COMMISSION ON ENHANCING NATIONAL CYBERSECURITY

Meeting of the Commission on Enhancing National Cybersecurity

PANELIST AND SPEAKER STATEMENTS

University of Minnesota

Minneapolis, Minnesota

August 23, 2016

Table of Contents

Dr. Massoud Amin

Mr. Chairman, Distinguished Commissioners, panelists, NIST staff, Colleagues and guests. Good morning. I am Massoud Amin, and on behalf of the University of Minnesota Technological Leadership Institute, more commonly referenced as TLI, we welcome you. We are honored to host this timely meeting and thank you for your leadership in helping ensure the security of our nation.

The University of Minnesota has had a long, distinguished history of pioneering contributions to security. I have had the distinct honor to be a part of it as a professor of electrical & computer engineering where I continue my R&D projects toward secure self-healing smart grids and as director of the Technological Leadership Institute. For nearly three decades, TLI has been developing the next generation of technological leaders through our Master of Science degrees, and since 2009 in the Master of Science Security Technologies degree program. Our more than 1300 alumni of our graduate programs are successfully innovating in all areas of technology in more than 400 enterprises - and nearly 180 of them are focused on security – including the areas in today's dialogue, which we cover in the Security Technologies degree program here at the University.

You will hear from experts who will provide a summary of the State of our cyber security– Activities, Accomplishments, Opportunities and Challenges ahead. We will also review the evolving spectrum of cybersecurity threats and countermeasures, which continue to improve yet poses novel threats, in several areas including:

- Challenges confronting consumers in the digital economy
- Innovation (Internet of Things, healthcare, and other critical infrastructure areas)
- Assured products and services.

The more recent spectra of vulnerabilities (privacy concerns in an increasingly interdependent digital world, cyber-attacks and sophisticated malware, to personal privacy, safety and security) have been in the spotlight while our national and international critical infrastructures face new challenges.

Critical infrastructures such as energy, power and electric power grid, banking and finance, oil/gas/water pipelines, transportation, food/agriculture, health services, manufacturing, public health, financial systems, and telecommunications information networks including the Internet and embedded digital systems have become increasingly important, interdependent, critical and complex.

The security challenges of protecting human safety and the critical infrastructure in the United States and throughout the World have been highlighted during the last few decades. Worldwide cyber-attacks are on the rise with evolving spectra of threats and more sophisticated adversaries:

First, cyber-related RISK is significant:

The threat is real - The Vulnerabilities are widespread - And the Consequences can be disastrous

Cybersecurity threats represent one of the most serious national security, public safety and economic challenges we face as a nation. Understanding the dynamically evolving threats and emerging risk and our ability to assess and manage quickly changing risks is more important now than ever before.

President Obama's executive order, of February 12, 2013, highlights the cyber threat is one of the most serious economic and national security challenges we face as a nation and that America's economic prosperity in the 21st century will depend on cybersecurity. It provides a "framework" to effectively allow intelligence to be gathered on cyberattacks and cyber threats to privately owned critical national infrastructure — such as the private defense sector, utility networks, and the banking industry — so they can better protect themselves.

The very technologies that empower us to lead and create also empower those who would disrupt and destroy… our public and private enterprises, including corporate and government networks are constantly probed by intruders.

Our daily lives and public safety depend on power and electric grids, but potential adversaries could use cyber vulnerabilities to disrupt them on a massive scale. The Internet and e-commerce are keys to our economic competitiveness, but cyber criminals have cost companies and consumers hundreds of millions of dollars and valuable intellectual property.

Second, the challenges abound:

- Telecommunications and information processing (our) systems are highly susceptible to interception, unauthorized electronic access, and related forms of technical exploitation,
- And technologies to exploit these electronic systems is widespread and is used extensively.

BOTTOM LINE: The RISK is significant and the issues numerous and growing.

The answer to these challenges will undoubtedly take extended our discussions today.

In addition, since I was asked by the Commission to provide my input on addressing Digital Security and recommendations for action, enclosed please find an addendum outlining my detailed thoughts and recommendations provided for your reference on the next few pages. These are a subset recommendations, which I drafted in partnership and on behalf of the IEEE to advise the U.S. President's Quadrennial Energy Review (QER). Our team completed a report that provides guidance on grid-related developments to the U.S. Department of Energy and the White House for the nation's first-ever Quadrennial Energy Review.

As noted therein, the cost of developing and deploying a modernized, stronger, more secure and smarter critical infrastructure for the country is cost effective and should be thought of as an investment in the future.

In closing, I thank you for bringing this important dialogue to the University of Minnesota. We welcome our continued collaborations and look forward to maintaining our place together at the forefront of proactively addressing and confronting these security challenges.

*** * * * Thank you * * * ***

Addendum:

Question 1: *What do you feel is the most important thing the electric regulatory industry should accomplish over the next five years?*

Answer: It is imperative that we reduce uncertainty for investments in the grid, in innovation and research and development, in modernizing entire systems and encouraging development of capable human capital. Think systems, be forward thinking, be strategic, know the past, be open to innovation, develop a fresh outlook at what can realistically be achieved—what are the resultant primary, secondary and tertiary consequences? I quote HL Mencken, "For every complex problem, there's a single solution that is simple, neat and wrong!" Develop capabilities to understand and address such interdependent complex systems. As these systems interact with each other, there are many solutions that can come together under what we call design thinking. It involves care, patience, time and resoluteness not to fail. For more information on these thoughts, please read my article, "We are not in Kansas anymore" in the September/October 2011 edition of the Midwest Reliability Organization (MRO) newsletter.

Question 2: What are the persisting security concerns and why can be done?

Answer: As CIP 5 and cyber-physical programs are implemented and protections put into place, difficult choices will have to be made about how to handle a number of trade-offs:

- **Outdated regulatory framework**. One important constraint on regulatory oversight of security protection is the split jurisdiction over the grid, which is keeping us locked into the 20th century infrastructure. The bulk electric system is under federal regulation but the distribution grid, metering, and other aspects of the grid are regulated by individual states. Overlapping and inconsistent roles and authorities of federal agencies can hinder development of productive, public-private working relationships, thus a new model for these relationships is required for infrastructure security. For instance, a stockpiling authority, be it private or governmental, could obtain long lead-time equipment based on the power industry's inventory of critical equipment, which must include the number and location of available spares and the level of interchangeability between sites and companies. Clearly, further standardization of equipment will reduce lead times and increase the interchangeability of critical equipment. For example, the typical, state-level regulatory approach – cost-of-service rate making and volumetric pricing – puts IOUs and microgrids at odds. Most states regulate synchronous interconnections based on IEEE 1547 (please see section 1 of the IEEE QER report for more details) and FERC's small generator interconnection procedures (SGIP) in FERC Order 2006.
- **Controls and Communication** - Protection of power generation, transmission and distribution equipment is insufficient to guarantee delivery of electricity because widespread, coordinated denial of control and communication systems could cause significant disruption to the power grid. This includes SCADA systems, communications between control systems, monitoring systems and business networks. However, the power management control rooms are currently well-protected physically, although they may have cyber vulnerabilities. NERC requires a backup system and there are also manual workarounds in place. The Federal Energy Regulatory Commission (FERC) is working toward a common set of security requirements that will bring all electric sector entities up to at least a minimum level of protection.
- **Investments in security.** Although hardening some key components—such as power plants and critical substations—is highly desirable, providing comprehensive physical protection for all components is simply not feasible or economical. Dynamic, probabilistic risk assessments have provided strategic guidance on allocating security resources to greatest advantage. However, pathways to cost recovery and making a business case for security investments/upgrades, often pose challenges.
- **Security versus efficiency and ROI.** The specter of future sophisticated terrorist attacks raises a profound dilemma for the electric power industry, which must make the electricity infrastructure more secure, while being careful not to compromise productivity. Resolving this dilemma will require both short-term and long-term technology development and deployment along with supportive public policy for cost recovery, which will affect fundamental power system characteristics, spurring development of new business models/strategies.
- **Centralization versus decentralization of control.** For several years, there has been a trend toward centralizing control of electric power systems. The emergence of regional transmission organizations, for example, promised to greatly increase efficiency and improve customer service. But we also know that terrorists can exploit the weaknesses of centralized control; therefore, smaller and local semi-autonomous systems would seem to be the system configuration of choice (analogous to platoons during warfare with local autonomy, while coordinated with the overall mission of the operation). In fact, strength and resilience in the face of attack will increasingly require the ability to bridge simultaneous top-down and bottom-up decision-making in real time—fast-acting and totally distributed at the local level, coordinated at the mid-level and aligned with executive objectives.

What are some specific examples and actions required to improve security and resilience of the system?

POLICY REMAINS THE SINGLE BIGGEST INFLUENCE ON THE BUSINESS CASE

Example -- Microgrids: A 2013 white paper, "Results-based Regulation: A Modern Approach to Modernize the Grid," addresses the limitations of cost-of-service regulation and offers alternative regulatory models that each state could consider adopting.

A recent study of policies relating to microgrid adoption in Minnesota reveals that state regulatory policies often don't address microgrids at all. But the Minnesota study suggests that state policy define and acknowledge the opportunities presented by microgrids to achieve state policies regarding energy surety and the adoption of renewable energy sources and to "ensure that microgrids are properly valued and considered in energy resource and policy initiatives." The Minnesota study identified both regulatory and legislative steps to achieve these objectives. FERC policy covers DG-related projects up to 20 megawatts (MW) and how they interconnect with interstate transmission systems, relevant if the project plans to sell wholesale power into an independent system operator (ISO). FERC has issued a NOPR that it will amend its SGIP and SGIA (small generator interconnection agreement) to "ensure the time and cost to process small generator interconnection requirements will be just and reasonable and not unduly discriminatory".

State-level PUCs wield the most influence. Many states are reviewing related policies as they balance utility interests with ESCO competition and the needs of the commercial/industrial and residential utility customer sectors. A state-level, results-oriented regulatory approach that rewards utilities for adopting innovations that directly benefit their customers may encourage microgrid adoption.

In terms of a federal role in microgrid-related policy development, states will continue to exercise (and defend) their role in microgrid-related policy-making. With access to resources – possibly facilitated by the U.S. DOE – on related technology and standards, regulatory reform and stakeholder impacts, however, state regulators can create policies that favor microgrid development and balance the diverse interests involved.

FERC's small generator interconnection procedures (devised by SGIP, embodied in FERC Order 2006) also are relevant to this discussion.

State policies may also need to evolve with standards through a regular, consistent process, both to encourage microgrid development and reward utilities for cooperating with a customer benefit that cuts into its revenue. Policy and standards should work in hand-in-hand.

One area ripe for revision: Where a state has a restrictive definition for DG capacity for its interconnection requirements. Current rules require large microgrid proposals to forge unique agreements with a utility at great cost and uncertainty.

California regulators have articulated many of the issues that policy must address, as has the National Regulatory Research Institute. [20] Both efforts provide an in-depth look at the complexity and interrelated nature of many microgrid-related policy issues as utilities, independent system operators, ESCOs, customers and other stakeholders are linked technologically and in wholesale and retail markets.

Critical regulatory issues currently being reviewed include, among many others:

- How costs and benefits are apportioned to myriad stakeholders (and how that affects cost recovery for utilities),
- Whether a microgrid relies on the distribution system (or transmission system) for backup and how that might affect reliability,
- Whether and how to treat non-utility microgrid sponsors as utilities, and
- Multiple possible business models for utilities offering microgrids.

Metrics, Best Practices, and Roadmaps: Establish metrics on workforce and identify policies that facilitate necessary workforce development activities by the regulated companies. There is a

workforce crisis coming that could affect customer services and costs so it is in the public interest that regulators increase their oversight of workforce development.

Select a lead organization (perhaps DOE) to facilitate regulator / industry dialog by designing and holding workforce workshops for NARUC, FERC and NERC that create situational awareness for state and national regulators. The NERC System Operator Certification and Training program should be used as an example of a successful program for regulated training. Initially the focus should be on the workforce whose performance is most directly connected to reliability, such as system operators, linemen, planning engineers, protection engineers/technicians and substation operators. DOE can convene a cross functional group of experts to include industry, government agencies (DOL, DOE, NSF, DHS, and DOD) and regulators for the purpose of reviewing current practices in workforce benchmarking and create metrics to quantify the threat posed to the electric grid's performance by insufficient replacement workers. DOE could seek out opportunities to co-fund industry education and training programs (IEEE examples include Scholarship Plus, WISE, Plain Talk) and fund student and innovation competitions.

Improving Existing Survey and Assessment Tools: In generation, FERC has in the Form-1 a large amount of the material needed to support an assessment of the adequacy of the generation fleet. There are operational and maintenance aspects that are not included in the Form-1. FERC Forms 714 and 715 provide some, but not all of this information and Form 556 provides information on smaller generation facilities. Again the existing FERC data would not provide a complete survey, but it is a strong starting point to develop survey results from. For sales, forecasts, usage, and other consumption related information the Energy Information Agency (EIA) provides the best starting point.

Recommendation for a survey of the electrical infrastructure:

- Bring together the industry and end-user stakeholders to look at the existing survey tools, and define the overall needs for an industry wide set of survey tools. This working group should provide a clear requirements document on what needs to be surveyed, and the depth that the survey needs to cover.
- Determine what existing materials can be used to support the survey requirements, minimizing new data collection.
- Provide adequate resources to complete a survey tool set that supports the requirements that were developed by the stakeholder group and uses the data from existing sources.
- Working with an industry working group, define how the survey tool will be used both improving the infrastructure and in any regulatory actions. The tool set will fail, if there is no consensus among the stakeholder groups. A solid survey tool set for both self-assessments will provide a data driven way for the industry to determine where to focus research, standards development, training, staffing, and operational improvements for the industry. With the rapid changes in the environment this will allow the better deployment of scare resources.

