Commission on Enhancing National Cybersecurity

Established by Executive Order 13718, Commission on Enhancing National Cybersecurity

Meeting Minutes

August 23, 2016

University of Minnesota
TCF Bank Stadium
Dairy Queen Room
420 23rd Avenue SE, Minneapolis, MN 55455

The Commission on Enhancing National Cybersecurity was convened for its fourth public meeting at 9:12 a.m., Central Time on August 23, 2016 at the University of Minnesota, Minneapolis, MN. The meeting in its entirety was open to the public. For a list of attendees, please refer to Annex A.

Meeting Opening and Remarks

Tom Donilon, Chairman, Commission on Enhancing National Cybersecurity

The hearings today will inform the Report on Enhancing National Cybersecurity. On behalf of the Commission, we would like to thank the University of Minnesota for hosting the meeting.

Welcome and Overview

Dr. Massoud Amin, Director, Chair, Technological Leadership Institute; Distinguished University Professor, University of Minnesota

Dr. Amin welcomed the Commission Chairman and the Commissioners. The University is honored to host this timely and critical event. The University of Minnesota has a history of assisting with enhancing technological advances in the United States and acknowledged members of the University's Cybersecurity program and alumni in attendance.

The University's flagship cybersecurity program is informed by more than 1,300 full-time working professionals in the field of technology. Cyber risks are real and significant, affecting national security. He expressed gratitude to the Commission for addressing this area. Telecommunications and information processing systems are susceptible to exploitation. Technology affecting these products is used extensively. To adequately address these concerns requires effort both today and into the future.

Dr. Amin provided an addendum detailing his recommendations and concerns, one of which relates to proactive blocking, the ability of the government and industry to take proactive measures to the end that the infrastructure is smarter and more secure.

Panel 1: Consumers and the Digital Economy

Susan Grant, Director, Consumer Protection and Privacy, Consumer Federation of America
Mike Johnson, Director of Graduate Studies in Security Technologies, Technological Leadership Institute, University of Minnesota

Kevin Moriarty, Senior Attorney, Division of Privacy and Identity Protection, Bureau of Consumer Protection, Federal Trade Commission (FTC)
Sarah Zatko, Chief Scientist, Cyber Independent Testing Laboratory (CITL)

Susan Grant, Director, Consumer Protection and Privacy, Consumer Federation of America

Technology helps consumers to save time and money. At the same time, it also makes us vulnerable to many different issues. In many areas, we have no choice in the matter. It won't be long, before our cars will be able to communicate with each other. Technology is omnipresent. On campus, most schools require students to use computers in the classroom. Our health records are now electronic. Though privacy in the United States is considered a personal right, legislation guaranteeing privacy does not extend to all aspects of life. No federal law yet exists requiring companies to disclose their privacy practices.

Another area of vulnerability is in facial recognition. Our facial images are no longer private, but no legislation has yet been enacted to address this. In most respects, our telecommunications are protected, but the battle continues to address the ability of the government and ISP service providers to access that information. No oversight yet exists to ascertain the accuracy, origin, or use of accessible information, though discrimination may be employed when accessing big data. Transparency continues to be a challenge regarding disclosure of information and practices provided by companies. To a great extent, responsibility rests with the consumer, who must choose to opt out.

Privacy should not only be an option only for those who can afford it, but should be available to everyone. Consumers recognize that control remains with companies. But reservation on the part of the consumer should not be construed as enthusiasm. In light of the almost daily occurrence of a data breach, consumer concern is well-founded. At present, all the consumer can do is to hope that the data holder is sensitive to the need for privacy. The consequences (to the consumer) for thinking otherwise can be most severe. I offer the following recommendations for the commission to consider:

Privacy should be protected. We should be asked for consent and should not be forced to pay for it.

- Data usage should be protected.
- Industry should be required to protect privacy and security. More oversight, less self-legislation.
- The administration should advocate for the FCC and FTC to promote rules for businesses and industries.
- Big data should be reposited in a central location.
- The Government should support the development and use of encryption.
- Measures should be mandated to protect data from abuse.
- Two-factor authentication should be encouraged instead of relying on social security numbers for validation.
- More should be done to promote consumer education. It should begin in schools with additional information available to adults.

Mike Johnson, Director of Graduate Studies in Security Technologies, Technological Leadership Institute, University of Minnesota

Consumers need to be confident in the systems they use. That level of confidence decides whether or not a consumer feels comfortable and secure online, and is a useful metric to gauge success. However, consumer confidence is not the only metric. The fact that transparency remains elusive, means that consumer confidence remains negatively impacted. A clear strategy to instill confidence has yet to be formulated. This problem is exacerbated by the fact that regulators remain understaffed and under equipped.

Though PCI is the focus of activity, it doesn't get us there. We need to come up with a hybrid which mandates real enforcement and real penalties. Bi-directional authentication, buttressed by consumer confidence in the provider, will go a long way to improve consumer online security.

Kevin Moriarty, Senior Attorney, Division of Privacy and Identity Protection, Bureau of Consumer Protection, Federal Trade Commission (FTC)

The views expressed in this statement reflect my own opinions and does not necessarily reflect the collective vision of the FTC. There are three areas of focus:

- Data usage and maintenance.
- Technological development to process data in real time. The volume and duration of data storage increases its vulnerability to attach.
- Consumer awareness is deficient with regarding data usage and its governance.

The FTC enforces sector-specific statutes and is vigilant in protecting its data. Improvement is still needed to achieve transparency with regard to privacy practices. To achieve that objective, the FTC has hosted workshops and posted reports on big data practices. The organization has also sponsored a privacy conference for academics to provide information on privacy and data security.

The FTC also provides free guidance on online practices, spam, and file sharing.

Sarah Zatko, Chief Scientist, Cyber Independent Testing Laboratory (CITL)

Consumers want to make informed decisions, but are hampered by the lack of available information. The security industry has tried for years to generate consumer interest in security issues. But when consumers do acknowledge the need to act, little or no specific information is offered for them to be able to move ahead.

