproductive to create siloed, agency-specific or country-specific approaches to cybersecurity, and the federal government should promote polices that help break down the artificial barriers that hinder cybersecurity efforts. Unfortunately, without a common lexicon for cybersecurity and risk management efforts, federal, state, local, and international governments tend to create separate approaches to cybersecurity that ultimately lead to greater insecurity for governments, consumers, and private industry.

ITI strongly recommends the *Framework* as a policymaking tool. Promoting the *Framework* as a common language for policymakers can help align U.S. federal agency cybersecurity and risk management efforts. The *Framework* leverages public-private partnerships, is grounded in sound risk management principles, and helps foster innovation due to its flexibility and basis in global standards. The *Framework* has consistently been lauded for providing a common language to better help organizations comprehend, communicate, and manage cybersecurity risks. While it is important to stress that we are still in the early phase of a multi-year effort and we do not see this as a silver bullet solution, we believe the *Framework* has already helped and will continue to help improve cybersecurity, and its approach is worth prioritizing and replicating domestically and globally for both organizations and governments.

[7] National Institute of Standards & Technology, IoT-Enabled Smart City Framework, *available at* https://pages.nist.gov/smartcitiesarchitecture/.

The potential of the *Framework* to provide a common taxonomy for policymakers domestically and globally has yet to be fully realized. We urge Congress to support and oversee the implementation of the Trump Administration's cybersecurity EO that requires federal agencies to use the *Framework* to manage each agency's cybersecurity risk.

Without a guideline like the *Framework* around which to orient their efforts individual federal agencies, state governments, and other countries may fill the void with disparate and conflicting guidelines and regulations. For example, in April 2016, the National Highway Traffic Safety Administration (NHTSA) at the Department of Transportation released a request for public comment on an Enforcement Guidance Bulletin on Safety-Related Defects and Emerging Automotive Technologies.[8] The Bulletin endeavored to create a separate cybersecurity scheme for automobiles, but failed to create a prioritization of cybersecurity risks in a way that aligns with cybersecurity risk management best practices. The ongoing convergence of the automotive and technology sectors alone does not call for a separate regulatory structure to address automotive cybersecurity. NHTSA should, instead, leverage existing work like that being done by NIST, under the *Framework* and *Cyber Physical Systems Working Group*, or by the Department of Homeland Security (DHS) and international standards bodies.

States are beginning to legislate solutions and issue regulations as well, which is adding more complexity. Nevada Senate Bill 395 was recently introduced and opposed by ITI because of its intent to define CI in the state and develop a subsequent state plan with requirements that are not consistent with sound cybersecurity policy, or existing federal policy. This legislation would create a conflicting and competing definition of CI with those at the federal level designated by DHS. DHS is already in charge of designating CI and working with the private sector owners and operators to mitigate CI risk through federal law and policy. Additionally, the need to preserve and promote innovation and innovative technologies would be hindered by over-designating CI, which would thinly stretch already limited resources. Lastly, the bill would effectively provide public disclosure of vulnerabilities within CI systems, which is contrary to commonly recognized cybersecurity best practices. States should not be in the business of designating CI outside of the federal government's definition. It is incumbent upon industry and the federal government to educate states on the work currently being done at the federal level to mitigate security vulnerabilities at all levels of government.

Congress should look for ideal *outcomes*, not ideal *regulations*, which may not always be the same. This way of thinking opens the door to creative approaches that seek to harmonize cybersecurity regulations around a common set of principles that are flexible and adaptable to changing technologies and constant innovation.

[8] Department of Transportation, National Highway Traffic Safety Administration, Request for Public Comments, Docket No. NHTSA-2016-0040, April 1, 2016.