Pertinent IEEE QER recommendations[1] to the U.S. DOE, for your consideration:

Markets and Policy

- Use the National Institute of Standards and Technology (NIST) Smart Grid Collaboration or the NARUC Smart Grid Collaborative as models to **bridge the jurisdictional gap** between the federal and the state regulatory organizations on issues such as technology upgrades and system security.
- More transparent, participatory and **collaborative discussion** among federal and state agencies, transmission and distribution asset owners, regional transmission operators (RTOs)

[1] http://www.ieee-pes.org/component/content/article/158-uncategorised/749-qer

and independent system operators (ISOs) and their members and supporting research is needed to improve these parties' understanding of mutual impacts, interactions and benefits that may be gained from these efforts.

- Continue working at a federal level on better **coordination of electricity and gas markets** to mitigate potential new reliability issues due to increasing reliance on gas generation; and update the wholesale market design to reflect the speed at which a generator can increase or decrease the amount of generation needed to complement variable resources.

Asset Management:

- Support **holistic, integrated approach** in simultaneously managing fleet of assets to best achieve optimal cost-effective solutions addressing the following: **Aging infrastructure, Grid hardening (including weather-related events, physical vulnerability, and cyber security) and System reliability.**
- **Urgently address managing new Smart Grid assets** such as advanced metering infrastructure (AMI) and intelligent electronic devices.
- Encourage utilities to investigate practical measures to shorten times to replace and commission equipment failures due to extreme events or other reasons.
- In the case of long-duration interruptions, all utilities should adopt improved measures to provide customers with a timely estimate of when power is to be restored.
- When extreme events occur it is important for post-event reviews to determine impacts and lessons learned for better management of future events.
- Infrastructure security requires a **new model for private sector-government relationships**. Overlapping and inconsistent roles and authorities hinder development of productive working relationships and operational measures.
- Perform **critical spares and gap analysis**. A detailed inventory is needed of critical equipment, the number and location of available spares and the level of interchangeability between sites and companies. Mechanisms need to be developed for stockpiling long lead-time equipment and for reimbursement to the stockpiling authority, be it private or government. Other approaches include standardizing equipment to reduce lead times and increase interchangeability.
    - U.S. DOE should continue to work with industry to ensure that the protection of spares and all assets is carried out and that transportation of large equipment is feasible. We further recommend actions that might lure domestic manufacturing back into the U.S. for units 300 KV and above. (Progress in this area has been made with post-9/11 efforts initiated by EPRI's Infrastructure Initiative in September 2001 to March 2003, as well as with the EEI STEP (Spare Transformer and Equipment Program), which has been in place since 2004. Utilities should also continue to work with industry and manufacturers to expand the existing self-healing transformer programs, such as efforts now underway by EPRI and ABB. Further, many utilities have mutual aid agreements on spares.
- Increased federal R&D for emerging technologies that may impact T&D grids, including new types of generation, new uses of electricity and energy storage, with an additional focus on deployment and integration of such technologies to improve the reliability, efficiency and management of the grids.
- Application of proactive widespread condition monitoring, integrating condition and operational data, has been shown to provide a benefit to real-time system operations, both in terms of asset use and cost-effective, planned replacement of assets.

Reliability, Security, Privacy, and Resilience

- Facilitate, encourage, or mandate that secure sensing, "defense in depth," fast reconfiguration and self-healing be **built into the infrastructure**.
- Mandate consumer data **privacy and security for AMI systems** to provide protection against personal profiling, real-time remote surveillance, identity theft and home invasions, activity censorship and decisions based on inaccurate data.
- Support alternatives for utilities that wish to reduce or eliminate the use of wireless telecom networks and the public Internet where there might be concerns about increased grid vulnerabilities. These alternatives include the ability for utilities to obtain private spectrum at a reasonable cost.
- Improve **sharing of intelligence and threat information** and analysis to develop proactive protection strategies, including development of coordinated hierarchical threat coordination centers – at local, regional and national levels. This may require either more security clearances issued to electric sector individuals or treatment of some intelligence and threat information and analysis as sensitive business information, rather than as classified information. National Electric Sector Cybersecurity Organization Resource (NESCOR) clearing house for grid vulnerabilities is an example of intelligence sharing.
- Speed up the development and enforcement of **cyber security standards**, compliance requirements and their adoption. Facilitate and encourage design of security from the start and include it in standards.
- Increase investment in the grid and in R&D areas that assure the security of the cyber infrastructure (algorithms, protocols, chip-level and application-level security).

Robert Booker

Chairman Donilon, Vice Chairman Palmisano, and distinguished members of the Commission, thank you for the invitation to appear today and discuss the critical topic of cybersecurity. This topic is vital to our Nation and the healthcare industry that I am honored to serve.

My name is Robert Booker and I am the Chief Information Security Officer of UnitedHealth Group. I have served the company in this role since 2008. We are a highly diversified health and well-being company serving virtually every constituent of health care – patients, physicians and other care providers, hospitals, out-patient clinics and life sciences researchers, private and public sponsors of health benefits, state and federal government agencies, payers, regulators and others. Our enterprise has one mission: to help people live healthier lives, and help make the health system work better for everyone. The people I serve with are dedicated to continuously improving the quality of our performance for the individuals and customers we serve. Five key values guide our operations and every interaction: integrity, compassion, relationships, innovation and performance.

UnitedHealth Group is built on two business platforms: UnitedHealthcare, providing a broad range of affordable health benefits to serve the health care needs of people at every life stage; and Optum, for health services, analyzing data to create actionable information, improving consumer engagement and access and strengthening the performance of the care delivery system.

In addition to my role at UnitedHealth Group, I also serve on the Board of Directors of the Health Information Trust Alliance, most commonly referred to as HITRUST. HITRUST was founded in 2007 by a collection of security leaders across health insurers, health providers and health technology companies for the purpose of collaboratively addressing information security for all segments of the healthcare industry, including insurers, providers, pharmacies, PBMs and manufacturers. HITRUST is focused on elevating the level of information protection in the healthcare industry, facilitating collaboration between industry and government, and improving the competency level of information security professionals in healthcare.

Innovation in Support of Health Outcomes

The pace of innovation and availability of new and disruptive technologies has great potential to improve health outcomes for patients and their families. The potential includes solutions that enable individuals to live healthier lives, solutions to support families facing health challenges, and an improved ability for those individuals and families to successfully manage chronic conditions. Innovation is a health imperative for our nation when considered against the backdrop of needs:

1. **Health and Wellness** – over 80 million individuals in the US are considered obese with 79 million of those considered pre-diabetic. Multiple solutions have entered the market in support of weight loss, weight management and fitness training.
2. **Living Independently** – 77 million individuals in the U.S. are classified as "Baby Boomers" and 42 million families care for an elderly parent or adult. 25% of children and adolescents live with a chronic health condition.
3. **Condition Management** – 26.8 million non-institutionalized adults are diagnosed with heart disease. 16 million people are living with diabetes. 42 million people have hypertension.

The Internet of Things and their potential for aiding health outcomes includes devices focused on individual consumer health and devices that support chronic disease management. Current solutions are traditionally focused on narrow outcomes such as fitness monitoring, digital lifestyles, glucose management and weight management. The potential for broader health outcomes requires the ability to harness information from multiple devices, leverage analytics to provide data driven solutions, and assess patterns and relationships from that analysis to provide a holistic view of an individual's health.

As one example, support of independent living may be enhanced by giving secondary caregivers the capability to monitor their loved ones remotely and non-invasively. This is possible through the

integration of smart home technologies and fitness technology in conjunction with claims and pharmaceutical data. The desired approach is to support caregivers with an individual's daily status based on living patterns that can be key indicators of potential health events. Detected changes in routine can then be flagged for possible attention by a secondary caregiver. Such an approach will enable individuals to live at home with a better quality of life while focusing assistance in areas of need.

IoT technologies that support independent living include motion and door monitoring, fitness monitoring, audio monitoring, weight monitoring, and activity monitoring. However, the range of devices that may be applied to this important need have different interfaces, are designed on different service quality models, and are manufactured and supported for different consumer markets. A unification strategy is thereby required to achieve the desired outcomes.

Optum's unified approach to this innovation challenge considers application programming interfaces to address the range of device standards, a common approach to data analytics, and careful consideration of the narrowest set of information from such devices in support of the desired health outcomes while respecting privacy considerations. This is the innovation backdrop and integration challenge that cybersecurity must support.

Industry Backdrop

The health system in our country is a unique ecosystem that serves and integrates a range of constituents ranging from some of the nation's largest and most complex organizations to small care teams, and individual providers serving in rural communities. Regardless of size and cybersecurity awareness, all entities in the health system have a shared mission focused on the delivery of healthcare and health services to the patients and members that we serve. The distinctions of size and corresponding ability to invest in security have a bearing on the residual information and cybersecurity risk that faces the health system.

Healthcare organizations and providers are also responsible for meeting multiple regulations and security standards focused on the protection of protected health information as well as personally identifiable information. This personal and health information is both sensitive and significant in scale. And, the health industry has not been immune from the cybersecurity attacks facing our nation – both insurers and providers have been victimized by publicized attacks. These range from large and significant data breaches to smaller cyber-extortion attacks that have impacted care delivery at hospital systems and by clinical providers.

Risk Management Framework

The potential of new devices, evolving approaches to information technology delivery, and the varying cybersecurity awareness across the industry provide a complex backdrop against which to innovate. This complexity and the active threat landscape together create the potential to impede adoption of technologies that can improve health outcomes, improve quality of life, and serve the population. The health industry therefore requires an adaptive and flexible risk management framework to address regulatory and practical security obligations facing the industry.

A large subset of leading companies in the healthcare industry, through HITRUST, have developed such a risk management framework. The HITRUST Common Security Framework ("CSF") is a central component of the risk management framework and integrates and harmonizes discrete and authoritative sources of cybersecurity guidance into a single, flexible, and prescriptive control library that can be used by all types and all sizes of healthcare organizations. Today, over 80 percent of hospitals and health plans, as well as many other healthcare organizations and business associates, have adopted the HITRUST CSF.

Innovation requires both speed and agility, which is why the industry reviews and updates the CSF at least annually to ensure it remains relevant to the changing healthcare threat environment. The review takes into account changes in underlying regulations and standards and also considers best

practices and lessons learned from past events, security incidents, incident response exercises, and industry post data breach experiences. An adaptive and evolving risk management framework will provide an important foundation for health innovation.

Third Party Assurance

Innovation and the drive to improve health outcomes will combine the insights, technology and research from a variety of health and consumer-focused companies serving a variety of industries. That innovation and the relationships between those companies must be delivered in the healthcare industry's regulatory framework including required safeguards for electronic protected health information. An assessment and reporting mechanism to support these shared obligations is also needed to support needed collaboration while streamlining third-party risk management.

Industry leaders, including major health insurers and business associates, are using the risk management framework referenced above in support of third-party assurance. The objective is to reduce the overhead associated with different assurance processes required by different health companies to common industry suppliers. This common assurance program for third-party risk management will result in significant reductions in the cost and level of effort to measure foundational security requirements and ensure that they are sustained across the industry.

A further outcome of third party assurance is a common risk and controls vocabulary and lexicon. This common understanding is foundational to a shared understanding of risk and a unified control framework where multiple parties provide elements of the total control environment. A consistent understanding will improve the pace and quality of execution which are critical success factors to successful industry collaboration and innovation.

Cybersecurity Considerations

Residual risk of data breaches remains even as companies implement their respective security programs and provide each other assurances around how they will protect sensitive information. And, innovation and an increased reliance on electronic information will increase the overall inherent risk faced by these companies especially when considered against the interdependencies and complexity of the U.S. health system.

As a result, a number of healthcare companies are focusing on a resiliency approach based upon the NIST *Framework for Improving Critical Infrastructure Cybersecurity*.[2] The industry's focus in this area, including active collaboration with the public sector, helps organizations respond to incidents and minimize the impact of incidents where they occur.

The industry supported the development of implementation guidance and supplemental materials to address the specific risks of the Healthcare and Public Health sector and the healthcare operating environment. The resulting *Healthcare Sector Cybersecurity Framework Implementation Guide*[3] ("Guide") is based upon a collaborative effort between industry and the government via a working group co-chaired by HITRUST and the Office of the National Coordinator for Health Information Technology. This collaboration and the resulting Guide supports implementation of a sound cybersecurity program that helps organizations assess and improve their level of cyber resiliency.

The Guide explains the relationship between the NIST Cybersecurity Framework and the HITRUST risk management framework, and how the HITRUST risk management framework provides a model implementation of the NIST Cybersecurity Framework for the healthcare industry. The Guide also

---

2 NIST (February 12, 2014). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0. Gaithersburg, MD: Author. Retrieved from http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

3 Joint HPH Cybersecurity WG. (May 2016). Healthcare Sector Cybersecurity Framework Implementation Guide, Version 1.1. Washington, DC: Author. Retrieved from https://www.us-cert.gov/sites/default/files/c3vp/framework_guidance/HPH_Framework_Implementation_Guidance.pdf.

provides implementation guidance including a mapping of HITRUST CSF controls to the NIST Framework's subcategories which are similar to control objectives in other frameworks. The resulting implementation of a common risk management framework will result in cybersecurity resilience and more consistent understanding between companies collaborating and innovating together in the industry.

Cyber Collaboration

And, lastly, operational cybersecurity support requires active collaboration including the sharing of threat information and indicators of compromise. This sharing is aided by incident response exercises conducted locally, regionally and nationally.

In 2012, the industry, through HITRUST, launched a cyber-threat intelligence sharing and analysis program for the healthcare industry. This program provides for collaboration between the Department of Homeland Security (DHS) and the broader industry cyber-intelligence community for analysis, support, and the exchange of threat intelligence. The resulting program evolved into a cyber-threat exchange (CTX) program that accelerates the detection and response to threat indicators targeting healthcare.

A number of industry companies invest in CTX through HITRUST and the program is offered to the industry free-of-charge. The process of automatically collecting and analyzing cyber threats and distributing actionable indicators in electronically consumable formats (e.g. STIX, TAXII and proprietary SIEM formats) assists organizations of all sizes and cybersecurity maturity. HITRUST is also a federally recognized Information Sharing and Analysis Organization (ISAO) with strong relationships with Federal partners including DHS and the Federal Bureau of Investigation (FBI).