Though the consumer is provided with labels and other indicators, their largely technical nature is likely to be misunderstood by the less technical consumer. Additionally, labels might be duplicative and/or unclear. Consumers need reliable, quantifiable data. Existing labels, such as those issued by the FDA or by manufacturers of consumer products, should serve as models. As it is, the meaning behind existing security labeling is often confusing. Labels based on overly-broad certifications do not necessarily indicate that a product, once it is certified, will be subject to re-certification to keep pace with technological development and the evolving nature of cyber defense.

We recommend the practice of mandatory disclosure. Since consumers now have choices, we

should ensure that we provide them with information to enable them to make the right choices.

Panel One Discussion

Commissioners of the Commission on Enhancing National Cybersecurity

Ms. Wilderotter: Do you think the FTC will work more closely with DHS to get the word out and get consumer awareness out to the consumer?

Mr. Moriarty: The FTC is, first and foremost, a law enforcement agency. My division is more focused on law enforcement, but we do have online resources that are useful for consumers. We also have information and programs for business and on how to get the information out there. I'm not sure of the state of BDCE on consumer education, but I can get back to you.

Ms. Wilderotter: When the consumer does not know where to go to get information, they will mostly likely go to [the FTC] to get this information.

Mr. Moriarty: I don't want to suggest that we don't have the resources, but I'm not sure if we know that they don't know how to get the resources.

Mr. Donilon: Why hasn't there been a successful public campaign for consumer education?

Ms. Grant: It has to be an integrated process in people's everyday lives. They have a lot to worry about and this is only one thing that they have to worry about. They need places for people to turn to. Even with the FTC, the information is online and there isn't really anyone to call. If you want to get serious about it, you need to have something like a paid marketing plan, but you can't just do it once. We have to tell people what to look for.

Ms. Zatko: Industry needs to have incentives to do better jobs so that people know what they are doing when they are faced with decisions.

Mr. Sullivan: If there were labels, how do people know what labels will look like? How would we get companies to be more transparent with their privacy and are we successful?

Ms. Zatko: Are companies doing risky programming technologies and are they doing proper development? Currently, how are the consumer reports being used?

Mr. Sullivan: It is hard to image a non-engineer consumer digesting the information that type of information.

Ms. Zatko: If it's a score, it wouldn't be that difficult. Put it in a format that is understood by the normal consumer.

Mr. Sullivan: You would need someone to translate the ratings.

Mr. Donilon: It would help if the companies themselves provided some information.

Mr. Banga: How do we establish a percentage of average daily intake? It becomes a bit difficult as different companies have different needs.

Ms. Zatko: When we talk about consumers, we tend to mean people, but businesses (large and small) and government are also consumers. The purchasing officer of any organization of any size wants to make informed decisions. The goal is to output different reports based on different

audiences instead of a "one size fits all" format.

Mr. Banga: How do we get to that conceptualized data?

Mr. Lin: I'm in sympathy with the intent of what CITL is doing. How do you deal with more general recommendations? If there are particular plans on how to avoid some of the pitfalls, how will you do this fast enough to keep up with advancements in technology?

Ms. Zatko: We are taking a page from other industries. You don't have to fuzz every piece of software if you know how some other software works. The technology is so advanced, you can accomplish things in this realm. We want this to be an open standard, but also to keep the lights on to make it pay for itself.

Mr. Lin: Can companies seeking to protect intellectual property be a hindrance to testing groups like yourself?

Ms. Zatko: The companies should not want to keep industry standards private. They should not use negligent practices in code development, otherwise, there is no incentive into doing this at all. Safety should be prioritized just as companies try to prioritize their bottom line.

Ms. Grant: When I have a phone requiring an upgrade, I have to hit "I Agree." I could change phones and/or operating systems, but it's a hassle. I get impatient with the argument that people really want this targeted marketing. If that was the case, you could offer the option to agree or not agree. People should be able to use these tools, but also have a real choice.

Ms. Zatko: Quantifying the data being used could be designed differently to balance advertising and the privacy needs.

Mr. Lee: Is it really like nutrition labels or more like standards for automobiles? Are we in a situation in trying to provide transparency to the consumer and also mandating a level of security?

Ms. Zatko: I think there is a place for that. For instance, seatbelt laws are important, but it should be considered standard practice in technology. It is important that consumers to know who has what information. Standards need to be in place.

Mr. Moriarty: We don't have practices in violation of "Sector 5." We look holistically at the entire process.

Ms. Grant: I don't think the government should set technical standards, but should determine the basic steps needed for security. Make sure the security measures are up to date.

Mr. Johnson: Standards are necessary and needed if you are going to hold companies accountable for anything shy of a breach.

Mr. Lee: All software rots and browsers on any one day, might meet certain standards or expectations, but, over time, exploits are found and are fundamental in the architecture of the browser. How do you see labeling evolving in that type of situation?

Ms. Zatko: Did this company care enough to do the right thing in this situation. We can't say that this software is secure and cannot be hacked, but we can say that this software has been changed for the better and that is something for which the company should get kudos.

Mr. Lee: If I were to take some of your software and engage in reverse engineering and try to sell or use the information to consumers, would this make any difference?

Ms. Zatko: There shouldn't be any moral use tied to software because there is basically dual-use for any software being developed. If the software is being used offensively, it doesn't mean it shouldn't be used defensively.

Ms. Grant: In the current environment, it might be difficult to pass, but that is why discrete rule-making and narrow legislation is being promoted rather than a comprehensive package. The President's proposed privacy bill of rights was from a consumer perspective and didn't garner any "help" from consumer groups. We are going to continue to support something comprehensive and big picture, but will continue to support a narrower approach which could have a larger effect.

Ms. Murren: When you look at your model, what will it take to bring it to market for use world-wide?

Ms. Zatko: We will need more funding to hire more than two programmers and also need to operate in several environments so that we can best evaluate the software.