**The federal government should harmonize cybersecurity policies around risk management and international standards based in the *Framework for Improving Critical Infrastructure Cybersecurity* to avoid duplicative resources and requirements on federal agencies, state governments, and the private sector.**

The technology sector partnered with NIST for nearly three years to develop the *Framework* pursuant to EO 13636, which called for the government to partner with owners and operators of CI to improve cybersecurity through the development and implementation of a framework of voluntary, consensus, risk-based standards. The *Framework* provides an overarching structure, grounded in proven international standards and consensus best practices, to address organizational security across all CI sectors, while providing adaptability and flexibility to meet unique sector needs and address new threats.

As noted earlier, the *Framework* includes a common language for organizations to manage cybersecurity risks, and that language can be the basis for action by policymakers globally and domestically. Among other benefits, this approach can help prevent duplicative regulatory efforts.

One area where the *Framework* can be used in such a fashion is to drive cybersecurity alignment across federal agencies. As discussed further below, it is extremely important to push for alignment of federal agency cybersecurity practices, including orientation of federal agency efforts to the *Framework*, which will in turn facilitate mapping of agencies' cybersecurity risks to their missions government-wide. In fact, the recent cybersecurity EO clearly called for this risk management tactic.[9] The order requires each agency head to use the *Framework*, or any successor document, to manage the agency's cybersecurity risk and submit a risk management report to DHS and the Office of Management and Budget (OMB).

ITI previously recommended the Executive Branch develop guidance for federal agencies to apply the *Framework* to help them use business drivers to guide cybersecurity activities and consider cybersecurity risk as part of their risk management processes. To support agency heads in responding to the Trump cybersecurity EO, NIST released a request for comment on its proposed *Framework* implementation guidance.[10] NIST is effectively developing government-wide guidance in the same manner that many sectors currently do for their own use, and such a streamlined effort will reduce regulatory redundancy.

Beyond using the *Framework* in its exact form, private industry also adapts the principles expressed in the *Framework* to develop their own guidance, precluding the need for the federal government to create more granular cybersecurity regulations. For example, the financial sector compiled the Federal Financial Institutions Examination Council's Information Security Booklet, which was updated in September 2016 to provide a tool for financial institutions to implement a cybersecurity

[9] Executive Order 13800, *supra* note 5.
[10] National Institute of Standards & Technology, *The Cybersecurity Framework: Implementation Guidance for Federal Agencies*, Interagency Report 8170, *available at* http://csrc.nist.gov/publications/drafts/nistir-8170/nistir8170-draft.pdf.

program consistent with the *Framework*.[11] In the communications sector, the Communications Security, Reliability and Interoperability Council (CSRIC) provides recommendations to the Federal Communications Commission on optimal security and reliability of communications systems.[12] The CSRIC working group IV recently developed detailed voluntary risk management guidance mapped to the *Framework* for the communications sector.[13] NIST further developed a version of the *Framework* for small businesses to use to assist in protecting their data and intellectual property.[14]

***International Standards.*** The global ICT industry is heavily invested in developing standards for security management, and the United States should continue to lead the way in promoting adoption of industry-led, voluntary, globally recognized cybersecurity standards and best practices that avoid country-specific requirements. Many international governments have already been inspired by efforts like the *Framework* to develop their cybersecurity guidelines. Furthermore, the technology sector has supported organizations across the globe who use the *Framework*, and it is gaining traction internationally (e.g., Italy developed its own version of the *Framework* using a similar public-private partnership process; Israel has incorporated the Framework into its own cybersecurity guidance; and the British Standards Institute is developing a standard that assesses organizations' application of the *Framework).*

A central element of ITI's global advocacy efforts involve helping governments understand the critical importance of cross-border data flows, not only to the ICT sector, but also to the global economy. Global cybersecurity relies on the ability for data to flow across borders. Threat indicators, research and development, product design, and other information, when shared globally, aids in the development of robust mechanisms to protect against threats. It also ensures companies can perform operations, manage production schedules and communicate with subsidiaries and employees across the globe in a secure manner, enabling them to invest in and create technologies which are secure and, in turn, help protect the entire ecosystem upon which all stakeholders rely. The free flow of data across borders is necessary to enable a seamless and secure Internet experience for hundreds of millions of citizens around the globe.