Industry exercises provide an important mechanism to build awareness and ensure that communication alignments occur in response to incidents including the possibility of industry-wide cybersecurity events. The industry and HITRUST developed CyberRX in response to this need. CyberRX is now in its third year and delivers a series of industry-wide tabletop exercises developed to simulate cyber-attacks on healthcare organizations and evaluate the industry's preparedness against attempts to disrupt U.S. healthcare industry operations. Exercises are healthcare specific and are intended to address broader considerations including the targeting of information systems, medical devices, and other essential technology resources. Observations and lessons learned are analyzed to identify general areas of improvement for industry. The result is a series of recommendations for the industry and government including opportunities to enhance information sharing between healthcare organizations and government agencies.

Closing Remarks

Innovation in support of health outcomes is critical to our population. And, cybersecurity risks will remain and require ongoing vigilance. However, as technology evolves, a common foundation that supports engagement between companies and ongoing cybersecurity collaboration is critical to achieving the promise of new technologies against the current threat landscape. A risk management framework, mutual and shared assurance, and active collaboration in cyber resilience and cyber response together provide this foundation around which innovation can flourish.

On behalf of the UnitedHealth Group and our Optum and UnitedHealthcare entities, I thank the Commission for the opportunity to provide these comments and for your support in considering how we enhance cybersecurity for our Nation.

Edna Conway

To each of the distinguished members of the Commission, I express my and Cisco's appreciation for the opportunity to share insight regarding this critical area for our nation. I am Edna Conway and I have the privilege of serving as Cisco's Chief Security Officer for its Global Value Chain.

A Pervasive Security Approach to Trustworthy Technology

In a global digital economy, successful national cybersecurity requires an intertwined platform of collaboration, function and security. Security is not cybersecurity alone, rather cybersecurity must be part of a comprehensive security strategy.

A comprehensive strategy demands an architecture that designs, deploys and monitors the right security in the right place at the right time. The key to doing so is the value chain.

What is a value chain? Here is what I mean by today's value chain: the end to end lifecycle for hardware, software or services that deliver value.

Value Chain Stages

I offer for consideration foundational elements to build a value chain security strategy[4]:

- Retaining a third party value chain member's flexibility to deploy the right physical security, operational security and security technology, in the right stage of its own ecosystem. This allows for the proprietary innovation that our ecosystem members bring to the table.
- Applying a risk-based approach to the deployment of value chain security in order to ensure economic and operational viability. Namely, evading perfection being the enemy of progress.
- Avoiding proliferation of certification or accreditation schemes or guidelines. Leveraging those already in place should allow swifter implementation, broader adoption and further security enhancement. These include standards such as ISO 27001 "Information Security Management," ISO 27036 Part 3 "ICT Supply Chain Security," ISO 20243 "Mitigating Maliciously Tainted and Counterfeit Information & Communications Products," and NIST SP 800-161 "Supply Chain Risk Management Practices."

Given these foundational elements, the next step is building a flexible security architecture for the value chain.

Core Domains for a Value Chain Security Architecture

We suggest identifying core domains within the architecture. Consider the following:

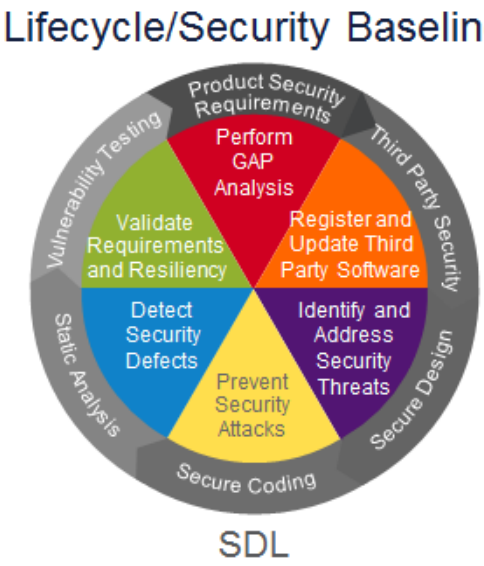
[4] These foundational elements must be adapted to the spectrum of value chain services and solutions. Examples in the Information and Communication Technology (ICT) value chain include components, systems, logistics, cloud services, and design services to name a few.

	Domain	Description
1	Security Governance	The security governance domain details requirements for an overall governance strategy to manage value chain security and compliance related risks by establishing requisite policies, standards and procedures.
2	Security in Manufacturing and Operations	The security in manufacturing and operations domain details requirements for manufacturing and operating procedures in order to protect material assets, intellectual property and information.
3	Asset Management	The asset management domain details requirements for securing IT and manufacturing assets throughout their life cycle.
4	Security Incident Management	The security incident management domain details requirements to establish a robust incident management process that should be followed for activities such as logging, recording and resolving of security incidents and anomalies.
5	Security Service Management	The service management domain details requirements, a) for the delivery of services in accordance with agreed upon delivery timeframes, quality and security levels, and b) establishing a business continuity plan/program in an event of service disruption.
6	Security in Logistics and Storage	The security in logistics and storage domain details security requirements that should be followed during storage and distribution of raw materials, inventory and finished goods.
7	Physical and Environmental Security	The physical and environmental security domain details requirements that value chain members must design and implement to control access to facilities, equipment and resources, and to protect personnel and property from damage, harm or unauthorized alteration.
8	Personnel Security	The personnel security domain details requirements to ensure that all value chain personnel who have access to any proprietary items, intellectual property and confidential information have the required authorizations, training, and contractual agreements including appropriate clearances, if required.
9	Information Protection	The information protection domain details requirements for protection of proprietary data through its lifecycle, such as data classification, handling, cryptographic controls and disposal. It also lists the requirements to be implemented on information systems that store or process intellectual property.
10	Security Engineering and Architecture	The security engineering and architecture domain details requirements to be followed during design, development, testing and rollout of products (tangible and intangible) and services.
11	3rd Tier Partner Security	The 3rd tier partner security domain details requirements focused on information security controls that must be implemented at downstream value chain members (4th parties, e.g. cloud service providers) in relation to procurement of goods and services.

Leveraging an architecture touching upon these domains can allow value chain members to effective collaborate and drive comprehensive security. The domains can also serve as an approach to embedding security (including cybersecurity) into government procurement.

Two key elements of Domain 10 are (i) focus on protection at the design/develop stage and (ii) customer transparency regarding the inevitable product security incident and mitigation solutions. We propose that consistent adherence to a robust Secure Development Lifecycle (SDL), which is repeatable, measurable and adaptable to varying development methods (e.g. Agile and Waterfall), can

increase the resiliency and trustworthiness of products. Further, a transparent Product Security Incident Response practice reflecting the results on continuous monitoring, the security impact of incidents, and mitigation methods is essential to the goal of assuring Trustworthy Products. Fundamental parts of an SDL include:



Layered physical and operational security along with security technology and development, and mitigation processes across the entire value chain can allow value chain members to effectively collaborate and drive comprehensive security. Inclusion of value chain security into government procurement can serve to increase assurance of delivery of trustworthy products.

I remain committed to being of service as you may deem appropriate.

Joshua Corman

Introduction:

Chairman Donilon, Vice-Chairman Palmisano, and distinguished members of the Commission, thank you for the opportunity to testify today on the need for Trustworthy Products in the Internet of Things.

My name is Joshua Corman. I am the Director of the Cyber Statecraft Initiative for the Atlantic Council[5] – a non-partisan, international policy think tank. I am also a Founder of I am The Cavalry (dot org)[6] – a volunteer, cyber safety initiative focused on public safety and human life in the internet of things. I am an adjunct faculty for Carnegie Mellon University's Heinz College. Lastly, I serve on the HHS Cybersecurity Task Force – initiated by Congress in the Cybersecurity Information Sharing Act of 2015.[7]

Trust, Dependence, and Confidence:

Markets are built on a foundation of consumer confidence; national and international security rely on trust.

The trust we place upon connected technology has outpaced their trustworthiness. Software introduces new modes of vulnerability; connectivity exposes us to new adversary classes. Our vulnerability and exposure are growing exponentially; our ability to defend is growing linearly.

Through our over dependence on undependable IT, we have created the conditions such that the actions any single outlier can have a profound and asymmetric impact on human life, economic, and national security.

"Our dependence on connected technology is growing faster than our ability to secure it – in areas affecting public safety and human life."

The phrasing for our founding "I am The Cavalry" problem statement was deliberate. When we're depending upon something that is unfit, we can make it more dependable – or depend upon it less. Many of these hyper-connected dependencies may be unsound – until such a time as they are worthy of the trust we already place upon them.

I'd like to focus my testimony on some uncomfortable truths, and more importantly, on the necessity of pursuing uncomfortable responses to rise to these challenges.

The Era of Consequential Failures:

The Internet of Things is not merely a security issue, nor a privacy issue.

The Internet of Things is **where Bits & Bytes meet Flesh & Blood**.

It's hard to argue that our cyber security best practices are working even in traditional applications. About 100 of the Fortune 100 have had a loss of intellectual Property and trade secrets. Nearly every breached retailer was compliant with PCI DSS. Breaches are getting bigger in both scale and impact like Target and Ashely Madison. Breaches are hitting Federal Agencies like the Pentagon and OPM. On a long enough timeline, our failure rate is approximately 100%; and that timeline is shrinking. We've not been sufficiently motivated (yet) to take corrective actions, because the losses have been acceptable (e.g. a 4% annual fraud rate).

Security failures are still less a function of how much we resource our defenses; more a function of the presence, focus, appetite of our predators. We are prey.

---

5 https://atlanticcouncil.org
6 https://iamthecavalry.org
7 https://www.congress.gov/bill/114th-congress/senate-bill/754

Failures are getting dangerous as we connect everything in the Internet of Things – such as the denial of patient care at Hollywood Presbyterian Hospital in California due to Ransomware.[8] With IoT, we're leaving the era of low consequence failures and acceptable losses. The consequences of failure will be measured in human lives, in material impact to GDP, in international peace & prosperity, and in the compromise of liberties and inter/national values – not merely eroded but **shattered** by a crisis of confidence. These emerging safety critical IoT uses are decades behind "best practices" – and even if they were to catch up, we will need far better and very different ones.

At some point, the costs of inaction eclipse the costs of action. Few people change until the pain of maintaining inertia exceeds the pain of making change. It is in our nature to wait for proof of harm and compelling events before initiating corrective actions – and in these cases, our unplanned and emotional responses can be protracted, malformed, compound harm, and delay lasting & effective remediation.

How IoT and Safety Critical Security are "different":

Most of our (debatably) "best practices" are highly tuned for financially motivated adversaries, with confidentiality impacts, in managed corporate environments, with common technologies, and established economics and time scales. As Greg Rattray previously testified, JPMC has over 2,000 security staff and is spending over $600M on IT security.[9] When this level of investment can't stop a motivated, determined adversary, how can a pacemaker patient hope to protect herself from harm?

Here is an over-simplified list of material differences across the various types of IoT. Differences in:

- *Adversaries*: Motivations, Objectives, Capabilities, Will
- *Consequences of Failure*: Life & Limb, Physical Damage, Market Stability, GDP, International and National Security
- *Context & Environments*: Operational differences, Migratory, Perimeter-less, Inaccessible, Difficult to Patch/Replace
- *Composition of Goods*: Hardware, Firmware, Software
- *Economics*: Margins, Buyers, Investors, Costs of Goods, Regulatory, Depreciation
- *Time Scales*: Time-to-Live (TTL), R&D Cycles, Response Times

A clinical medical device may face less talented, but more aggressive adversaries. IS/IL ideological adversaries wishing to inflict fear and loss of life (potentially combined with a Boston Marathon-like physical attack), against more open networks, using end-of-life operating systems, or incredibly expensive "heavy iron" where the hardware investment is meant to last for 15+ years, yet which harbors known defects from several years ago.

We must stop assuming "no one would hack XYZ". When we connect everything to everything else… with abysmal basic Cyber-Hygiene… attackable with free tools and exposed nakedly to the internet. It doesn't matter what most would do - it matters what one might do.

To this point. TriCk is an existence proof of why we're running out of time – of someone with the requisite Means, Motive, and Opportunity to inflict harm upon others. Tomorrow marks the one year anniversary of the killing of TriCk – aka Junaid Hussain - the former hacker from Anonymous' Team Poison moved to Raqqah and was recruiting and training hackers for the CyberCaliphate to attack their enemies. What they may lack in the resources and skill of a National State, they more than make up for in their willingness to use it. Sadly, we're not making it very hard for future TriCks to follow and pick up his mission – here and abroad.

---

8 http://www.csoonline.com/article/3033160/security/ransomware-takes-hollywood-hospital-offline-36m-demanded-by-attackers.html

9 http://www.nist.gov/cybercommission/upload/May_16_Panelist_Statements.pdf

The Promise and the Peril:

Connected Automobiles: According to NHTSA, 32,675 US lives were lost in 2014 (up ~ 8% in 2015) – 94% due to human error and human choice.[10] The promise of Autonomous or Semi-Autonomous vehicles could save around 100 lives per day. That said, an exotic death due to car hacking could shatter the confidence of the public in these otherwise life-saving technological advances.

Connected Medicine: The promise of telemedicine could dramatically advance the quality and availability of care and improve our lives. The promise of precision medicine and machine learning could enable the breakthroughs that end our most vexing medical challenges. That said, sustained denial of patient care would trigger a retreat to less vulnerable, but also less advanced models of care.

Humans adopt technologies for their immediate, obvious benefits, but we seldom to the costs/benefit analysis of the less obvious, deference costs and risks. We love our benefits; we just can't afford them all. We're addicted to technology adoption and we're amassing unsustainable levels of technical and security debt. Our situation is not unlike the Sub-Prime Mortgage Crisis, Compound Derivatives, and *The Big Short*.[11] Waiting for the collapse is too late to get in front of it. We seldom see the inflection point until we're being crushed by it.

Tactics (Security Labels/Signals & Supply Chain Transparency to enable/support free market forces):

It took decades to get us into this situation; it may take a decade or more to get us to a more tenable and sustainable state. The most immediate corrective actions can include Security Labels/Signals & Software Supply Chain Transparency to enable and unlock Free Market Forces and corrections.