Mr. Chabinsky: In my view, the Commission can provide information on how the government can change some things. We have things like the Congressional Budget Office, which is supposed to ascertain the cost of legislation. Could you envision whether it should be Congress, the Executive Office, or private parties to assess the security and privacy ramifications of that bill?

Ms. Grant: I wouldn't want it to become another ORIRA, and go to another black hole due to political protection. It would need to be an independent agency with the expertise, but democratic considerations are at stake, not just cost. Most technologically advanced societies have data protection agencies. Business and government need an independent agency.

Mr. Chabinsky: Is it time to take some security choices away from the consumer?

Ms. Zatko: Security technology is a moving target, but I think that's where insurance comes in. If you have an unsafe vehicle, it will affect your insurance premiums. Cyber insurance is currently looking for a way to collect better actuary data. Insurance is a great way to change market motivation. I don't think what you are saying is impossible, but you have to be sure this is something you want to avoid obsolescence.

Mr. Moriarty: We recently worked with the HHS Office of Civil Rights to develop an easy-to-use device for mobile health devices. There is HIPPA and the FTC Act, both of which contain health breach data information. There is more that can be done.

Ms. Anton: Are there states other than California which have things in place for this to cover other applications within HIPPA?

Mr. Moriarty: I know HIPPA was expanded in the Fall of 2013, but I would say "no," because I am not sure how the California law is affected by HIPPA updates.

Mr. Moriarty: In general, we have sector-specific agencies, such as HHS, providing information.

Ms. Anton: Given that the internet of things touches so many systems, do you think broader statues are needed since the internet of things touched so many different sectors?

Ms. Zatko: Data collection and privacy aren't something that we are looking at because so many other organizations are looking into this.

Mr. Moriarty: The Commission's position should be the broader guidance regarding unneeded data and data which should not be collected.

Mr. Palmisano (via KT?): Is there a technology where consumers can both assert and hide identity simultaneously?

Mr. Johnson: There are ways to do this within browsers to cloak identity but then provide identity to make this happen. This should be an area of further research.

Panel 2: Innovation (Internet of Things, Healthcare, and Other Areas)

Robert Booker, Senior VP, Chief ISO, UnitedHealth Group, Optum, Inc.

Brian McCarson, CTO, Intel IoT Strategy; Sr. Principal Engineer, Chief Architect, Intel IoT Platform

Gary Toretti, Chief ISO, Sabre Corporation

Since the late 1950s, when Sabre was created through a joint venture with IBM and American Airlines, we have been in the forefront of integrative solutions. Four central pillars are being addressed today: sensible regulations, self-protecting systems, multi-factor authentication, and education. Taken together, our systems will be better equipped to handle cyber-attacks. Though the pace of technology continues to move at the speed of light, applicable legislation does not. Over time, the government has introduced overlapping, duplicative, and variant standards, and audit requirements. As a consequence, the proliferation of new regulations will only complicate the problem as well as add to the cost of doing business. Efforts should be undertaken by the Administration and Congress to streamline existing standards. Patching and updating self-protecting systems are crucial, because today progress is virtually non-existent. Over thirty years of experience, it is true that cyber-attacks can come in the form of devices as innocuous as digital recorders attached to the internet. How often are our personal devices patched? Anything with an operating system, like a car, a house, or a refrigerator, can be the channel for the next cyber-attack.

To address this threat, we recommend increased deployment of self-protecting systems. Products should be connected to an external system through a secured, authenticated, encrypted tunnel, to seamlessly receive as-needed updates and patches. There should be an initiative by the industry, supported by the government, to improve authentication mechanisms by adopting a set of best practices encompassing the continuing development of stronger self-protecting systems. Passwords continue to be an ineffective way to protect data. If biometric data is stolen, it is extremely difficult to protect data guarded by this criteria.

All companies should already have in place a cyber education or awareness campaign, supplemented by instructional videos. At Sabre, we have successfully deployed an internal phishing campaign to sensitize employees to potential breaches and to expose them to the various forms which an attack can take. In closing, we offer five recommendations:

- Collaborate and share information
- Foster creation of a single standard framework

- Develop self-protecting systems and keep them up to date
- Continuous security knowledge by updating tools to foster employee and customer awareness regarding the protection of sensitive information
- Cyber health education

Brian McCarson, CTO, Intel IoT Strategy; Sr. Principal Engineer, Chief Architect, Intel IoT Platform

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. 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."

- 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.
- Establish a Chain of Trust.
- Foster Interoperability. Interoperability has several dimensions.
- Accelerate leadership in IoT Security.

We are becoming a smart and connected world.

Robert Booker, Senior VP, Chief ISO, UnitedHealth Group, Optum, Inc.

UnitedHealth Group is built on two business platforms: United Healthcare, 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.

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.

The internet of things and its 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.

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.

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.

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. Their view 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.

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. Innovation to support health outcomes is critical. Cybersecurity risks require ongoing vigilance. But as technology evolves, a common foundation supporting engagement between companies and ongoing cybersecurity collaboration is critical to achieve success.

Panel Two Discussion

Commissioners of the Commission on Enhancing National Cybersecurity

Ms. Wilderotter *[to Mr. Booker]*: Do you require innovations test a certain standard of security?

Mr. Booker: Yes. We look at how we monitor the systems and potential of device providing a lack of integrity. Costs, we look at improving outcomes. Inherit complexity with how healthcare operates. Innovation will evolve. In time standards will make this easier.

Ms. Wilderotter: Do you require a certain standard of built-in device security today?

Mr. Booker: We do look into these capabilities and start with security very early. We look at how we monitor the system and how these devices work. We think of the potential the device has, with respect to lack of integrity. There are devices emerging in the market which may not qualify as candidates, due to lack of security integrity.

Ms. Wilderotter: As we think about policy, you talk about foundational security from an IoT perspective. How should we think about legacy products which didn't start with IoT?

Mr. McCarson: We should invest in some of the products and capabilities currently being used. In my view, a sound approach would be for the U.S. to take into account currently binding requirements as well as requirements which can be put in place. If you look at work being done in the automotive industry, if it's something involving in the protection of human lives, there is a standard which must be met for that component.