Some international developments threaten the ability for these essential data flows to continue. The Proposed Wassenaar Rule imposing restrictions on the sale of cybersecurity technology such as intrusion detection software is an extension of a troubling global trend of erecting barriers to the free movement of global data. Another example of this trend is the 2015 invalidation of the U.S.-EU Safe Harbor Framework by the Court of Justice of the European Union.[15] While preventing misuse of certain types of technology and protecting the privacy of individuals are both legitimate goals, if

[11] FFIEC Information Technology Examination Handbook, *Information Security*, September 2016, *available at* http://ithandbook.ffiec.gov/media/216407/informationsecurity2016booklet.pdf.
[12] Communications Security, Reliability and Interoperability Council IV, FCC, *available at* https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-0.
[13] Communications Security, Reliability and Interoperability Council IV, *Cybersecurity Risk Management and Best Practices, Working Group 4: Final Report*, March 2015, *available at* https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.
[14] National Institute of Standards & Technology, *Small Business Information Security: The Fundamentals*, November 2016, NISTIR 7621, *available at* http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf.
[15] *Maximillian Schrems v Data Protection Commissioner*, https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf.

not handled in a targeted manner, broad restrictions can undermine the security of global cybersecurity infrastructure.

***Global Standards and the Internet of Things (IoT)***. Many of the existing foundational elements that drove the development, evolution, and investment in the modern Internet ecosystem are necessary to harness the potential of the IoT. Adoption of global, consensus-based standards, as discussed above, is critical for providing the interoperability necessary for the IoT to thrive. As the IoT technology landscape comes into greater focus, various global, industry-led standards-setting organizations (SSOs) have formed technical and study groups to ascertain to what extent additional standards development is necessary, including for cybersecurity. These bodies are typically international in scope, drawing experts and participation from across the globe and various industry sectors that will be impacted by and benefit from IoT. It is important for the Department of Commerce and, more generally, all governments to share their needs and requests with these SSOs and, when appropriate, actively participate in these processes.

Federal agencies should similarly support IoT standardization and encourage other governments to follow a similar approach which opts for global standards and approaches rather than undertaking standardization activities that may be duplicative of, or even conflict with, global, industry-led IoT standards. In fact, government, industry, and other stakeholders, through collaborative efforts, have stepped up to address the issue of cybersecurity of connected devices.

Disparate cybersecurity regulations can cause confusion among federal, state, local, and international governments as well as private industry, and multiple legislative efforts to tackle cybersecurity in a disconnected fashion on a sector-by-sector basis can not only cause confusion, but also create a false sense of security for both companies and consumers. Thus, harmonizing cybersecurity policies around a risk management approach informed by international standards can help to optimally allocate resources without imposing duplicative compliance burdens on federal agencies, state governments, and the private sector, while providing better security.

**The fast pace of technological innovation, such as the Internet of Things, accelerates the need for harmonization and adaptability of cybersecurity regulations.**

The IoT is a collection of external devices and sensors that generate data, which, through an Internet connection, can be analyzed to provide actionable information. The range and application of these devices is virtually limitless, but we generally view them in three distinct categories: 1) commercial or industrial; 2) personal or mobile; and 3) household.

Commercial and industrial IoT devices are by far the largest category, and where many of our companies see the biggest opportunity to enhance productivity and efficiencies, improve real-time decision making, and solve critical societal problems. Estimates predict the value of this category will eclipse $7 trillion by 2030.[16] Examples of commercial and industrial IoT include predictive

[16] Accenture, *Winning with the Industrial Internet of Things*, released 2015.

equipment maintenance, facility heating, cooling and lighting management, transportation fleet management and improvement, as well as other large scale uses.

Personal or mobile IoT technologies are likely familiar to most, given the ubiquity of wearable watches, health monitors, and similar devices connecting to the Internet via wireless broadband connections or mobile phones. But the more significant gross domestic product impact will be derived from autonomous vehicles and cars connected to the Internet via cellular or other wireless technologies.