Security Labels:

2 years ago, *I am The Cavalry* published a "5 Star Automotive Cybersafety Framework" to catalyze multi-stakeholder collaboration and achieve *safer* outcomes, *sooner*, if we work *together*. This January we published a comparable "Hippocratic Oath for Connected Medical Devices" in concert with the FDA's DRAFT Post-Market Guidance and Cybersecurity Workshop. Both recognize as a given that "all systems fail" and expect manufacturers to be prepared for failure (and transparent about how). Essentially, the guidance asks manufacturers to tell the market how they:

1. Avoid Failure (Safety by Design)
2. Take Help Avoiding Failure (Third Party Collaboration – Vulnerability Disclosure Programs)
3. Notice & Learn from Failure (Evidence Capture)
4. Respond Quickly to Failure (Security Updates)
5. Contain & Isolate Failure (Segmentation & Isolation - of Critical Systems from Non-Critical Systems)

The full 5 Star & Hippocratic Oath can be found at https://www.iamthecavalry.org/ These were not meant to be the finish line, but rather the starting line. Sadly, without government mandate and/or incentivizing, we may not see adoption of even these basic five ready postures for failure before 2025.

For run-of the-mill consumer IoT, even basics like "State if you are patchable – and for how long do you commit to offering patches" could allow adequate supply to be paired with increasingly informed demand.

Software Supply Chain Transparency & Cyber Hygiene:

Known Vulnerabilities are a public health issue. While I was the CTO for Sonatype, we were the custodians of the largest free repository of open source software components in the world: Maven

[10] http://www.nhtsa.gov/About+NHTSA/Press+Releases/2015/2014-traffic-deaths-drop-but-2015-trending-higher

[11] https://en.wikipedia.org/wiki/The_Big_Short

Central. As a security professional, I studied the global consumption rates of which projects, which versions, which vulnerable versions were consumed, and if or how quickly the fixes were taken.

Initially I studied which open source projects addressed Known Vulnerabilities best. Dan Geer (CISO of In-Q-Tel) and I published findings[12] that showed only 41% of the Known Vulnerabilities ever got fixed, and the ones that were fixed had a Mean-time-to-Remediate of 391 Days. While some projects fixed most of their dependency vulnerabilities, others fixed few or even none. In the absence of transparency of these risks, manufacturers assume supply chain vulnerabilities are unavoidable and do not take action.

Next we studied thousands of applications in the market. while there is variety by type and age of application, modern software is about 90% assembled from 3rd party and open source software components. Much like automotive manufacturing, software too has a supply chain… we just don't manage it like one (yet). A typical application has about **106** 3rd party & open Source components (parts). By ratio, almost a quarter (**23%**) of that count totaled the known vulnerabilities (unique CVEs). This avoidable, elective attack surface is also bad for business, as they can trigger unplanned, unscheduled work for developers, service interruptions for operations and business operations, and protracted Mean-time-to-Identify and Mean-time-to-Repair. When an outbreak like Heartbleed or BashBug or Apache Commons Collections is being exploited in the wild, these delays give asymmetric advantage to our adversaries. In fact, to tie this back to life & limb, the Ransomware that infected large portions of hospitals was an avoidable, Known Vulnerability in a Medical technology product supply chain.

Over the past 4 or so years, I've been working on a rubric – based on Edwards Deming's proven Toyota Supply Chain principles from the 40s and 50s. Three supply chain principles made for more reliable and profitable manufacturing:

1. Use fewer and better suppliers of parts
2. Use the highest quality parts from those suppliers
3. Track which parts went where, so that when something invariably goes wrong, you can issue a prompt, agile, and targeted recall.

These software supply chain principles are being voluntarily and enthusiastically adopted in Agile and DevOps organizations – as a way to drive efficiency. This has been one of the most adopted patterns pushed through my Rugged Software and Rugged DevOps work.

On the market enablement/correction side, a trio of requirements has been attempted and adopted in a number of places in response to the feeling that organizations can no longer size nor manage their 3rd party IT risk. This trio is loosely embodied in procurement language/requirements in a few places:

1. Ingredients: Provide a Software Bill of Materials (BoM) of the 3rd party and open source software parts (w/ versions) used in your products (ideally machine readable)
2. Hygiene: That list should not contain Known Vulnerabilities (CVEs in NVD) without a justification (the key is transparency)
3. Patch-ability: Because future vulnerabilities are inevitable, your products must be patchable in a reasonable time frame (terms set in support language)

Such a trio allows for benefits including:

1. At development, producers of goods will be conditioned to avoid elective attack surface and vulnerability when cost neutral, less vulnerable, compatible versions are readily available.
2. At procurement time, buyers can leverage this transparent hygiene to affect purchasing decisions in a free market – based upon their risk appetites, and other factors.
3. In operations, when a new attack like the hospital Ransomware or Heartbleed is in the wild, organizations can immediately answer two questions: a) Am I affected? B) where am I

[12] https://www.usenix.org/system/files/login/articles/15_geer_0.pdf

affected? This streamlines corrective action and reduces adverse outcomes including physical harm.

It is worth noting that a few larger players in the software industry had very pronounced negative reactions to even the transparency of a Software Bill of Materials. While it may be difficult to get from current state of unmanaged hygiene to the desired state of reasonable hygiene – when these known vulnerabilities can lead to loss of life, we must take action. Deming introduced these efficiencies **to advance** business goals – decades before Nader's *Unsafe at Any Speed* raised automotive safety concerns. Moreover, such a standard of care for Known Vulnerabilities may insulate and bound any eventual Software Liability regime – which many feel is inevitable now that software can affect flesh & blood (albeit challenging to design/implement well).

These principles are gaining free market momentum.

- ABA/FSSCC "Purchasers' Guide to Cyber Insurance Products"[13]
- FS-ISAC (Financial Services – ISAC) "Appropriate Software Security Control Types for Third Party Service and Product Providers"[14]
- UL Cybersecurity Assurance Program[15]
- Mayo Clinic and ExxonMobil Procurement Language[16]
- H.R.5793 Cyber Supply Chain Management and Transparency Act of 2014 (Government in the role of buyer, as opposed to regulator)[17]

While much of the private sector talks about sophisticated, state sponsored adversaries, Known Vulnerabilities play into far too many public and high profile breaches. Further to our benefit, the adversaries most likely to inflict harm are relatively less skilled and resourced than others may be. Improving basic hygiene of low hanging fruit of Known Vulnerabilities may be the equivalent of a reinforced cockpit door for airplanes – a highly effective, relatively lower cost security measure taken after 9/11.

The bottom line is… Today's consumers cannot tell good products or vendors from bad ones. We keep hearing a strong preference for voluntary, free market forces instead of government legislation or regulation. But… at several points in history, legislated/regulated transparency is the very thing that fixes free market forces. In these cases, the role of government is to do the fine-tuning and alignment that lets them stay out of the way and lets markets adapt to an ever changing technology landscape.

Mid to Long Term:

While it is initially prudent to pick the "low hanging fruit" and solve the easy and uncontroversial problems, what that leaves you with are the really, really hard and controversial ones. As such, we must boldly pursue uncomfortable, unobvious potential solutions to our emerging challenges. This posture will necessarily require exploring the dark and uncharted edges of the map and is likely to challenge conventional wisdom, entrenched institutional beliefs, and put people outside of their comfort zones.

Software Liability (The elephant in the room):

I gave a talk a few years ago suggesting Software Liability may be the worst possible idea – except for all others. For a number of reasons (many very good reasons) we've put off any form of Software Liability. Against the list of valid reasons not into introduce software liability (which I can enumerate)

---

13 https://www.fsscc.org/files/galleries/FSSCC_Cyber_Insurance_Purchasers_Guide_FINAL-TLP_White.pdf

14 https://www.fsisac.com/sites/default/files/news/Appropriate%20Software%20Security%20Control%20Types%20for%20Third%20Party%20Service%20and%20Product%20Providers.pdf

15 http://www.ul.com/cybersecurity/

16 Perrin, Dan. "A new narrative on cyber security". The Hill. May 4, 2016. http://thehill.com/blogs/congress-blog/technology/278712-a-new-narrative-on-cyber-security

17 https://www.congress.gov/bill/113th-congress/house-bill/5793

– there is a large and growing list of reasons to introduce it – in a thoughtful, measured, and plan-full way. With a compelling event or case law, done wrong, introducing liability could destroy the software industry. Done right, it is economic, in the interest of the public good and public safety, and could even be stimulative to catalyzing real and measured cyber insurance.

Risk burdens should be placed on those in the best position to manage and avoid risk. Today, a producer of software who makes a risk decision for its customer, is under no obligation to tell their customers the risks it is passing on to them (think transparency), and can not be held liable for harms which manifest upon their customers. The situation is untenable.

Further, markets want to be efficient. One role of a market is to reveal true costs and place the cost burden on the least cost avoider in the system. This may adjust the cost of goods, but the system wastes less and can spend liberated time and resources on purchasing new goods and services.

Many think Software Liability is inevitable – if not imminent now that IoT failures have physical consequences.

Grand Challenges:

Necessity is the mother of invention. Much like the Space Race, the Moonshot, and the Manhattan Project, Apollo 13 (and even "The Martian"), grand challenges and (inter)national imperatives are the crucibles that uncover and birth innovations, inventions, and breakthroughs which we can re-purpose and use to benefit defenses, markets, and other challenges – as collateral benefit. Let's science the heck out of this.

It is our hope, that such a focus and leadership can raise literacy, catalyze new thinking, experimentation & capacity building such that we can avoid or dampen any confidence shattering events. Regardless, we must stimulate discussion, debate, and preparedness in the case that true failures are required to initiate corrective action.

The Cuyahoga River in Ohio caught on fire more than 20 times before we finally instituted the Clean Water Act and other action. Our fear in waiting for our Cyber Cuyahoga moment – be it in connected cars, in smart cities, in massive healthcare outages and losses of life – is that our response times will take years. In other words, response will look a lot less like a routine update to a mobile device, and a lot more like a Deep Water Horizon, with sustained suffering and incredibly long tails of costs and harm.

Again, it took decades to get us into this situation; it may take a decade or more to get us to a more tenable and sustainable state. We're unlikely to have that much time. We must begin. We must begin now.

Susan Grant

I'm Susan Grant, Director of Consumer Protection and Privacy at Consumer Federation of America (CFA), an association of local, state, regional and national consumer organizations and state and local government consumer protection agencies from across the Unites States. I appreciate your inviting me to speak with you today about the challenges confronting consumers in the digital economy. The challenges are many, from unfair and undisclosed digital rights restrictions to Internet fraud, problems with interoperability to systems failures such as the recent computer meltdowns at Southwest and Delta Airlines. My focus today will be on concerns about privacy and security. I am not a technologist, which is a good thing for my work on these issues, because my views are from the perspective of the average consumer.

Consumers want and need to use digital products and services

The Internet and digital products and services have become essential parts of our lives. We use them to access government services; to buy and sell things; to bank, invest and borrow; to pay our bills; to raise money for charitable causes and make donations; to create art, music and literature; to obtain health care services; to teach and to learn; to keep in touch with friends and family; to publicly share our experiences; to entertain ourselves and others; and to participate in our democracy. Seventy-two percent of Americans own smartphones and 89 percent use the Internet, according to a February 2016 Pew Research Center study.

Indeed, we have little practical choice about using the Internet and digital products and services. Many government benefits are delivered electronically. Smart cards are replacing cash and tokens for public transportation. In some communities smart meters are mandated for our homes. Other appliances that were once "dumb," such as refrigerators, are being turned into digital devices that do much more than the basic functions they used to perform, including track our behavior. Dedicated short range communications services will be installed in new cars starting next year. Some schools require students to use computers. Electronic health records systems are being implemented. In some cases, the only way to communicate with companies, obtain owners' manuals, and get service when we have problems is online. We live in a brave new world built on ever-accelerating technological advances.

These advances can help make our lives easier and safer, save us time and money, spur creativity and civic discourse, and enlarge our voices individually and collectively. But they can also make us more vulnerable to commercial and government surveillance, unfair discrimination, anti-competitive practices, and identity theft and other hazards.

Consumers are concerned about their privacy and security but have little control

Privacy is a fundamental human right, but in the U.S. we lack a comprehensive legal framework to protect it. Instead, we rely on narrow sectoral laws and self-regulation, leaving huge gaps. For example, the privacy of our health care records is protected but the data generated by Fitbits and other wearable health devices and health-related apps are not. While financial institutions are under some legal constraints concerning the collection, use and sharing of our personal information, most businesses are not. There is no federal law that requires them to even disclose their privacy practices or to give us any say in what they do. For instance, we have no privacy protection under federal law for the one of one of the most intimate types of personal data, our facial images. The privacy best practice recommendations for the commercial use of facial recognition technology are so weak that even if they were widely adopted, they provide no meaningful privacy protection. The privacy of our telephone records is protection, but there is a fierce battle underway right now over the Federal Communication Commission's (FCC) proposed rules to protect the privacy and security of the personal information that our Internet Service Providers can derive from our online activities.

Verizon's acquisition of Yahoo is the latest illustration of the fact that these days, the product or service that is being provided may be ancillary to the *real* commodity, our personal data. Information about us – our financial situations, our health conditions, our sexual orientations, our affiliations, our

interests, our political positions, and more is gleaned from our activities online and offline, across platforms, analyzed, combined into digital dossiers and used by companies and their affiliates and business partners, or sold to the highest bidder, for profit. We have little insight or control over the accuracy of this information, who has it, and how its use may impact us. Are you receiving solicitations for prime loans while I'm being solicited for predatory financial products? Are you seeing a different price than I am for the same product or service? Are you being unfairly discriminated against on the basis of "big data?" Can your personal information be used in ways that might embarrass you? You can get your credit score and understand the factors that go into it, but do you know about the secret scores that are being compiled about you?

Most descriptions that are provided about companies' privacy practices are deliberately opaque and any controls that consumers may be offered are usually unclear and fairly limited. Where the default is placed matters, and for the most part the burden is on consumers to opt out, rather than on the data collectors or users to obtain their affirmative agreement. AT&T's "pay for privacy" option for some of its high-speed Internet services is wrong-headed because privacy shouldn't be an option only for those who can afford to pay more – it should be everyone's right.