Mr. Toretti: I agree with Mr. McCarson's approach. You have to assess the legacy infrastructure and, over time, come up with standards over a period of time comprised of various phases.

Mr. Sullivan: In the PC and mobile world there is the OS platform. You can put apps on top of it, but there is still that platform. Would that platform break down in IoT?

Mr. McCarson: My own view is there are distinct similarities between a toaster talking to an oven, and a fit bit talking to a phone. Those similarities are hardware-based. The toaster is my toaster and the oven is my oven. Create a hardware-based root of trust.

Mr. Sullivan: Is the market taking us there or should the Commission make this a recommendation?

Mr. McCarson: I don't think the market will take us there, unless there is a demand to make it go there. In my view (not shared by all of my colleagues), a case will not be made to move in that direction until there is a catastrophic event. I think this Commission has the opportunity to protect the consumer from threats in the marketplace to which the consumer is largely unaware.

Mr. Gallagher: What I heard from all of you is a very complex built ecosystem from the ground up, even though we currently deal with a rapidly changing system. Are we always going to be behind the deployment curve? What are some specific things you believe would allow wide-adoption of something like EPID, at market scale? What could the government do to support this adoption?

Mr. McCarson: Let's take a practical example. This is a space where government has regulations on what can be approved as a monitoring device. These devices don't necessarily call for a framework at the hardware level. The same framework can be used to create requirements for a health-monitoring device which encrypts data to avoid monitoring. I think the Commission could help because some of the issues are privacy-related. The lack of a clear standard and vision slows down the industry. I believe the technology exists today which does not rely on just one company. Implementation will reduce the cost in patient care and stays in the emergency room.

Mr. Gallagher: You seem to be proposing sector-based regulations. As a supply chain matter, does this require security in the chips being created?

Mr. McCarson: In terms manufacturing, there exist about 15 entities with a bit more to allow for design manufacturing. Devices can be built to enable consumers to assign the unique ID. The manufacturer need not be the one to identify the device. The purchaser can provide that ID.

Mr. Toretti: The technology exists today. People must be held accountable to implement that information. We need to set standards from the perspective of development which bakes-in

security from the beginning.

Mr. Donilon: I think the question is, what is the accountability mechanism which should be used?

Mr. Booker: I think we are still at the incubation stage. It takes a time for upgrade medical devices currently running on deprecated technology. The government can assist in primary research in this area. This could be the foundation from which to validate the technology.

Mr. Banga: Let's say it gets implemented in various ways, some better than others. Most of the effort and behavior goes into catching it after it has been used. How do we catch it at the compromise?

Mr. McCarson: Let's say the toaster is talking with the oven, it may be perceived as normal talking between devices. You would probably find specific packet sizes passed between the devices. If you have robust threat detection software, you can check for changes in the system.

Mr. Banga: Should the Commission be in a place to allow for that type of detection or should that be left to market practices?

Mr. McCarson: The Commission has the opportunity to do that. I would recommend starting with certain industries. There should be very specific guidelines for things like remote patient monitoring, the energy grid, and others. We have the opportunity today to create the framework for this.

Mr. McCarson: The U.S. can differentiate in the next level of what you just described. We can provide next level incentives.

Mr. Lin: The primary issue for security in the healthcare sector, is data breaches and data getting out that shouldn't get out. We are now starting to see ransomware. I was wondering about a darker future in which medical information is not only viewed, but altered. How would it change the focus if you started to worry about unauthorized altering of medical data within devices? One of the things we grappled with would be, what are the incentives for getting people to actually do what they should be doing? We don't see the market pushing in that direction.

Mr. McCarson: I was one of the first to deal with identify fraud. People today are more aware of privacy concerns.

Ms. Murren: My question relates to electronic medical records. If we go back to 2004, there was a huge push by the government and the private sector to widely and quickly adopt electronic medical records for consumers with the idea that it would make healthcare better, safer, and cheaper. Now, a decade later we've never been less healthy, healthcare costs have escalated annually, and people's personal health info has been exposed. Is there any learning we can take from that and apply it to the IOT, and what can be done differently?

Mr. McCarson: Progress has been made in terms of health data interchange. The promise of how much information and how much data interchange will create the outcomes we're seeking is probably the active question we need to continue to look at as an industry. I think we still need to continuously examine the integrity of data and be aware of whether it's complete or not. As we move into a population of providers that are more digitally savvy, those things will also begin to take root. We'll start to see providers interacting more with electronic the health records system

directly. Health records are complex, and we are always looking at new pathways to deliver care which can amplify concerns. As the population becomes more digitally savvy, some current obstacles will continue to break down. The Commission has great opportunity to help utilize the interrelationship between public and private sector in this space vs. applying regulations.

Mr. Torretti: The industry has moved at the speed of light, but identity management is moving at a snail pace. There is a multitude of user ids, and accounts. Many sites don't require multi-factor authentication, which makes it much more possible for accounts to be stolen through key stroke loggers or other methods. I would ask the Commission how do we go back to these devices everyone has and create multi-factor identification.

Panel 3: Assured Products and Trustworthy Technologies

Edna Conway, CSO, Global Value Chain, Cisco Systems, Inc.
Joshua Corman, Director, Cyber Statecraft Initiative; Former CTO, Sonatype; Co-Founder, I am The Cavalry and Rugged Software
Ken Modeste, Global Cybersecurity Technical and Strategy Lead, Underwriters Laboratories, Inc. (UL)
Dr. Ron Ross, Computer Scientist, National Institute of Standards and Technology (NIST)

Ken Modeste, Global Cybersecurity Technical and Strategy Lead, Underwriters Laboratories Inc. (UL)

Each day UL works collaboratively with manufacturers, retailers, trade associations, public interest groups, and international regulatory authorities to further advance safety, performance and security through applied science. Through our research, testing, and certification we help ensure that the products people use every day, whether they be in the home, office, or connected to the internet meet safety, interoperability, and performance standards.
From our beginning 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. More recently, we have expanded our capability in key areas and broadening the definition of safety, and moving from the physical to the virtualized world. Throughout its history, UL has understood the relationship between security and safety, and it is certainly true in today's connected world.