Finally, household IoT applications range from smart appliances to smart thermostats, and intelligent home monitoring and security systems. These products connect through residential broadband or home Wi-Fi networks to provide energy savings and home automation and security benefits.

While IoT is not new – since the Internet was invented, various devices have been connected and networked in attempts to improve convenience, functionality, and other purposes – these now hallmarks of IoT are increasingly achieving much greater success and occurring on a more pervasive scale. Indeed, the rapid growth of networked devices and Internet applications due to the availability of components, Internet service, and the technology that make Internet connection possible – whether we are talking about Smart Grid, Smart Cities, Connected Autos – have us fast headed toward an Internet of Everything. Given this, the U.S. government and other government bodies must look at the underlying technologies and assess where current authority, oversight, and regulation already exist. They should also seek to identify areas where government has taken successful approaches, and replicate that activity in other areas. There are a number of relevant policy areas where authorities already exist, where government is facilitating IoT development, and where industry is working with government to address new or evolving issues stemming from the IoT, including cybersecurity.

Where such regulations, guidance, and oversight do not exist or are ineffective in covering emerging technologies, this should reinforce the importance of creating adaptable, technology-neutral approaches that can outlast new developments in technology.

***Cybersecurity and IoT***. Significant activity continues to take place across both government agencies and the private sector to strengthen our cybersecurity, including for IoT. The interests of government and industry are aligned as both aim to minimize vulnerabilities and create networks, products, and devices that are as secure as possible. Consequently, much of the activity designed to enhance cybersecurity takes place in consultation and close collaboration with the private sector, and we strongly encourage that public-private partnership approach to continue.

ITI's member companies are at the forefront of providing security solutions from devices at the expanding network edge to the cloud, and across the network and IoT. With billions of additional devices coming online, ITI's companies ensure that security is embedded in IoT platforms at the outset of the manufacturing and design process for each new device. Security must be built into

both hardware and software at the outset to ensure there are redundancies, to prevent intrusions, and to create secure and trusted IoT systems. Advances in hardware technology allow for security to be physically built into a system. For example, semiconductor manufacturers can design chips with built-in safeguards. Encryption, for instance, can be baked in at the chip level. Manufacturers can also prevent chips from being rewritten by designing fuses into chips. If a hacker attempts to access or rewrite data, the fuse pops and prevents the data from being rewritten. Similarly, on the network side, devices communicating with the network will require a reliable level of service and connectivity, as well as high security, to prevent unwanted intervention. New Internet protocol architectures are more adaptable and use advanced technologies to pervasively distribute security, treat individual users and devices with an appropriate level of performance and privacy based on their needs, and automate manual processes to improve scale and availability. Application programming interfaces (APIs) facilitate data interactions between edge devices, code modules, applications, and backend IT systems. Organizations can leverage API management software to address security as an architectural challenge in the development of IoT applications.

Federal government stakeholders have a critical role to play in fostering security across the IoT; excellent groundwork has already been laid in this area and should be leveraged going forward. The result of industry partnership with the NIST on the *Framework* is a set of voluntary guidelines, best practices, and standards to help critical infrastructure, businesses, and other private and public actors to better manage cybersecurity risks, including for the IoT.

Taking a similar public-private partnership approach, NIST recently released a *Framework for Cyber-Physical Systems* (the *CPS Framework*),[17] also developed in partnership with industry, academic, and government experts. One of the key working groups in the cyber-physical systems project is focused on cybersecurity and privacy.[18] The *CPS Framework* provides guidance to manufacturers, including detailed technical guidance for building secure products for IoT, Smart Cities, Industrial Internet and other applications. On the flip side, viewing cybersecurity uniquely for each application, whether it be a home computer or an automobile, and mandating prescriptive security checklists is inflexible and will leave industry less able to quickly and efficiently respond to new threats, potentially stifling innovation.