But don't consumers want to exchange their personal information for a discount or other benefits? As a 2015 study showed, that's a fallacy. Consumers recognize that they have little control and that the deal is lopsided. Their resignation should not be interpreted as enthusiasm. Surveys show that consumers are concerned about their privacy and the risks of disclosing their personal information, even to save money.

Consumers are also concerned about the security of their personal information. A government study showed that 19 percent of Internet-using households reported that they had been affected by an online security breach, identity theft, or similar malicious activity during the 12 months prior to July 2015. It seems that not a day goes by without another data breach in the news. Consumers should do what they can to secure their own devices and use safe online practices. But when the data is out of their hands there is nothing they can do to secure it – they have to trust that the data holder will do so. Most of the data breach bills that have been introduced in Congress are not about improving security, they are about setting weak requirements for data breach notice and preempting states that have stronger standards.

When consumers' information is compromised, whether through breaches or trickery such as phishing, it is important to not only learn from the experience in order to prevent it from re-occurring in the future but to mitigate the damage and help consumers recover from whatever fraud might have resulted.

The "Internet of Things" exacerbates concerns about privacy and security because of the amount and sensitivity of data that can be collected about us will increase dramatically and the consequences of privacy or security failures can potentially be far more severe. It is urgent to address privacy and security issues now, rather than wait until business models based on the unfettered collection and use of our personal information, coupled with the lack of investment in adequate security, become so entrenched that it will be impossible to change the facts on the ground. Business will innovate within the public policy parameters that we set.

While my focus today is on privacy and security in the marketplace, there are challenges for digital consumers in government's collection, use and security of personal information as well.

Recommendations for government and industry

- **Privacy should be the default.** We should be asked for our consent before our personal information is used for purposes other than those for which we provided it and not be forced into agreeing or to pay to protect our privacy.

- **Data security should be automatic.** We don't allow consumers to use unsafe products. We have safety standards and recalls. We shouldn't let consumers use unsafe digital products and services. Security should be built in.
- **Industry should be required to protect consumers' privacy and security.** We need enforceable laws, not more self-regulation, which has not sufficed and never will.
- **The Administration should back rulemaking for privacy and security.** The Administration should express strong support for the FCC's broadband privacy and security rules and advocate for the Federal Trade Commission to have the ability to promulgate such rules for the business sectors over which it has jurisdiction.
- **The United States should establish a Data Protection Authority**. We need a central authority that will coordinate government policies concerning privacy and security.
- **A central source should be created to access data brokers and the information they hold.** We have a central source through which consumers can access the credit reporting agencies and their credit reports. This gives them the ability to see what information has been collected about them and correct it if it is inaccurate. We need a similar system for data brokers.
- **Government agencies should consider privacy and security in promoting technology.** For instance, we support calls for the FCC to require car manufacturers to implement privacy and security safeguards in using the spectrum that they have been allocated for the operation of dedicated short-range communications services in automobiles.
- **Government should support the development and use of secure communications tools and technologies such as encryption.** Policies that prevent or undermine these tools expose consumers and businesses to unwarranted security threats.
- **Measures should be mandated to protect consumers' data from abuse.** The Administration set a good example by requiring both chip and PIN for credit cards used by the federal government. Two-factor authentication and other security measures should be encouraged and the use of Social Security numbers as identifiers for purposes other than validation for government benefits should be eliminated.
- **More should be done to educate consumers about privacy and security.** That education should begin early in schools and there should also be more support for programs to educate adults. This will require a major and sustained effort by government, industry and nonprofit organizations and adequate resources.

Mike Johnson

Good morning Chairman Donilon, Vice Chairman Palmisano, and members of the Commission. I would like to thank you for the opportunity for the Technological Leadership Institute (TLI) to participate in this critical conversation through hosting the commission meeting and presenting on this topic today. TLI has a long history of digging into technology and security challenges to contribute to the discussion, which hopefully leads to meaningful changes. Our unique structure that includes programs for Management of Technology, Security Technologies, and Medical Device Innovation affords us an opportunity to view this issue from a slightly different perspective as our institute works to address the integrated issues across our three programs. The ongoing escalation of cybersecurity threats is one of those critical issues that demands targeted attention, as failing to provide meaningful improvements in this security arena will have potentially devastating impacts to the interconnected and dependent industries and functions that support the strength of the United States economy.

Cybersecurity threats and their intersection with consumers is a central concern in this issue as economic related activity and even delivery of many basic services is heavily dependent on internet connected systems and the millions of users interacting with them. In consideration for improving the state of security around this issue I have four areas of focus for my comments today.

Consumer trust and confidence

Gaining and maintaining consumer confidence is a concept that has been discussed by providers of online service since the first transaction systems appeared on the internet. Initially the concern for providers was demonstrating competence to the potential customer to prompt them to interact with the new technology and delivery approach, frequently with the goal of reducing costs at or even the need for physical locations. Today this consideration has matured well beyond basic customer adoption of delivery channels and is foundational to the continued viability of our current economic and delivery models. All of the recommendations discussed today should support the goal of increasing the confidence that users of these critical systems have in fully engaging but feeling that their personal data and other assets are properly secured.

Shared accountability

- The nature of securing interactions between users and providers online places responsibility for different aspects of the security posture on both sides of the transaction. The consumer must understand and follow best practices to protect themselves from endpoint risks and the provider is obligated to both secure the transaction itself as well as any information collected as part of that transaction throughout the lifecycle of the relationship. This shared responsibility introduces confusion and ambiguity that impacts the user's ability to feel confident that all aspects of security are accounted for.
- Businesses, government, and advocacy groups have long been increasing the quantity and quality of information provided to the user population with the intent of improving the security awareness on the consumer side of the transaction. These efforts, while important, cannot be the only layer of controls available to protect the endpoint issues in this relationship.
- Businesses and other online providers must augment the user awareness control layer with technology controls that assist in alerting both the user and the provider that there may be a problem with the security of the transaction, either due to connectivity risks or endpoint issues like poor configurations or infected customer systems. There are currently tools available that attempt to address this space but their use is inconsistent and the quality not assured. More effective tools are needed to support this need, and broader usage and standardization would likely also improve the quality of the system.
- Oversight of this arena has historically been distributed among multiple regulatory agencies and industry groups, and there is a lack of consistency in the expectations for providers, the level of oversight conducted, and the repercussions to providers for non-compliance or ineffective security controls. A balance needs to be found that provides useful guidance and

consistent enforcement for providers that would bolster user confidence that all parties are investing appropriately and their data is protected. Both regulatory and independent structures should be considered, including hybrids that might leverage peer accountability within industries and real penalties for failure to comply enforced through governmental oversight.

Effective but useable controls

- Innovation is ongoing in the security controls arena, and investment supporting this innovation activity in both commercial and academic environments should be increased. The example of the long hoped for death of passwords should drive our goals for these efforts as effective replacements for currently ineffective and cumbersome identification and authentication methods would not only increase security but I believe have a significant impact on overall consumer confidence and engagement as it represents the most visible aspect of security for the typical online user.
- The tendency for business and regulatory decision makers to accept lesser quality controls in the desire to balance the usability/impact versus effectiveness quandary has often left users unnecessarily exposed. The EMV/Chip card transition is a good example of an industry failing to push for the more effective and equally usable option. Chip and PIN has been in place many years elsewhere, but US cards are Chip and Signature based partially due to perceived consumer issues, cost challenges, and business process resistance. Consumers are ready, or need to be ready, to engage in security controls that have the most effective outcomes.
- Usability of user focused security tools and controls is hampered by the wide variety of systems, processes, and configurations used to implement similar technology between different providers. Standardization or federation of these tools, while exposing the system to potential risk of increased scrutiny by bad actors and broader impact from vulnerabilities, would allow for stronger controls and acceptance by users who would only need to understand one system rather than many systems. Increased standardization can also assist small and mid-sized providers more effectively increase their ability to provide adequate security, ensuring this important sector of the delivery model remains economically viable.
- Risk based controls such as user behavior analysis and authentication escalation should be used more frequently. This will reduce the burden for the vast majority of interactions and reserve the more arduous security processes for higher risk activity. This would be more effectively leveraged in the standardized approach listed above.

Identity as the language of security

- In order for fraud and identity theft related impacts to be successful, confidence in the actual identity of the user interacting with the system needs to be weak. Strengthening identification, authentication, and authorization activities for online interactions could substantially reduce the impact from malicious actors. A stronger system of identification could potentially have positive effects beyond the transaction itself.
- Action has been initiated by NIST to explore a national system of trusted federated identification, but progress seems slow. Increased support from all interested parties including commercial and advocacy groups could help move this important initiative forward and offer increased options for both providers and users.
- Identity initiatives need to be bi-directional to be a truly effective at increasing confidence. Consumers who have confidence in their own identity and authentication process, and also trust the identity of the entity that they are interacting with, are going to be more engaged and feel safer in sharing their sensitive data.

Progress is being made in improving security controls despite what consumers hear regarding breaches and vulnerabilities in the media. A problem with our current path is that it follows whack-a-mole responsive tactics rather than using a holistic approach that includes all providers and increases transparency for improved accountability. It will take a coordinated effort and increased funding

combined with a clear strategy that shares the goals with users giving them increased reason to expect better security to move the confidence level of the typical online user. Thank you for the opportunity to contribute to this discussion and I look forward to future success in supporting users in their online security challenge.

Brian McCarson

Distinguished members of the Commission, I am Brian McCarson, the CTO and Senior Principal Engineer of the Internet of Things Strategy and Integrated Products Division at Intel Corporation. I lead the IoT Technology, Standards and Pathfinding Team and oversee the development of the Intel IoT Platform. In addition to my role at Intel, I also serve on the global Industry Standards Boards of the Open Connectivity Foundation (OCF) and on the Edge Computing Consortium. Thank you for the opportunity to provide our ideas on innovation and recommendations for actions that the Commission can take to enhance our national cybersecurity as we move into the next Administration and beyond.

Intel believes the IoT presents a transformational opportunity for the US and the world. It will enable innovation, increased productivity and new efficiencies across the public and private sector. With an estimated 50 billion devices and 212 billion sensors expected to connect to the Internet by 2020, the IoT offers unprecedented global economic and social opportunity. The IoT presents the opportunity to connect these devices, efficiently analyze the data, and use that knowledge to improve real- time decision making and address societal problems. And in doing so, IoT is expected to have a multi-trillion dollar global economic impact. What should most excite U.S. policymakers is that America and other developed economies are expected to capture 70 percent of this impact, if we lead in addressing the potential barriers to technology adoption.

There are several potential barriers to delivering on the promise of IoT, but none as critical as security. Like Congress, Intel prioritizes security, as each connected device or sensor could also represent a point of vulnerability as a new threat surface that might stifle innovation and adoption. As a result, I would like to propose the following recommendations to counter this possibility.

First, *Establish Security as the Foundation*: it is important that the IoT is secure from the sensor to the cloud, including all hardware and software. Intel believes that the strongest foundation for a secure IoT is integrating security capability at the outset. Starting with the development and design phase of all cyber physical systems and their components, security must be designed in from the beginning. We must also develop infrastructure compute capability and include security algorithms alongside of Internet infrastructure, to enable the attestation of the integrity and authenticity of IoT elements as they move through the hardware manufacturing lifecycle, the software integration phase, user deployment and data creation process. As Intel prioritizes security as the foundational element in our IoT solutions, we are building cryptography into our chips to enable strong identity and data protection. On top of security in the compute device itself, our IoT solutions employ advanced hardware *and* software security to prevent harmful applications from being activated on the device or from taking down the network. Why is this important? Because integrating multiple layers of security at the outset enables trusted data necessary for successful IoT deployments.

An example of an important Intel IoT security technology that is both hardware-based and software-enabled is Intel Enhanced Privacy ID (EPID). EPID may be used for very robust device identity, which is critical for IoT. It is imperative that an IoT system be able to trust that the data it's using is coming from a known and secure device. EPID goes a step further by offering anonymity-preserving properties that allow a device to be securely identified as part of a group, without revealing its specific individual identity within that group. To enable the industry to incorporate this level of hardware security, Intel has released this technology for broad licensing and it has been adopted as an industry standard. Why are these strategies important? Because integrating multiple layers of security at the outset enables more robust IoT deployments and because offering open standards makes security more widespread in the massively-connected IoT ecosystem. The U.S. government should encourage open security standards to maintain the long term viability of IoT and to foster solutions that are interoperable and reusable across a variety of use case deployments, vendors, sectors and geographies.

Second, *Establish a Chain of Trust*: We must be able to rate the trustworthiness of IoT elements, so that users (and the devices or wearables that serve as their proxies) can decide which trusted devices are

safe to connect to or allow connections from, which cloud infrastructure offers the safest haven for data storage, which is the best dataset to use for reliable decision making, and how to gage what constitutes normal versus anomalous behavior in IoT systems. A chain of Trust must be established so that we are able to attest to the trustworthiness of devices during their life cycle, beginning with manufacturing and later during provisioning then deployment. With an established chain of trust, there is a foundation established for trusted analytics and in turn, trustworthiness of the decisions being made from the analytics. Intel believes that all participating IoT elements should be architected to enable some degree of direct measurability, not only for security, but also for reliability, safety, and optimization. Analytics on these measurements can boost our ability to identify anomalies and violations in a timely manner. Technologies such as blockchain also offer promise to validate reported measurements and transactions. To help align the industry toward achieving Trust, it would be beneficial if there were standards-based common criteria that could serve as guidelines to help specify the security goals for IoT systems and how to measure against those goals. One outcome would be for all IoT elements to be able to report the degree to which they meet these criteria, assisting with the evaluation of trustworthiness and the strength of security offered.