Powered by software embedded in devices, the virtual world poses a new set of risks. We have built a knowledge base of everything from wearable devices to chip cards. That gives us a special insight into trends impacting connected technologies today. In wearable devices, we are hard at work at ways to secure private information, some of it sensitive personal health data shared over wireless networks. There are many different interoperability protocols in use, and we test for them for interoperability, so they each exchange information with another at the same time making sure they don't interfere with other systems.

Last October was the U.S. deadline for shifting responsibility from banks to merchants for any fraud committed during instore purchases. Merchants raced to adopt chip card technology prior to the deadline. Having already implemented chip cards for Europe and other parts of the world, UL had the core capability to meet the challenge facing U.S. retailers. We educated them about the transition, how to upgrade their point-of-sale terminals, increase overall public awareness, and contributed to security for both retailers and consumers alike.

Of the total universe of devices, it's paramount we understand the rest of people and develop solutions to meet this challenge. Recognizing this need in April of this year, UL launched a voluntary cyber security assurance program, called UL CAP that addresses the many risks associated with connective technologies.

The CAP Program was established with input from academia, government, and industry groups. The mission is simple, but important. To help vendors identify security risks in products and systems, and to suggest foundational elements required for good cyber hygiene. We built CAP around UL standards, providing innovations with a testable set of cybersecurity criteria for network connectable products and systems.

Working with our clients, CAP accomplishes four things: it assesses software weaknesses and vulnerabilities; it minimizes exploitation; it reviews and assesses security controls; and increases overall public security awareness. Software flaws and weaknesses attributable to known security incidents stand at the very heart of CAP, and is our primary driver in developing the technical requirements for our program. Based on this experience, we believe that government, working in partnership with industry, should take two key steps.

Step one, develop a scientific methodology for assessing software products, and provide metrics for identifying, measuring, and addressing vulnerabilities and weaknesses. In addition, we believe that when independent, third party organizations conduct testing and certifications, it increases trust in the market place.

Step two, use existing methodology to assess a vendor's ability to execute security objectives across the entire supply chain. This begins with manufacturers using established practices to develop, build, and support products and systems for sale and give system operators maintenance. This begins with manufacturers using established practices to develop build and support products and systems for sale and giving system operators maintenance and asset owners the ability to configure and asset owners the ability to install configure and support systems.

I'm proud to report the CAP program is already gaining supporters. In June, UL and the US Department of Veteran Affairs announced a cooperative research and development agreement program for medical devices, cybersecurity standards, and certification. The program will support improvement of veteran patient safety and security, through the use and verification of the UL CAP program.

We believe this work will contribute to broader awareness of medical device vulnerabilities and threats, as well as refine existing and emerging standards and practices. As we all know, the federal government shares many of the same goals as the private sector. We think it should leverage the private sector's expertise, knowledge, and resources when considering developing regulations and administering programs. We encourage the government to utilize public-partnerships in developing public policy by adopting consensus based standards and accreditation schemes, and globally recognized practices to meet its compliance interests.

By working with the private sector government agencies can access this additional data, promote transparency, leverage private sector resources, and contribute to economic and job growth. We

believe that cybersecurity necessitates a strong private public partnership. CAP is well on its way to providing a framework that supports the commission's objective to strengthen cyber security and to better ensure public safety and enhance innovation. I appreciate this opportunity speak about this today, I look forward to answering any of your questions.

Dr. Ron Ross, Computer Scientist, National Institute of Standards and Technology (NIST)

I've been in this business a long time, going back to 1976 to the Anderson report for the Air Force that was our first real dive into cybersecurity. It's now 40 years later and the question that I'd like to pose is, how did we get to where we are today, where we're having a commission where this is become just the hottest topic. What's the basic problem that we're facing? Why have we not been able to fix the problem up to this point, and what are some ways we can think about the problems differently moving forward? That's the nexus of the big ideas.

About 2 years ago this problem became very clear to me, because we are the greatest innovators in the world we have the greatest technology. As all the panelists said today, the technology is very powerful, very affordable. We buy a lot of it. In some sense what we're witnessing here, in this cybersecurity problem is the American love affair with technology. It became very clear to me, as a security professional when I was at a movie about a year-and-a-half ago and with my wife and discovered there is an app that will tell the optimal time to go to the restroom in the movie. It's humorous, but we know as a security people it's dangerous to download the application.

It was mentioned this morning in the previous panel when downloading a new app and it before installing it the user must say yes to these 40 things that the app needs to have access to.

The real message I want to convey to the commission is a strategic issue. We talked a lot about tactics. We're doing a lot of great things in security, but they're all tactical. Tactics win battles. Strategies win wars. We have to have a larger holistic view of this problem because one of the things that comes with all this advanced technology, and our propensity to buy it and use it, is we just are not looking in the right places for the answers to some of the really dangerous things that we're facing. I've tried to convey this, and this is going to get worse with the convergence of cyber and physical systems, and all the things that come with the internet of things. There are 6 billion devices today. We're adding another couple hundred million every month.

The fundamental issue I'd like to put before you is the issue of complexity. Commissioner Chabinsky, in his last question, started to address this. That is our number one threat. It's not on any NSA top 10 list, or the CIA's top ten list, but when you look at this from an engineering and a scientific perspective, we have to be able to solve that complexity problem, if we are ever going to be able to build systems that are as trustworthy as they need to be. I'm not ever going to talk about fully assured, highly trusted systems because you can't get high assurance and trustworthiness everywhere.

The question I think we all need to look at is, don't we need to be able to have that level of trustworthiness and assurance where we need to have it. That's kind of a fundamental underpinning of my remarks today. I use the analogy of above the waterline and below the waterline problems, because most of our cyber security work today, whether you talk about patching and configuring your firewall, and doing all the asset inventories. That is called cyber

hygiene and that's all good to do. We're doing a lot of good stuff there, but below the waterline is where the real danger lies. I use the term, "sharks and glaciers" because everything bad that happens with sharks and glaciers happens below the waterline.