Perhaps of greater concern is the potentially counterproductive precedent of creating siloed approaches to cybersecurity across different ICT applications, as part of the IoT and beyond. As more "things" are connected to the Internet to make our lives richer and more efficient, we do not need to reinvent the wheel when it comes to security, as each of these applications or use cases gains prominence. At different stages of the recent past, policymakers have considered whether new regulatory regimes were needed to better secure CI, the electric grid, cloud computing, or health IT, and in each instance, after close examination, the benefits of approaches grounded in voluntary, consensus-based international standards that both promote innovation and preserve the promise of interoperability have carried the day. The alternative – a world in which we endeavor to

[17] National Institute of Standards & Technology, *Cyber-Physical Systems Framework*, May 2016, *available at* https://s3.amazonaws.com/nist-sgcps/cpspwg/files/pwgglobal/CPS_PWG_Framework_for_Cyber_Physical_Systems_Release_1_0Final.pdf.
[18] https://www.nist.gov/el/cyber-physical-systems/cps-pwg-security

separately regulate each new ICT application or IoT vertical – is not realistically scalable, and simply unsustainable in an IoT world.

Thus, the technology industry constantly works to stay ahead of threats to the IoT, not only through its own solutions, but also in partnership with the federal government. The ICT industry leads and contributes to a range of significant public-private partnerships, including information sharing, analysis, and emergency response with governments and industry peers. In addition to the NIST CPS Working Group and NIST *Framework*, some examples include: 1) NIST Cybersecurity for IoT program; 2) National Telecommunications & Information Administration Multi-stakeholder process on IoT patching; 3) DHS IoT security principles; and 4) Federal Trade Commission (FTC) 2015 Internet of Things Staff Report, among others.

Policymakers and regulators should reinforce this collaborative environment to encourage innovative, public-private cooperation on these issues, rather than top-down regulations that may duplicate ongoing work. Through oversight, policymakers should also better coordinate the many IoT security-related policy efforts currently in progress across the administration.

For example, we were encouraged to see DHS take the lead on IoT security through its publication of non-binding principles in its IoT security guidelines[19] released in November 2016. Industry was given the opportunity to provide input prior to its publication; however, at the time of publication, DHS may not have been fully aware of other federal government efforts around IoT security. For example, following a request from the Information Technology Sector Coordinating Council (IT-SCC) during the DHS IT Sector Leadership Meeting in April 2017, after reviewing the public websites of over 70 Federal Departments and Agencies, the DHS Office of Cybersecurity and Communications (CS&C) staff compiled a list of existing federal IoT projects and highlighted overlap between those projects and CS&C's proposed initiatives in federal IoT procurement guidance, end-user critical infrastructure sector guidance, and smart city guidance. They discovered 30 IoT-related security initiatives across the federal government—from one-time white papers and policy proposals to working groups and fully developed programs and guidance.

Multiple agencies already have workstreams on IoT issues surrounding smart cities, smart grid security, home device security, medical devices, and automobiles, among others. While all may have value in specific industries, and perhaps more broadly to the general IoT security discussion, lack of coordination can minimize the effectiveness of both the implementation of the initiatives and any public-private collaboration that may have contributed to them.

Following its publication of current federal IoT efforts the IT-SCC and DHS are working collaboratively on a specific workstream—providing actionable IoT buying and deployment guidance for public and private stakeholder use. As Congress considers what action, if any, it should take regarding IoT security, before moving forward, we recommend members first use these

[19] Department of Homeland Security, *Strategic Principles for Securing the Internet of Things (IoT),* November 15, 2016, *available at* https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf.

results and conduct a similar evaluation of current laws and existing proposed legislation on IoT security that may overlap or create duplicative requirements on governments, companies, and consumers. Further, if Congress decides to act, it should seek flexible, risk management solutions that are adaptable in multiple industries rather than mandating prescriptive checklists that slow, or even halt, security innovation.