Third, *Foster Interoperability*: Interoperability has several dimensions. One aspect is to support interoperability of new devices with legacy devices and legacy infrastructure, neither of which may have been built with required levels of security nor designed for compatibility. Techniques are needed to sandbox legacy systems to reduce security risks, while at the same time enabling interaction between old and new technologies. Another aspect to interoperability is data sharing. There is a strong need for data to be self-describing, to support data aggregation and data analytics. In fact, there is a strong need for all IoT elements to be self-describing, what some in the standards community would call Semantic Interoperability; to capture not only what an element is but its function or role in the larger ecosystem. A third facet of interoperability is to support the inherent compositionality of IoT solutions, which are often composed from systems of systems. It is no longer the case that a single vendor will manufacture the full end-to-end integrated IoT technologies, as might have been the case a decade ago. As a result, trustworthiness is more crucial and calls for open interfaces and APIs that mediate the relationship among specified components. Government-endorsed efforts such as the NIST Smart Cities initiative are good examples of the kinds of interoperability analysis, comparison and testing that must be supported. Towards that end, Intel has contributed the Intel® IoT Platform, which includes IoT reference architectures and a set of IoT ready technologies that provide secure, open, standards-based, scalable and interoperable technology building blocks. In addition, Intel leads, participates and monitors many of the IoT-related standards bodies such as OCF, IIC, OpenFog, ECC, IETF, 3GPP, NIST, IEEE, and others.

Finally, *Accelerate leadership in IoT Security*: How can policymakers accelerate IoT deployments to ensure U.S. leadership? Candidly, the U.S. is behind. Other countries such as China, Brazil and the UAE are aggressively investing in and deploying IoT to transform their economies, address societal problems, and spur innovation. Many have adopted National IoT Plans with time-bound goals and are investing heavily in IoT R&D and infrastructure. The U.S. needs to do the same and needs to act now. Congress can advance our nation's IoT momentum by collaborating with industry to establish a National IoT Strategy that includes a strong security foundation and by encouraging Public-Private Partnerships that uniquely focus on security, yet aim to improve manufacturing productivity, optimize transportation efficiency, reduce energy consumption, sustain our environment and accelerate smart cities and towns. Promoting industry alignment around these large-scale IoT deployments based on secure, open and interoperable solutions will deliver immeasurable benefits and showcase U.S. leadership.

While I have been using the term Security, it is intended as a broad category term to cover Security, Privacy and Trust. To accelerate leadership in IoT Security, we want to be clear that the U.S. must invest in IoT research focused on Security, Privacy and Trust. For example, Intel has partnered with the National Science Foundation to fund academic research in the areas of Cyber Physical System Security & Privacy, as well as Information-Centric Networking in Wireless Edge Networks, both of

which are tackling fundamental security challenges. With the sheer volume of data coming off of IoT devices, it is imperative we foster research that allows us to balance security and privacy. High frequency data in one domain can often leak confidential information from another domain; for instance, smart meters that collect energy data every 10 minutes can reveal not only whole-house energy usage, but other behaviors of household members, including if anyone is home, how many individuals are at home, if they are awake, asleep or working, what specific devices populate the home, etc.

Finally, there is a human element to accelerating cybersecurity leadership. The U.S. must work to create more security professionals, if we expect to be able to embed robust security in our products and infrastructure. For example, DHS and Intel are jointly funding a Cybersecurity Workforce Initiative to support this objective.

In conclusion, we are becoming a smart and connected world. The Internet of Things has the promise of improving our work, our communities, our homes and our lives, but we must design our systems with security and privacy built into them from the outset. Intel is confident that the U.S. can enhance our national cybersecurity with a continued open and joint dialogue as you are doing here today and by implementing these recommendations. I appreciate the opportunity to offer our thoughts and ideas on this important matter, and would like to thank the Commission for their ongoing work and collaboration. I look forward to your questions.

Ken Modeste

Good afternoon Chairman Donilon, Vice-Chairman Palmisano and Distinguished Members of the Commission, my name is Kenneth Modeste and I am the Global Cybersecurity Leader for Connected Technologies at UL LLC. Thank you for the opportunity to appear before you today to share our thoughts on and experiences with improving cybersecurity.

UL has been advancing safety science in the US and around the globe for 122 years that is firmly rooted in the tradition of our founder to always know by test and state the facts. Through investments in research and standards development, UL's 11,000 employees work to increase the adoption of safer, more secure, more sustainable products in the marketplace. UL has promoted consistently the need to work collaboratively with manufactures, retailers, trade associations, public interest groups and international regulatory authorities to further advance safety, performance and security through applied science.

UL continuously work with many industries to assess the safety of new technologies and mitigate new risks through the development of standards and third party certification programs. From our beginnings at the Chicago World's Fair in 1893 and the introduction of electricity to every technological innovation since, UL has been one of the most recognized and trusted resources for advancing safety. In addition to electrical safety, UL's services in the 21st century provide a holistic approach to safeguarding security, performance and global market accessibility in a connected world.

Internet of Things and the UL Cybersecurity Assurance Program (CAP)

The Internet of Things provides great opportunities for increased productivity and capabilities, reduced costs and expanded innovative connected environments. As our world becomes more connected, security increasingly is a major concern for manufacturers and consumers alike as it impacts safety, performance, privacy and market accessibility. Recognizing both the promise and challenge presented by the projected proliferation of the Internet of Things (IoT), UL launched a cybersecurity assurance program called UL CAP to address risks associated with connected technologies. In essence, UL realizes that in a connected world, security has a big impact on safety. UL believes that its UL CAP program aligns with this Commission's goals and objectives to enhance national cybersecurity and promote safe adoption of innovative technologies and ideas.

Not only is security essential for the adoption of connected technologies, but it is an instrumental component for further innovation of the IoT. As with electricity, to become a transformative technology, a foundation of safety and performance needs to be established. The UL CAP establishes criteria in a series of published standards that attempt to address security risks in a wide range of product areas including industrial control systems, medical devices, automotive, HVAC, lighting, smart home, appliances, alarm systems, fire systems, building automation, smart meters, network equipment, and consumer electronics.

UL CAP implements measures to address foundational elements required for good cyber hygiene in the software supply chain. Its primary objective is to manage underlying causes of software vulnerabilities that create the ability to circumvent security controls in products and systems. This program's initial focus on addressing software, provides a uniform mechanism that is applicable to most IoT products and systems in the supply chain; as the common problems associated with software are similar regardless of the product and its use. The program promotes best practices to develop, maintain and support software to mitigate and control security risks that are prevalent today thereby fostering ongoing innovation and deployment of IoT. UL CAP is a voluntary program that industry can support and adopt based on their needs.

Recommendations – UL CAP

Software flaws and weaknesses that are attributable to a majority of the security incidents was a primary driver in developing the technical requirements as part of UL CAP. UL worked with multiple public and private sector stakeholders to build UL CAP to being addressing the causes of some

common flaws and weaknesses by developing standards for testing of products and assessing of organizations within the supply chain.

The UL CAP program has identified two key methods to address software flaws and weaknesses that can potentially cause security vulnerabilities that we would like the Commission to consider. They are:

1. Develop a scientific methodology to assess software in products and provide metrics tied to how software vulnerabilities may be identified and measured as well as the means to address them. The key to deliver on the accuracy of a vendors' claims is the use of a TRUSTED independent third party assessment per published testable and reproducible requirements.
2. Use existing methodologies to provide assessment throughout the supply chain of vendors' ability to execute on security objectives. This begins with manufacturers and their supply chain using established practices to develop, build and support products and systems for sale. System operators, maintainers and asset owners ability on installing, configuring and supporting systems up until decommissioning is imperative to driving consistent supply chain hygiene.

UL CAP Testing and Certification

UL CAP uses the new UL 2900 (Software Cybersecurity for Network Connectable Products) series of standards to offer testable cybersecurity criteria for network-connectable products and systems to assess software vulnerabilities and weaknesses, minimize exploitation, review security controls and increase security awareness. UL CAP is applicable for vendors looking for trusted support in assessing security risks while they continue to focus on product innovation to help build safer, more secure products, as well as for purchasers of products who want to mitigate risks by sourcing products validated by a trusted third party.

UL 2900 is designed to evolve and incorporate additional technical criteria as the security needs in the marketplace mature and industry adopts best practices. One of the elements slated for future editions is expanding beyond software assessment and providing criteria for hardware evaluations.

In utilizing UL CAP, there are several paths an organization can take:

1. Test to specific set of criteria within UL 2900 based on the security maturity of the product. This can provide additional value to a vendor in building their products and systems.
2. Evaluate and test products and systems using the full 2900 set of requirements and once compliance is met, UL can certify the product.
3. Assess the supply chain vendor's ability for building and maintaining products using generally acceptable software development and organizational models.
4. A combination of the above. It provides independently assessed, measurable criteria that purchasers can use to assess the security features of a product and systems.

By choosing one or some of these paths, organizations can begin a process to validate their security claims, and purchasers of products and systems can use this to assess their vendor supply chain.

UL believes that products and systems should be safe, reliable, and secure. As we become a more connected world, security will continue to be a major enabler for manufacturers and consumers alike to adopt newer innovative technologies for the 21st Century. UL believes the UL CAP program provides a framework in support of the Commissions objectives to strengthen cybersecurity in both the public and private sectors, to better ensure public safety, and enhance innovation.

I appreciate the opportunity to speak today and look forward to our continued engagement.

Kevin Moriarty

Statement of the Bureau of Consumer Protection, Federal Trade Commission

Presented by Kevin Moriarty, Senior Attorney, Division of Privacy and Identity Protection

Commission Chair Thomas E. Donilon, and Commissioners of the Commission on Enhancing National Cybersecurity, I appreciate the opportunity to appear before you on behalf of the Bureau of Consumer Protection to discuss the Federal Trade Commission's efforts to protect the privacy and security of consumers' information.[18]

Challenges Confronting Consumers in the Digital Economy

There are a variety of challenges consumers must confront in the digital economy. First, data is collected from consumers at every turn, all day long—on the internet, through their mobile phones, in stores and malls, and through devices in their cars and as they exercise.[19] Many of the companies that obtain consumer data are behind the scenes and never interact with consumers. These companies include hundreds of data brokers that collect and combine data from multiple sources and develop detailed profiles for sale to other companies. As a result, much of this data is collected without consumers' knowledge.

Second, technological developments have enabled the vast storage and real-time processing of data once thought to be cost-prohibitive. As a result, data is now stored for long periods of time and used and re-used for many different, often unanticipated purposes.[20] The companies that obtain and use all of this data may not store it securely, as shown by all of the breaches we are seeing in the marketplace. Indeed, in the last year, headlines have been filled with reports of data breaches impacting millions of Americans. These events serve as a constant reminder that consumers' data is at risk. Hackers and others seek to exploit vulnerabilities, obtain unauthorized access to consumers' sensitive information, and potentially misuse it in ways that can cause serious harms to consumers and businesses. In fact, identity theft was the second top complaint on the list of consumer complaints received by the FTC and other law enforcement agencies this past year,[21] and the Bureau of Justice Statistics estimates that 17.6 million persons—or 7 percent of all U.S. residents ages 16 and older—were victims of identity theft in 2014.[22]

Third, consumers do not have effective ways to learn about these data collection and usage practices and, consequently, make informed choices about them. Privacy policies—once thought to be a tool for giving consumers the information needed to make these choices—are long and legalistic, difficult for the average consumer to read and understand. Consumers are not going to stop what they are doing to decipher them, especially when many of the companies that collect and use their data are third parties they do not even know about.

---

18 Mr. Moriarty's prepared statement, oral statements, and responses to questions are his own and do not necessarily reflect the views of the Commission or of any Commissioner.

19 FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY iv (2014) [hereinafter "FTC DATA BROKER REPORT"], https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

20 FED. TRADE COMM'N, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? UNDERSTANDING THE ISSUES 5 (2016) [hereinafter "FTC BIG DATA REPORT"], https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf

21 FED. TRADE COMM'N, CONSUMER SENTINEL NETWORK DATA BOOK FOR JANUARY – DECEMBER 2015 (2016), https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2015/160229csn-2015databook.pdf

22 BUREAU OF JUSTICE STATISTICS, VICTIMS OF IDENTITY THEFT, 2014 (2015), http://www.bjs.gov/content/pub/pdf/vit14.pdf.

These issues drive much of what the Bureau of Consumer Protection's Division of Privacy and Identity Protection does. Over the past few decades, protecting consumer privacy and security has been a top priority. Although technologies, business models, and the digital marketplace have evolved, our central goal has remained constant: to protect consumers' privacy and data in a way that fosters trust in the marketplace, and preserves and complements innovation.

FTC's Role in Protecting Privacy and Data Security

The Commission has undertaken substantial efforts to promote consumers' privacy and data security in the private sector through civil law enforcement, policy initiatives, and business guidance and consumer education.

A. Law Enforcement

The FTC has unparalleled experience in consumer privacy and data security enforcement. The Commission has used its core enforcement authority—Section 5 of the FTC Act—to take action against companies engaged in unfair or deceptive practices involving the privacy and security of consumers' information.[23] If a company makes materially misleading statements or omissions about a product or service, including its privacy or data security features, and such statements or omissions are likely to mislead reasonable consumers, such statements or omissions can be found to be deceptive and in violation of Section 5.[24] Further, if a company's privacy or data security practices cause or are likely to cause substantial injury to consumers that is neither reasonably avoidable by consumers nor outweighed by countervailing benefits to consumers or to competition, those practices can be found to be unfair and in violation of Section 5.[25] The FTC also enforces sector-specific statutes that protect certain health,[26] credit,[27] financial,[28] and children's information.[29]

The FTC's current privacy enforcement priorities include mobile, health, the Internet of Things, and data security. One example of FTC enforcement action in the mobile area is the *Snapchat* case. In that case, messaging app Snapchat promised that the photos and videos sent through its app would disappear at a time set by the sender.[30] The FTC alleged that, in fact, recipients could use easy workarounds—such as third-party apps—to keep the messages forever. Despite a researcher warning the company about this possibility, the complaint alleged, Snapchat continued to misrepresent that the sender could control how long a recipient can view a "snap."

The FTC has been equally vigilant in protecting data security. The Commission has brought nearly 60 cases alleging that companies failed to implement reasonable safeguards for the consumer data they maintain. For example, the FTC recently announced a settlement with computer hardware company ASUS for allegedly failing to take reasonable steps to secure the software on its routers. According to the complaint, the company's failures to timely address vulnerabilities or notify consumers about the availability of security updates resulted in critical security flaws in its routers that put the home networks of thousands of consumers at risk.[31] The complaint also alleged that the routers' insecure

---

23 15 U.S.C. § 45(a).