When talking about problems of complexity, hardware and software, firmware, and applications all of these things coming together an incredibly complicated world. We are literally building a world that is highly functional but one we don't fully understand. In order for us to be able to protect the things that we value as a nation, and this is not just about your kid's smart phone working, it is about nuclear command and control systems, power plants in Chicago, medical devices, hospitals, and financial systems, that have to operate as part of the critical infrastructure with some level of trustworthiness.

If we don't have that, then society breaks down from that point. So, how do we deal with all this? The Defense Science Board (DSB), about three years ago, put out an incredibly important piece of work. The DSB was asked by the military, could the U.S. military withstand a massive cyber-attack and still defend the country? That's a pretty important question. They came back in the report and described different levels of vulnerabilities.

There were three different classes of vulnerabilities. The basic idea was that there are known vulnerabilities. That's what we deal with every day. Every week vendors announce the latest patches. We all know about it, and we rush to patch before adversaries can take advantage and exploit. The second class of vulnerabilities are the-zero day vulnerabilities. These are the unknown vulnerabilities. They are the ones we don't know about yet, that are growing at an alarming rate.

Because complexity is exactly equivalent to attack surface, and the more we grow through innovation and sheer demand for these products, systems, and services, just by definition the attack service is growing at an alarming rate. There are the known vulnerabilities, the unknowns, and the third class of vulnerabilities that the adversary actually develops within our systems and networks after they've taken control of the network. Two thirds of those vulnerability classes, the unknowns and the ones the adversary actually builds within networks and systems, are totally off the radar of consumers, and I would argue, most of the folks who are building systems at this point. So how do we deal with that? The only way to deal with that problem is to apply good architectural and engineering standards and best practices.

We've known about these things for a long time. In fact, we have 40 years of security design principles and system security engineering concepts and techniques that we know how to do. The question is, are we willing to do it? That's really the central question for the commission when you take your recommendations back to the President. Sometimes, knowing the right thing to do and having the will to do it are two very different things. The Defense Science Board report was very compelling. Today, there's a whole movement in our security industry to focus on intrusion, detection, and response. Basically, they've decided collectively that systems can't be protected anymore it's just too difficult.

As a result, we decide to become better hunters of vulnerabilities, and we're going to we're going to focus all our efforts on finding those vulnerabilities and fixing the vulnerability. The problem with that strategy is, it's like having a push-mower, and then buy a riding lawn mower, figuring

you'll be able to cover more of the backyard. While at the same, time you buy 6 or 12 new acres of land. The point is, you keep on buying more land, and your tools can never keep up. We call this the "N +1" vulnerabilities problem. Take all the vulnerabilities that exist today, find them and fix them. There will be one more tomorrow, 10 more the next day, and 100 more the day after that. Why, because the attack surface is growing and growing and growing.

We can't protect what we don't understand. We don't have visibility. I spent a long time in the military. It's almost like sending American military forces into combat with without night vision capabilities. They're fighting blind, and we're going to have to do a much better job. It goes to the commissioner's statement about making things simpler. There's no rule that says just because we can build something and we can connect it, we should. Those are decisions that go back to basic architecture and design. There is the idea of resiliency, but we're never going to have perfect security. We hear it's either secured, or it's unsecured. The answer is, it's never going to be fully secured. What we try to do, is increase the penetration resistance on the system to the point where the adversary has to work harder to get access than they are willing to work.

We also have to recognize we are up against nation-state level resources in many cases. The NSA situation and the OPM breach are examples. We will continue to face nation-state levels of attacks because we are a rich target of opportunity. Our paradigm needs to switch to penetration and resistance first. We know from literally two decades of collecting threat and attack data that about 5 or 10 percent of attacks will always succeed with a determined adversary. They will overwhelm at some point and get access. What happens then? The next phase is to limit the damage they can do once they're inside.

Limiting the damage once they're in. What does that mean? It means limiting the time on target, and we can do that through virtualization techniques or limiting lateral movement through the system. Attackers try to find the low-hanging fruit, they escalate privileges until they find a target. That was what the OPM breach was all about. How to limit damage once they're in? Through domain separation, and putting up greater interior walls within the system. I use the example of a safe deposit box: I've got locks on my front door, but I still have a safe deposit box because some of my stuff would be vulnerable in the house. I take it to the bank. It's hard to do, but I know my most valuable property is safe.

In the case of OPM, if they do get in the SF 86 database, are they going to walk away with 22 million records, or are they going to walk away with ten thousand records. Those are the architecture and design decisions that have to be made; not after, but before, as part of the discussion of how do we build security into these systems.

What I would say in conclusion is, if our bridges were collapsing, and our airplanes were crashing at the same rate our systems are failing, we wouldn't be going out collecting more threat data, as we tend to do. We would call in the scientists and engineers. In fact, right here at the University of Minnesota, a few years ago the bridge collapse happened. Many colleagues of mine in the computer science department had a bird's eye view of the bridge collapse in real time.

The first group to be called in following that incident were the engineers. They did root-cause failure analysis. They figured out what was wrong and now the bridge doesn't fail any more. Things are always going to fail at some point. But the question is, where are the scientists and

engineers in building our systems today? This isn't just a problem of smartphones and tablets. The fact that we are totally dependent on information technology for everything we do, whether it's the intelligence community, the warfighters, the manufacturing community, the banking community. In fact, without dependable information technology, your mission or business is going to fail at some point. The problem is, it's not always looking for the cyber Pearl Harbor. The problem is we look for incidents in terms of the kinetic world vs cyber world. In the kinetic world when the World Trade Center was attacked, we could see the attack. We internalize what's happening in kinetic space. With cyberattacks, it happens in cyberspace.