In lieu of IoT security legislation, we recommend Congress act to fill gaps that have already been identified. First, Congress should pass the Developing Innovation and Growing the Internet of Things Act (DIGIT Act),[20] which brings together federal departments with a role in IoT to coordinate activity, including on cybersecurity, and would be a significant down payment on the problem of lack of coordination in development of IoT security best practices.

Second, the Small Business Administration (SBA) has programs to educate small and medium-sized business owners (SMBs) about cybersecurity, provide resources to assess information security resilience, and create customized cybersecurity plans. Congress can reinforce these and other programs by providing more resources to these programs and for agencies to educate SMBs on risk management.

Third, Congress could direct the SBA to work with NIST and Small Business Development Centers to address IoT security by creating, maintaining, updating, and disseminating cybersecurity resources specific to SMBs development, adoption, and use of IoT products.

Finally, Congress could also direct the FTC to work with NIST to create, maintain, and update cybersecurity resources for consumer development, adoption, and use of IoT products so that consumers can look critically at IoT devices.

The IoT is in its very nascent stages and presents us with limitless possibilities if we have the vision and environment to achieve them. We look forward to working with Congress to advance IoT security, and we ask that you evaluate existing policy tools and use caution before taking actions that may inadvertently or unnecessarily impede IoT innovation and disadvantage U.S. competitiveness.

**The federal government should prioritize implementing Section 10 of Executive Order 13636, which clearly contemplated regulatory streamlining, by designating one agency or combination of agencies to assess and coordinate federal agency cybersecurity practices.**

Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*,[21] called for a voluntary, risk-based cybersecurity framework, and that is exactly what NIST produced, with significant input from industry. While we support and value the inherent "voluntariness" of the *Framework* and do not suggest NIST and Congress lose sight of that, it is clear -- given the recent Trump

[20] S. 88/H.R. 686, *Developing Innovation and Growing the Internet of Things Act*, 115th Cong. (2017).
[21] Executive Order 13636, *supra* note 4.

Administration cybersecurity executive order and increasing use of the *Framework* approach internationally and at the state and local level -- that policymakers and regulators are increasingly looking to the *Framework* for inspiration. Indeed, this was anticipated in Section 10 of EO 13636, which contemplated opportunities the *Framework* created for regulatory streamlining. Indeed, then White House cyber coordinator, Michael Daniel, indicated the Obama Administration was "beginning a process to identify federal regulations that are excessively burdensome, conflicting, or ineffective."[22]

We believe more can and should be done to reinforce the *Framework* as voluntary while also embracing its use by regulators to streamline and eliminate superfluous cybersecurity regulations. Reconciling the multiple and often divergent cybersecurity policy efforts across the federal government is becoming an increasingly urgent need. Having achieved widespread cybersecurity awareness, seemingly every federal agency is examining a separate piece of the cybersecurity puzzle through its own lens, often developing their own guidance and/or prescriptive requirements, and leading to an overall cybersecurity approach more reminiscent of a patchwork than a coordinated strategy. Instead, to fully realize the benefits offered by the IoT and innovations such as Big Data Analytics, the federal government should promote policies that help break down barriers to connecting devices and correlating data.

How can we accomplish this? The key is that the *Framework* should not serve as the impetus or rationale for extra layers of regulation—that's not regulatory streamlining, it is regulatory redundancy, and multiple layers of redundant regulations will not create better cybersecurity for anyone. Rather, it can be held up as a voluntary risk-management based tool around which policymakers and regulators should orient their efforts to improve cybersecurity. While not the perfect or only solution, doing so will help reduce regulatory redundancy.