24 *See* FTC Policy Statement on Deception, *appended to Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 174 (1984), https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception.

25 *See* FTC Policy Statement on Unfairness, *appended to Int'l Harvester Co*., 104 F.T.C. 949, 1070 (1984), https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness; 15 U.S.C. §45(n).

26 16 C.F.R. Part 318.

27 15 U.S.C. §§ 1681–1681x.

28 16 C.F.R. Part 314, implementing 15 U.S.C. § 6801(b).

29 15 U.S.C. §§ 6501-6506; *see also* 16 C.F.R. Part 312.

30 Snapchat, Inc., No. C-4501 (F.T.C. Dec. 23, 2014), https://www.ftc.gov/enforcement/cases-proceedings/132-3078/snapchat-inc-matter.

31 ASUSTeK Computer Inc., No. C-4587 (F.T.C. July 18, 2016), https://www.ftc.gov/enforcement/cases-

"cloud" services led to the compromise of thousands of consumers' connected storage devices, exposing their sensitive personal data on the Internet. Under the order, ASUS must establish a comprehensive security program and notify consumers about software updates or other steps they can take to protect themselves from security flaws.

B. Policy Initiatives

The FTC has also pursued numerous policy initiatives to enhance consumer privacy and data security. The FTC has hosted workshops and issued reports recommending best practices designed to improve privacy and data security, increase transparency, and highlight the privacy and security implications of new technologies and business practices. Indeed, the FTC held its first workshop on Internet privacy more than twenty years ago, in June of 1996.[32]

In the privacy space, the FTC's policy work has built on recommendations from its 2012 Privacy Report, which set forth key privacy principles that should apply across diverse technologies and business models.[33] That report was the culmination of years of research and investigation, including three public workshops, a publicly released preliminary draft report, and multiple rounds of public comment. The report recommended that companies implement privacy protections, such as data minimization and security, at the outset of product development ("privacy by design"); simplify the ways they provide privacy choices to consumers; and improve transparency of their privacy practices.

The FTC has applied these principles to a broad array of emerging technologies and business practices. For example, the FTC issued a staff report on the Internet of Things ("IoT") last year. The report recommended best practices for companies, and also addressed how longstanding privacy principles can be adapted for the Internet of Things.[34] The report also addressed the continuing relevance of the principles of transparency and choice in the Internet of Things, even given the lack of traditional screens or interfaces to communicate with consumers. In addition, the report discussed the different tools that IoT companies are using to communicate privacy information to consumers—such as point-of-sale disclosures, set-up wizards, or even codes on the device. And the report discussed the importance of reasonable collection limits, de-identification of data, and strong security measures.

Similarly, the FTC has hosted workshops and issued reports on so-called big data practices. In 2014, it issued a report on the data broker industry, which described the depth and breadth of data brokers' information collection and use practices; recommended improved transparency for the industry; and suggested additional tools through which consumers could exercise choices about their data.[35] Earlier this year, the Commission issued a report entitled *Big Data: A Tool for Inclusion or Exclusion?*,[36] which highlighted a number of innovative uses of big data that provide benefits to underserved populations, while also examining possible risks that could result from biases or inaccuracies in big data.

The FTC also regularly holds events designed to enhance public understanding of key issues involving privacy and data security. For example, last fall the agency held a workshop on cross-device tracking

---

proceedings/142-3156/asustek-computer-inc-matter.

32 *See* Press Release, FTC Workshop on Consumer Privacy in Cyberspace to Be Held June 1996 (May 15, 1996), https://www.ftc.gov/news-events/press-releases/1996/05/ftc-workshop-consumer-privacy-cyberspace-be-held-june-1996.

33 FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

34 FED. TRADE COMM'N, CAREFUL CONNECTIONS: BUILDING SECURITY IN THE INTERNET OF THINGS (2015) [hereinafter "FTC IOT SECURITY REPORT"], https://www.ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf.

35 FTC DATA BROKER REPORT, *supra* note 2.

36 FTC BIG DATA REPORT, *supra* note 3.

to examine the privacy and security issues around the tracking of consumers' activities across their different devices for advertising and marketing purposes.[37] In January 2016, the Commission hosted the first-of-its-kind PrivacyCon, which provided a platform for academics to discuss cutting-edge research and trends in protecting consumer privacy and security.[38] The FTC has announced the second PrivacyCon, to be held in January 2017.[39] And most recently, the FTC announced that it will host a series of seminars this fall to examine three new and evolving technologies that are raising critical consumer protection issues: ransomware, drones, and smart TV.[40]

C. Business Guidance and Consumer Education

Finally, the FTC creates business guidance and consumer education to enhance the impact of its enforcement and policy development initiatives. The Commission has used a variety of tools—publications, online resources, workshops, and social media—to provide educational materials on a wide range of topics, including mobile apps, children's privacy, and data security. For example, the FTC has long sponsored OnGuard Online, which educates consumers about many online threats to consumer privacy and security, including spam, spyware, phishing, peer-to-peer file sharing, and social networking.[41]

Additionally, the Commission has also issued numerous education materials to help consumers protect themselves from identity theft and to deal with its consequences when it does occur. The FTC recently launched an improved version of IdentityTheft.gov[42] (robodeidentidad.gov in Spanish[43]), a free, one-stop resource people can use to report and recover from identity theft. Now, identity theft victims can use the site to create a personal recovery plan based on the type of identity theft they face, and get pre-filled letters and forms to send to credit bureaus, businesses, and debt collectors. During 2015, people viewed IdentityTheft.gov more than 1.3 million times and ordered more than 3.7 million related publications in English, Spanish, and four other languages.

Business education is also an important priority for the FTC. The Commission seeks to educate businesses by developing and distributing free guidance. Most recently, the Commission launched its Start with Security initiative, which includes a guide for businesses that summarizes the lessons learned from the FTC's nearly 60 data security cases,[44] as well as videos.[45] As part of this initiative, the FTC also has organized one-day conferences in Austin, San Francisco, Seattle, and Chicago, to bring business owners and developers together with industry experts to discuss practical tips and strategies for implementing effective data security.

---

37 FTC Workshop, Cross-Device Tracking (Nov. 16, 2015), https://www.ftc.gov/news-events/events-calendar/2015/11/cross-device-tracking.

38 FTC Conference, PrivacyCon, Jan. 14, 2016, https://www.ftc.gov/news-events/events-calendar/2016/01/privacycon. Research topics included the current state of online privacy; consumers' privacy expectations; transparency tools for revealing data discrimination; the economics of privacy and security; and security and usability.

39 *See* Fed. Trade Comm'n, *PrivacyCon: Call for Presentations* (last visited Aug. 17, 2016), https://www.ftc.gov/privacycon-call-for-presentations.

40 *See* Press Release, FTC to Host Fall Seminar Series on Emerging Consumer Technology Issues (Mar. 21, 2016), https://www.ftc.gov/news-events/press-releases/2016/03/ftc-host-fall-seminar-series-emerging-consumer-technology-issues.

41 *See* http://www.onguardonline.gov/. Since its launch in 2005, OnGuard Online and its Spanish-language counterpart Alerta en Línea have attracted more than 25 million visits.

42 See https://identitytheft.gov/.

43 *See* https://robodeidentidad.gov/.

44 FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESS (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

45 Fed. Trade Comm'n, *Start with Security: Free Resources for Any Business* (Feb. 19, 2016), https://www.ftc.gov/news-events/audio-video/business.

In addition, the FTC develops privacy guidance for specific industries. For example, the FTC has developed specific guidance for mobile app developers as they create, release, and monitor their apps.[46] The FTC also creates business educational materials on specific topics— such as a tool for health-related mobile app developers to understand what federal laws and regulations might apply to their apps,[47] as well as business guidance aimed at helping health app developers comply with the FTC Act.[48] Further, the FTC released guidance about ways to provide data security for Internet of Things devices, which includes tips such as designing products with authentication in mind and protecting the interfaces between devices and the Internet.[49]

Conclusion

Thank you for the opportunity to provide information regarding the challenges confronting consumers in the digital economy. The FTC is committed to protecting the privacy and security of consumers' data, and I am happy to answer any questions you may have regarding our work in this area.

46 Fed. Trade Comm'n, *Mobile App Developers: Start with Security* (Feb. 2013), https://www.ftc.gov/tips-advice/business-center/guidance/mobile-app-developers-start-security.

47 Fed. Trade Comm'n, Mobile Health Apps Interactive Tool (Apr. 2016), https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool.

48 Fed. Trade Comm'n, *Mobile Health App Developers: FTC Best Practices* (Apr. 2016), https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-app-developers-ftc-best-practices.

49 FTC IOT SECURITY REPORT, *supra* note 17.

Dr. Ron Ross

Chairman Donilon, Vice Chairman Palmisano, and distinguished members of the Commission, I want to thank you for allowing me to discuss some of the nation's challenges and opportunities in protecting the systems and networks that support the United States critical infrastructure as well as the important business functions that drive the national economy. My name is Ron Ross and I am a Fellow at the National Institute of Standards and Technology. I have over thirty years of computer and information security experience that includes a variety of positions in the United States military, Intelligence Community, Federal Civilian government, and the private sector. Currently, I lead the Federal Information Security Modernization Act Implementation Project, the Joint Task Force Cybersecurity Project, and the Systems Security Engineering Initiative.

The Current Landscape

The United States, along with every other industrialized nation, is experiencing an explosive growth in information technology and living in a world fueled by almost limitless technological innovation—including the development of computing and communications capabilities that are unparalleled in the history of mankind. The technology is powerful, affordable, and compelling, driving massive consumerization from large corporations to small businesses to individuals with their personal devices. The rapid and continuing technological advancements and the dramatic growth in consumer demand is occurring simultaneously with an emerging convergence of cyber and physical systems—sometimes characterized as the *Internet of Things*. This unprecedented technical innovation, mass consumption of new technologies by governments, businesses, and individuals, and ubiquitous deployments of those new capabilities worldwide, have resulted in a highly complex information technology infrastructure of systems and networks that are very difficult to understand and therefore, protect. As a nation, we are spending more on cybersecurity today than at any time in our history, while simultaneously continuing to witness an increasing number of successful cyberattacks and breaches by nation states, terrorists, and hacktivists that are stealing our intellectual property, national secrets, and private information. The situation is not getting demonstrably better over time and will have a debilitating long-term effect on both the economic and national security interests of the United States.

The Basic Problem Is Simple

Our fundamental cybersecurity problems today can be summed up in three words—*too much complexity*. Put another way, you cannot protect that which you do not understand. Adversaries view the U.S. critical infrastructure and our thriving businesses and industry as a target of opportunity, each adversary with potentially different capabilities and intentions. Increased complexity translates to increased *attack surface*. This provides a limitless opportunity for adversaries to exploit vulnerabilities resulting from inherent weaknesses in the software, firmware, and hardware components of the underlying systems and networks. We have characterized this situation as the *N+1 vulnerabilities problem*. The Defense Science Board pointed out in its 2013 study[50] that vulnerabilities can be categorized by type: those vulnerabilities that are known; those vulnerabilities that are unknown; and those vulnerabilities created by adversaries after they have taken control of your system and network.

Simply stated, there are vulnerabilities that you can find and fix, and there are those that you cannot detect and therefore, remain unmitigated. The increasing complexity and attack surface in critical U.S. systems and networks both in the public and private sector, virtually guarantees that the number of serious weaknesses and exploitable vulnerabilities that lie "below the water line" will continue to grow at an alarming rate. While we are making significant improvements in our intrusion detection and response capabilities, those types of tools and associated cybersecurity tactics fail to address the fundamental weaknesses in system architecture and design that can only be addressed with a holistic approach to protection that is based on sound systems security engineering techniques and security

[50] Defense Science Board Report, *Resilient Military Systems and the Advanced Cyber Threat*, January 2013.

design principles. The ultimate objective is to make our systems and networks more penetration-resistant; capable of limiting the damage from cyber- attacks by reducing the adversaries' time on target or lateral movement through the system; and sufficiently resilient to support critical missions and operations.

Why the Problem Is Difficult to Describe

We operate in two very different worlds—a world of *kinetic space* in which we can engage all of our senses, and a world of *cyberspace* which flies below the radar in a collection of bits, bytes, electrons, and integrated circuits made of silicon. Kinetic attacks such as the September 11th terrorist attacks on the World Trade Center and Pentagon can be observed and internalized and make a lasting impression on all of those individuals who witnessed the devastation. In contrast, cyberattacks operate in cyberspace which is analogous to having cancer in the early stages—the individual feels fine, cannot detect any life threatening condition, and as a result, goes about their business as usual as the cancer spreads to vital organs. While cyberattacks occur on a regular basis, result in serious or catastrophic consequences, and are widely reported in the news media, most organizations feel fortunate that the attacks are happening to others and not them. The cyberspace nature of the problem gives organizations a false sense of security since their systems appear to be operating normally while the adversary steals their intellectual property and highly sensitive information through an exfiltration attack. Strategically-placed malicious code can also hide in the complexity of the information technology infrastructure, giving adversaries the opportunity to bring down an organization's critical capability at a time of their choosing.

Engineering-Based Cybersecurity Solutions

Today, we have a high degree of confidence that the bridges we cross and the airplanes in which we fly are safe and structurally sound. We trust those entities because they are designed and built by applying the basic laws of physics, principles of mathematics, and concepts of engineering. If bridges were routinely collapsing and airplanes were crashing frequently, the first people called upon would be the scientists and engineers. They would do root cause failure analysis, find out what went wrong, and make the necessary recommendations to fix the problem. Cybersecurity efforts today are largely focused on what is commonly referred to as cyber hygiene-related activities—activities such as asset inventories, patching of systems, configuring firewalls and other commercial products, and scanning for vulnerabilities. While all important and necessary security activities, by definition, they operate "above the water line" and cannot affect the basic architecture and design of the system. Achieving perfection above the water line can still render our critical systems and networks highly vulnerable due to the inability to manage and reduce the inherent complexity of the information technology infrastructure.