The analogy I would use is like having cancer. In the early stages of cancer, I feel fine and things don't get bad until the cancer replicates to the vital organs. That's one of the reasons why we can't attack this problem, because we think in kinetic terms, and all the bad stuff is happening in cyberspace. Just because your system is up and operating and you think everything is fine, the adversary is ex-filtrating intellectual property out the back of the system.

We are losing, I think the director of NSA said not too long ago, a trillion dollars a year in intellectual property. If you want to bring a superpower to its knees, don't defend these systems. Because the adversary will continue to bleed intellectual property and innovation. Everything that we value as a nation will erode, and erode, and erode, until we wake up one day and we're not where we once were.

I grew up in the sixties and there's no doubt building more trustworthy systems is going to be more expensive than in the past. It's going to be more difficult to do. But I remember during the Cold War, we had a national strategy that was called mutually assured destruction. Possibly most people here may be too young to remember it. We had the nuclear triad, the submarines, the bombers, and the missiles. It was the largest investment cost this country ever made in defending itself. We made the investment knowing very well that there was a very low probability of ever using that capability. We came close a couple times, like in 1962. We made the investment because the assets were worth protecting; our way of life and freedom are priceless. These are things that are so valuable that deserve that level of protection.

That means we're going to have to take a hard look at this problem to protect the things we value the most. We talk about a grand strategy, or a Manhattan-type project. I use the example of NASA and NASCAR, two different worlds but both have something in common. In 1961, President Kennedy made a very famous speech. I was 10 years old and a big fan of model rockets. He challenged the country because the U.S was in a hot missile race with the Soviet Union. He said we were going to go to the moon and do other things by the end of the decade, not because they are easy, but because they are hard. That was 1961.

In 1969, a short eight years later, I remember it like it was yesterday. It was July 20th,and I was a freshman at West Point. I'd been there for20 days, and they woke us up at 2 o'clock in the morning. They marched all 4,400 cadets into a room of this size and we watched the first moon landing. How did we do that with 1950s and '60s technology? The answer is easy, American innovation.

There is no problem a challenge that we can't confront if we bring what I call the essential partnership to bear: government, industry, and academia. The President challenged the best and

the brightest to solve a very, very difficult and challenging problem, one where we all saw the common threat. There is a common threat today, and I would argue today that our cyber security threats and problems every bit as dangerous as those cold war issues.

The real issue is, they operate in cyberspace not kinetic space and I think the challenge for all of us today is, can we recognize the challenges in cyberspace and develop an appropriate strategic plan that activates the essential partnership. We still have the best software developers in the world, and we're capable of solving these problems; I think we can do it we just have to get our heads focused. The commission can play a critical role in providing advice to the next Administration.

Joshua Corman, Director, Cyber Statecraft Initiative; Former CTO, Sonatype; Co-Founder, I am The Cavalry and Rugged Software

There were so many good discussions this morning that I feel compelled to try to add something new to the equation. I wear a few hats as described. I am the new director of the Cyber State Craft Initiative with the Atlantic Counsel, a non-profit policy think-tank in DC. I'm one of the founders of IamtheCalvary.org, which I think is particularly germane today, because we are a group of white hat security researchers founded 3 years ago on August 1st.We are squarely focused on public safety in human life in the internet of things. We make a sort of joke, with contrast to this morning, which is, that we love our privacy but we'd like to be alive to enjoy it.
I think when we look at the most cybersecurity failures, they've been in the realm of acceptable losses. One of the reasons we're still grappling with many of these is because we have lacked a sufficient catalyzing event to create a corrective action. We have kind of solved the easy problems. If it really was easy, we would be done by now. Where we find ourselves now, is with the really, really hard problems.

I intend turn up the heat a little bit, and focus on some of the things I don't think get enough air time. This commission is uniquely placed to make recommendations to the next Administration. I believe we're going to see the first consequential failure in cybersecurity during the next presidency. If we are prepared for that, we may be in a better position to respond in an intelligent way. We all know that markets depend upon trust. But for a moment, especially since it's late in the afternoon, please stare at the ceiling for a good 10 seconds. This building is made of steel and concrete, and not once in the many hours we've been here today has anybody sat in perpetual fear this building was going to collapse on us. The reason we didn't is because this infrastructure that modern societies are built upon is dependable and trustworthy.

The issue I see with the Rugged Software Manifesto, is that our dependence on software and digital infrastructure is becoming as ubiquitous as steel and concrete. However, it's not nearly as dependable or trustworthy. One thing that what we know as computer scientists is that software is nearly infinitely vulnerable. I think we have an expectation that we can place that dependence there, and the software will be worthy of that dependence. We will never have the same level of assurance and trustworthiness in software, which is infinitely malleable, as we do with steel and concrete. Perhaps the very expectation that we can place that trust, is one of the core structural issues.

When we founded the cavalry three years ago, what we said was, the cavalry isn't coming. No one's going to come save us on issues of public safety and human life; Therefore, we must be the

voice of reason and technical literacy, and go to public policy makers and the safety-critical industries to share our expertise on what we know about cyber security failures. We chose the problem statement very, very carefully. I'm going to read it word for word. We said, "Our dependence on connected technology is growing faster than our ability to secure it in areas affecting public safety and human life." To the comment on the last, the purpose of saying 'our dependence', is that when something is not dependable, we can either put a Herculean effort into making it more dependable, or we can depend upon it less.

When I saw Bluetooth being put on an insulin pump that could administer a lethal dose of the drug and cause a fatal outcome, I said, "What the hell were they thinking?" There's no requirement to put Bluetooth on everything. Dr. Kevin Fu, one of the first medical device hackers, said it's the bacon principle. Everything's better with bacon. Everything's better with Bluetooth. We have this assumption that the technology we're using is trustworthy, so we're putting it into every aspect of our lives.

The concern we have is, that trust is not well merited. If we think about IT and software, we have been loath to regulate the software industry. It's the one area of our life where there's no liability. Liability came up this morning, and is going to come up again. There are reasons, and healthy reasons, why we didn't introduce software liability. It was the fastest growing sector of the economy, a global market, and we didn't want to introduce barriers to entry or innovation. There was a long list of good reasons not to introduce liability into society for software.