EO 13636 required agencies to "1) assess the sufficiency of existing regulatory authority to establish requirements based on the *Cybersecurity Framework* to address current and projected cyber risks; and 2) identify proposed changes in order to address insufficiencies identified."[23] Several agencies released reports,[24] and concluded "existing regulatory requirements, when complemented with strong voluntary partnerships, are capable of mitigating cyber risks to our critical systems and information."[25]

Thus, we recommend this administration and Congress complete what the prior administration did not—consult CI partners within and outside the federal government to identify those ineffective, duplicative, or burdensome regulations and take action to eliminate them. President Trump has

---

[22] Michael Daniel, *Strengthening Cyber Risk Management*, February 2, 2015, *available at* https://obamawhitehouse.archives.gov/blog/2015/02/02/strengthening-cyber-risk-management.
[23] Michael Daniel, *Assessing Cybersecurity Regulations*, May 22, 2014, *available at* https://obamawhitehouse.archives.gov/blog/2014/05/22/assessing-cybersecurity-regulations.
[24] Department of Homeland Security, *Executive Order 13636—Improving Critical Infrastructure Cybersecurity*, Reports, 2014 *available at* https://www.dhs.gov/publication/eo-13636-improving-ci-cybersecurity; Department of Health & Human Services, *Executive Order 13636, Section 10(b)—HHS Assessment*, May 12, 2014, *available at* https://www.phe.gov/Preparedness/planning/cip/Pages/eo13636.aspx; Environmental Protection Agency, *Drinking Water and Wastewater Resilience*, 2014, *available at* https://www.epa.gov/waterresilience.
[25] *Id.* at Department of Homeland Security, *Executive Order 13636—Improving Critical Infrastructure Cybersecurity*, Reports, 2014.

taken initial steps to examine and streamline regulations through two executive orders that would 1) require elimination of two regulations for every new regulation and prudent cost management of planned regulations;[26] and 2) create regulatory reform officers within each agency to implement regulatory reform initiatives and policies, including reducing the number of regulations and controlling regulatory costs.[27]

Efforts to improve IoT cybersecurity, and overall federal cybersecurity, should leverage public-private partnerships and build upon existing initiatives and resource commitments. Working together, federal government partners, including DHS, NIST, and the White House, can work with industry to help spearhead a regulatory streamlining effort to rationalize not only IoT security initiatives, but also overall federal government cybersecurity regulatory efforts.

**Reform government acquisition procedures to allow for deployment of agile federal procurement processes to acquire cybersecurity products and services, and align corresponding guidance among agencies for consistent application across the government.**

Improving and strengthening our nation's cybersecurity posture is rightly a top priority for our government and changing how the federal government integrates cybersecurity into its own acquisition process for procuring of goods and services will help improve federal government cybersecurity resiliency. Over the last few years, the federal government issued several cybersecurity orders[28] and regulatory measures to enhance cybersecurity resiliency within the federal government and CI controlled by the private sector. Federal agencies recognize the need for greater control over federal network security, and have thus created their own unique cybersecurity acquisition systems and regulations.

With a lack of coordination by OMB, agencies will continue to perpetuate a patchwork of requirements for contractors, and each agency will develop their own cybersecurity requirements for acquisition purposes. Federal requirements on contractors to sell cyber products and services and to protect federal data and information are growing, and industry is concerned over the increasingly complicated regulatory landscape they face to ensure information assurance while providing services to federal agencies.

Illustrative of the number of overlapping and potentially conflicting requirements contractors currently face is the following inventory of ongoing regulatory actions:

- Department of Defense (DoD) Final Rule on Network Penetration and Contracting for Cloud Computing;

[26] Executive Order 13771, *Reducing Regulation and Controlling Regulatory Costs*, January 30, 2017, *available at* https://www.whitehouse.gov/the-press-office/2017/01/30/presidential-executive-order-reducing-regulation-and-controlling.
[27] Executive Order 13777, *Enforcing the Regulatory Reform Agenda*, February 24, 2017, *available at* https://www.whitehouse.gov/the-press-office/2017/02/24/presidential-executive-order-enforcing-regulatory-reform-agenda.
[28] EO 13636, *supra* note 4; and Executive Order 13691, *Promoting Private Sector Cybersecurity Information Sharing*, February 13, 2015, *available at* https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari.