The only way to address the ongoing "N+1 vulnerabilities problem" is to build more trustworthy secure components and systems by applying well-defined security design principles in a life cycle-based systems engineering process. Security, much like safety, reliability, and resilience, is an emergent property of a system that does not happen by accident. The disciplined and structured approach that characterizes engineering-based solutions is driven by mission and business objectives and stakeholder protection needs and security requirements. Those highly- assured and trustworthy solutions may not be appropriate in every situation, but they should be available to those entities that are critical to the economic and national security interests of the United States—including, for example, the electric grid, manufacturing facilities, financial institutions, transportation vehicles, water treatment plants, and weapons systems.

To support these objectives, NIST has embarked upon a multiyear systems security engineering initiative to define how security design principles can be applied within a standardized systems engineering process. We are bringing forward specific considerations to government, industry, and academia for a multidisciplinary approach in the engineering of trustworthy secure systems. These considerations are grounded in the fundamentals of computer science, mathematics, and

engineering—as well as over forty years of well-defined security design principles that represent the state of the practice.

A National Strategy Focused on Trustworthy Systems

During the Cold War, the United States invested in a nuclear triad of bombers, missiles, and submarines as a central element in its national strategy to defend the country against a first strike from the Soviet Union. It was the single most expensive investment ever made by the United States, although there was an extremely low probability that we would ever use that capability. The justification for such an expensive investment with low probability of use was directly related to the "asset valuation" that was a key part of the national *risk assessment*. The asset in question was the preservation of the United States of America, our freedom, and our way of life. The consequences of not making the investment in a defensive capability sufficiently strong to defend against or deter a Soviet first strike would have been catastrophic. The cybersecurity threats to our critical infrastructure, businesses, industrial base, and research and development activities today are every bit as important as those kinetic threats that the United States faced during the Cold War—and potentially more important. In fact, the complete dependence on advanced technology, and the interconnected nature of our critical systems and networks, increases the risk exponentially.

Bringing science and engineering-based solutions to cyberspace will require a significant investment of resources and the involvement of the *essential partnership* including government, industry, and the academic community. To meet a similar national challenge and threat in 1960, President Kennedy engaged the best and brightest from government, industry, and academia to do what most thought impossible—putting a man on the moon and returning him safely to Earth before the end of the decade. Eight short years later, we had accomplished the impossible. The clock is ticking and time is short. We have an opportunity to do what is necessary to protect our national treasure and defend the country in the brave new world of cyberspace.

In particular, the following recommendations are provided as part of a national strategy for building, deploying, and sustaining trustworthy secure systems for the United States:

- ***Near Term: Immediate Steps to Stop the Bleeding (1-2 years)***

  The federal government should lead by example by immediately:

  - Conducting an *asset valuation* of all federal data, information, and system assets to categorize and triage by consequence of loss (i.e., low-impact, moderate-impact, high-impact);[51]
  - Reducing the complexity (and attack surface) of deployed systems and networks by moving nonessential or less critical assets (e.g., data, applications, and services) to validated cloud service providers or other validated external service providers (i.e., eliminating the clutter that organizations must deal with in their protection strategies);
  - Prioritizing the remaining essential and critical assets; and
  - Applying system security engineering best practices to reengineer the organization's essential and critical systems and networks to: (i) increase penetration resistance to

[51] Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, provides a comprehensive approach to categorizing federal information and information systems based on a worst-case impact analysis and risk to organizational operations, assets, individuals, other organizations, and the Nation.

attacks; (ii) provide a capability to limit the damage to the organization if the attack is successful; and (iii) make the systems and networks survivable.[52]

- ***Mid-to-Long Term: Building a Trustworthy Secure Systems Infrastructure (3-10 years)***

  The federal government should lead a comprehensive public-private partnership to develop trustworthy secure systems for the United States. The partnership should include industry and the academic community and focus on a broad framework and foundation for trustworthy computing and a reasonable execution path for implementation. Activities include:

  - Developing trusted commercial operating systems and applications;
  - Developing trusted firmware and hardware platforms;
  - Building secure supply chain models and approaches;
  - Developing systems security engineering curricula in colleges and universities to ensure that the next generation of systems developers possess the requisite knowledge, skills, and abilities to build trustworthy secure systems; and
  - Creating a national-level trustworthy computing framework to establish the basic foundation for building, deploying, and sustaining trustworthy secure component products and systems.[53]

A national strategy for creating more trustworthy secure systems requires a holistic view of the problem space, the ability to bring to bear the concepts, principles, and best practices of science and engineering to solve the underlying cybersecurity problems, and the leadership and will to do the right thing—even when such actions may not be popular.

[52] NIST Special Publication 800-160, *Systems Security Engineering, Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, 2nd Public Draft, May 2016, provides a roadmap for conducting such reengineering activities.

[53] R. Bigman, *Building a Trusted Computing Foundation*, Input to the Commission on Enhancing National Cybersecurity, August 2016.

Gary Toretti

Chairman Donilon, Vice-Chairman Palmisano and distinguished members of the Commission, my name is Gary Toretti, Vice President and Chief Information Security Officer at Sabre and it is my pleasure to be here with you this morning to discuss my thoughts and recommendations on enhancing cybersecurity. We welcome the President's Executive Order creating the Commission on Enhancing National Cybersecurity because it covers a topic that is vital to the health and future of our nation.

Since the late 1950's when Sabre was created through a joint venture between IBM and American Airlines, we have been at the forefront of creating innovative technology. Sabre was the world's first computerized airline reservation system and has evolved into a technology ecosystem that touches almost every stage of travel.

Our Global Distribution System ("GDS") is one of the largest real-time computer systems in the world. Today we annually process over $120 billion of travel spend and board over 585 million passengers. We have nearly 10,000 employees in 65 countries and customers in over 160. Including our headquarters in Southlake, Texas, we have six facilities across four continents that produce cutting edge technology. Overall our GDS, Airline and Hospitality Solutions are used by approximately 420 airlines, 750,000 hotel properties, 425,000 travel agents, 39 rental car companies, 52 rail carriers, and 17 cruise operators. Sabre is facilitating travel every minute of every day around the world through our technology.

As individuals, businesses and governments continue to become more interconnected there is a greater need for all technology users, especially government and business, to streamline, collaborate and develop a multi-layered approach to security. The approach should encompass four central pillars: sensible regulation, self-protecting systems, multi-factor authentication and education. Taken together, a cybersecurity approach built on these four pillars will enhance and strengthen our nation's current and future systems from cyber-attacks.

The creation and use of technology is moving at the speed of light but the laws and regulations that govern its applicability are not. It is imperative to begin streamlining the current regulatory framework. The government has created a plethora of overlapping, duplicative, and varying standards in the form of mandatory regulatory requirements, voluntary standards, and audit requirements. Generating more regulations or standards, without understanding the impact of current laws and regulations, will increase the current compliance confusion that could exponentially and disproportionately increase compliance costs for all companies – large and small - or even discourage companies from implementing best in class security systems. Efforts should be undertaken by the Administration and Congress to streamline existing standards.

As industry moves to the Internet of Things, there is the need to address the patching of these devices because it is limited to non-existent. Over thirty years of career experience has taught me that an attack can come from something as seemingly innocuous as a consumer Digital Video Recorders ("DVR") connected to the Internet. Attackers use unprotected environments to launch Distributed Denial of Service ("DDOS") type of attacks using multiple compromised systems, which are infected with a virus, used to target a single system. Anything with an operating system, such as a refrigerator, connected car, or connected house, could be the next potential launch pad for the "bad guy." To counter this type of attack there should be a concerted effort to develop and deploy "self-protecting systems." The "Internet of Things" products should connect to an external system through a secured authenticated / encrypted tunnel to receive updates or patches as required to increase security strength. By automating key security functions like patch management, we can dramatically decrease the exposures and previously unknown vulnerabilities better known as zero day exploitations.

Along these same lines there should be an initiative by industry with support of the government to improve authentication mechanisms by adopting a set of best practices that embrace the continuing development of stronger multi-authentication mechanism controls. It is well documented that passwords alone continue to be an ineffective way of protecting information. Users often have

insufficiently complex passwords, repeat passwords across accounts, or have so many different passwords that they forget them and write them down creating open doorways for hackers to infiltrate computer systems. And while biometrics increase the level of security over passwords alone, once this personal unique identifier has been stolen it is all but impossible to alter a person's fingerprint, iris scan or facial qualifiers – meaning that once compromised it is incredibly challenging to protect information guarded by these identifiers.

And finally, there must be a stronger effort to share and adopt best practices by government and industry and bring this knowledge into schools. All companies should already have in place a cyber-education campaign that continuously reminds and educates their employees of the need to be vigilant about protecting information. This happens through awareness campaigns and instructional videos. At Sabre we successfully deployed internal phishing campaigns to help create awareness and sensitize employees to the many forms a cyber-attack can take and remind them to think before they click. This type of campaign should be replicated with our youngest digital users. Providing schools and educators with a set of best practices will give teachers the knowledge and tools to educate students of all ages about the importance of creating a safer and more secure digital ecosystem. This will not only heighten awareness around the protection of information but may have the effect of creating an early interest in innovation and technology.

The Commission has the opportunity to play an important role in highlighting the need for the adoption and development of a set of constructive guidelines that will provide a roadmap to our elected officials, government agencies, businesses and educational institutions about the need to safeguard sensitive information from cyber-attacks.

In light of the above, I have five specific recommendations. They include:

1. **Collaboration and Sharing**

   The U.S. Government should build upon its charge of sharing best practices and threat indicators among and between businesses and government. The government should continue to encourage the growth of Information Sharing and Analysis Centers, like the Aviation ISAC, which promotes the sharing of information among the aviation sector plus the refinement of the sharing portals of the Department of Homeland Security. These are positive actions that should continue and broaden as technological innovations proliferate.

2. **Fostering & Encouraging the Creation of a Single Standard Framework**

   The U.S. Government should undertake an initiative to study the current overlapping and duplicative regulatory framework and propose a blueprint for streamlining it where appropriate.

3. **Develop Self-Protecting Systems**

   A significant number of large data security incidents today continue to occur because hackers exploit long-identified vulnerabilities on systems. The government and industry should collaborate to develop and adopt self-protecting systems, which can minimize the number of easy targets for hackers.

4. **Continuous Security Knowledge**

   Businesses should continually challenge their employees to understand and adopt methods to safeguard sensitive information. This includes the distribution of monthly newsletters, posters, training courseware, security awareness tests and, for example, an internal phishing exercise so people understand and learn what to look for before they blindly click on an attachment or email.

5. **"Cyber Health" Education**

   There should be a recognition and encouragement to create "Cyber Health" classes in classrooms, which should start as early as pre-K. It is not enough to rely on creating interactive and

informative websites; children should be taught early about a set of best practices and the consequences of failing to act responsibly.

Again, I want to thank the Commission for given me this opportunity to discuss this important topic and look forward to answering any questions.

Sarah Zatko

There are many, varied challenges confronting consumers in the digital economy. While the erosion of ownership and the decreasing expectation of privacy are serious concerns, this statement will focus solely on challenges that our charitable organization, the Cyber Independent Testing Laboratory (CITL) is striving to address.

Software today is very complex, and that complexity means an increase in bugs and vulnerabilities. This is part of the cost of ownership for this software, for corporations and individuals alike. This complexity and accompanying risk is a problem in not just traditional software, but also the broader "internet of things" (IOT), which includes everything from insulin pumps[54] to automobiles[55]. It is important, as a consumer, to be able to understand the comparative levels of risk and vulnerability that a piece of software or a computer system embodies, and use that as part of their decision making process.

Consumers who want to seek out a secure product today have no reliable information they can use to assess the security of products. Some vendors describe the security of their product by advertising or marketing claims such as 'secured by technology X'. These approaches generally seek to capitalize on brand name recognition. For example, a website might claim to be secure because it uses SSL. Unfortunately this tells the consumer nothing about whether the implementation of SSL is strong or weak, protected or vulnerable. These labels do not convey meaningful information, vary in how they relate to actual software security, and are not standardized.

1) Consumers need quantifiable, comparable, easily understood data about the risk profile of the software they use and depend upon. Think of this as the "nutritional facts" label, but for software. Some safety technologies, such as address space layout randomization (ASLR), non-executable stack & heap, stack guards, are proven and well tested, and have been known to make software safer for over a decade. These technologies are easy to enable in commercial software, but are not universally used in commercial code. Omitting such technologies from a commercial software product today is like having a modern car that is sold without airbags or seatbelts. Such an omission should be disclosed to consumers, ideally through some universally applied labelling or via easy to use online resources providing consumer advocacy information.

2) To follow the nutritional label analogy further, legislation is not an appropriate tool for making software safer. People are able to make, sell, and buy junk food; it just has to be labeled in such a way that it is easy to determine that it falls under that category. Those who have special dietary needs can look at the sodium or fat or sugar content and know that a particular item is outside their personal restrictions. Legislating a "one size fits all" solution for nutrition would be impossible, as different people have different dietary needs, and scientific understanding of what is and isn't healthy changes over time. If nutrition is a swiftly moving target, technology is even more so, and legislation is not agile enough to keep up with new technological advances and standards.

3) It is also important that legislation not stand in the way of security research or consumer advocacy efforts. Currently disassembly is just barely legal, while the legal status of reverse engineering is ambiguous. Disassembly does not reveal proprietary IP, but does provide the means to ascertain information about the safety and security properties of software that the consumer should be aware of. Independent review of commercial products is imperative, and should not be put at risk by legislation that disallows standard research practices.

4) While specific software development processes should not be mandated, we should have mandatory disclosure of the contents and security properties of software by a trusted, independent

54 http://www.bloomberg.com/features/2015-hospital-
55 http://www.bbc.com/news/technology-33650491

party. This information should in turn be available to the public. It is important that the testing organization is one whose impartiality and reliability can be trusted.

The software market has evolved a great deal in the past few years. Consumers now have choices about what product they use to fill any particular software need, but they can't make informed security choices without actionable data. The actions recommended above would allow software consumers (be they individuals, corporations, or governments) to make purchasing decisions to suit their own security needs.