- DHS Safeguarding of Controlled Unclassified Information Proposed Rule;
- OMB's proposed guidance on cybersecurity protections;
- DHS Class Deviation 15-01 Safeguarding of Sensitive Information;
- NARA Safeguarding of Controlled Unclassified Information Final Rule;
- DoD, GSA and NASA Basic Safeguarding of Contracting Information Systems; and
- Anticipated Federal Acquisition Regulations (FAR) clauses on these topics (along with the fact that the FAR does not currently address the existing regime).

This complexity of cybersecurity regulations is burdensome not only to current contractors, but also to new entrants and small businesses.[29] In some cases, existing contractors are exiting the federal marketplace because of the regulatory compliance cost. For instance, small businesses' implementation of the DoD network penetration rule is burdensome and not affordable. Recently, DoD and DHS initiated efforts to reach out to Silicon Valley to explore ways for more non-traditional ICT companies to sell their products and services to the federal government.[30] Setting many complex and confusing rules can create an impediment for agencies to accomplish what DoD and DHS seek—small business and non-traditional players as federal government suppliers. In 2016 alone, approximately 7 rules were issued impacting contractors.[31]

We recommend that Congress direct OMB to develop guidance to create an efficient and effective cybersecurity acquisition infrastructure. OMB should harmonize cybersecurity regulations for federal agencies to ensure that they are applied consistently across the entire federal enterprise. Without such management, this array of new requirements, regulation, and guidance will add further confusion for the acquisition community, increase the compliance burden for both the government customer and the vendor community, and significantly increase costs to the taxpayer for the technology goods and services the government mission requires.

Finally, Congress should reform government acquisition procedures to allow for deployment of agile federal procurement processes to acquire cybersecurity products and services, and align corresponding guidance among agencies for consistent application across the government. The federal government procurement system cannot keep up or stay ahead of ever-growing cybersecurity threats. According to the *State of Federal IT Report, "*Agency CIOs sometimes anticipate that potential acquisitions will take up to two years to ultimately select a vendor. A result of this delay is that technologies that are considered state-of-the-art when a new procurement is envisioned are often outdated by the time a contract is awarded. The lengthy procurement process can also create significant barriers to improving the cybersecurity posture of an agency because of difficulties in rapidly procuring and deploying innovative, cutting-edge cybersecurity technologies."[32] We recommend Congress incentivize agencies to use more agile processes, such as

[29] https://www.crowell.com/files/Contractors-Caught%20in-the-Cyber-Minefields-More-Rules-and-Greater-Confusion-for-Public-Sector-Cybersecurity.pdf.
[30] DHS Silicon Valley Program, *available at* https://www.dhs.gov/science-and-technology/hsip; DoD Diux Program, *available at* https://www.diux.mil/.
[31] http://www.natlawreview.com/article/more-cybersecurity-changes-expected-contractors-2017.
[32] State of Federal IT Report, pg. 120, January 2017.

those used in the private sector, to procure cybersecurity goods and services and harmonize all regulations with which contractors must comply.

**Conclusion**

The ICT industry is constantly innovating and is committed to facilitating the protection of our customers, including governments, businesses, and consumers. Security is essential to the federal government mission and should no longer be treated and addressed in a patchwork, uncoordinated fashion. Allowing the furtherance of uncoordinated security approaches will simply perpetuate a security regime that is only as strong as the weakest link. This committee's oversight of cybersecurity regulation harmonization will be critical to developing effective and efficient cybersecurity policies for the federal government, particularly our critical infrastructure, which, in turn, impact the private sector.

We stand ready to provide you any additional input and assistance in our collaborative efforts to develop balanced policy approaches that help all of us to collectively improve cybersecurity risk management and resilience while avoiding duplicative and costly regulations.

I thank the chairman, ranking member, and members of the committee for inviting me to testify today and for their interest in and examination of this important issue. I look forward to your questions.

Thank you.