The challenge is bits and bytes now meet flesh and blood. In the internet of things, software failures can cause physical harm. It not only can erode, but shatter trust in key markets. When we speak about consequential failures, we note that about 100 of the Fortune 500 have lost intellectual property or trade secrets in the last three years. Nearly every PCI-compliant credit card merchant has lost credit card information. In both cases, the failure rates approximate 100% on a long enough timeline. The assumption that we know how to secure software or that we know how to secure IT, is a very faulty assumption. We're placing that weak, vulnerable software into our cars, our medical devices, our clinical hospital environments, our industrial control systems, and our homes. To date, nearly every internet of things device that our research community has tried to hack has been successfully compromised. Again, our failure rate is about 100%.

I want to set out two disturbing vignettes. The first one is, for a few years I researched Anonymous. There are very, very few hackers in Anonymous. One of those hacking crews that actually knew how to hack was called Team Poison. One of the members of Team Poison went by the handle of Trick. Tomorrow marks the one-year anniversary of when he was killed with a drone strike in Raqqa, Syria. What you have with Trick, was someone who was not a very talented hacker, but had enough hacking skill so that with the means, motive, and increasing opportunity, could inflate the loss of life on the U.S., or our allies.

It doesn't take much skill, unfortunately. It takes a search engine like Shodan to see industrial control systems directly connected to the internet. These systems often have default usernames and passwords that can't be changed even if users wanted to. They may also have a free attack tool, and the last bit is the willpower to use it. If harm as a prerequisite contains means, motive, and opportunity, in Trick we saw that out of 7 billion people, the assumption that no one would

hurt us is a very, very, poor assumption.

The second vignette is that this spring in Hollywood California, Hollywood Presbyterian Hospital was accidentally hit by a piece of ransomware that did not get paid in time. As a consequence, they had to divert incoming patients and ambulances to other facilities. They considered moving resident patients to another facility as well. Though they claim no one was hurt this time, but if an accident can cause a denial of patient care in a modern clinical environment, what happens when you combine that with someone like Trick?

One could argue that our dependence on digital infrastructure and areas of public safety and human life is unsafe at any speed. Even if we were to copy the best practices of the private sector, that wouldn't be good enough. We have resigned ourselves to the idea that we can't prevent things. We can only detect or respond. When my credit card is compromised, I can get a new one. But when the other half of your wallet, your family, is compromised, how do you get a new one of those?

I see about 80 billion dollars U.S. spent on protecting credit cards and highly replaceable information, and we're failing. I see very little commensurate care being given to the higher consequences of failure of public safety and human life. I think it's high time we do something about that.

The last bit is we do know some of the technical solutions that could improve things. You heard some this morning from Ms. Zatko, you've heard others about trusted platform modules and hardware roots of trust. We have some of the technical solutions figured out. Some of them we don't. We're going to need a grand challenge. We're going to have to be like in "The Martian", where they said we are going to science the heck out of it. We will need to science the heck out of some of this. In other areas, the gap is not our technical availability, it's our political will, I make two recommendations, which we can talk about during the discussion. One of them is, some in the market cannot make an informed decision, so I've been working on a rubric for several years around software supply chain transparency and food-type labels that do not require an engineering degree.

The simple idea was is actually manifested in a bill inside the Underwriters Laboratory cyber assurances program, the financial services ISAC, American Banking Association guidance, and in the Mayo Clinic's procurement guidance. This is essentially a little trio that could be a near-term fix while working out better engineering solutions. It basically said that anything we buy should provide a software bill of materials for the third party and open source software used in the construction of the goods. Think of it as an ingredients list.

Two, that list should not contain known vulnerabilities or known defective parts without justification. We're not talking about zero days, we're talking about not using a part that's known to be bad.

Three, since future vulnerabilities are inevitable, goods and services must be patchable. In other words, identify the ingredients. They must not be known to be vulnerable, and must be patchable. The idea there had two obvious benefits. At procurement time, a consumer can make an informed risk decision about which company takes better care of their cyber hygiene.

Then when there's an attack, like a Heartbleed, or a bash bug, or the ransomware that ran rough shod over the hospital, we are then able to answer two questions very quickly: Am I affected, and where am I affected, within minutes. To tie all this together, such a bill of materials would have prevented this particular spate of ransomware that's hitting hospitals. It was a known vulnerability in a JBoss component in a single manufacturer's device. If the hospital had known that they were exposed, they could have taken corrective action to fix it. We're talking about the consequences of failure being measured in human life, in GDP, in national security, and maybe putting blood and treasure overseas in a response. If we are unwilling to do even something like a transparent label for the software that we provide, I think what we have is an untenable situation.

The more strategic elephant in the room, which I hope gets some discussion, is software liability. Its time has probably come, especially for safety-critical industries where bits and bytes meet flesh and blood, and where the consequences of failure will be measured in physical harm. It's wildly unpopular and there's fear that if we did it wrong we may hurt the economy, that we may destroy the software industry. There's some legitimate concerns in there. However, the difficulty of solving a problem is an independent value of the necessity and importance of solving it. I think we're at the point now where we have to have those really difficult conversations.

On the Health and Human Services Task Force over which I served, we had no obvious solution to stopping a sustained denial-of-service attack on any hospital in the U.S. When we try to talk about what corrective actions might look like, their response time engineering-wise or research-and-development-wise; to rotate out old technology is a minimum of 10 years. If we want to wait for our Cuyahoga-River-on-fire moment, if we want to wait for the catastrophic failure to catalyze corrective action, we're looking at about a decade to fix it. Alternatively, we think labels such as the food-type labels for detailing the risk being passed on was a good idea. I'll end with one more label that we've been using with the Cavalry, which is a 5-star cyber safety framework for connected vehicles. We should also have a Hippocratic Oath for medical devices with the basic idea all systems fail.

We want you to describe how you're prepared for failure across five dimensions: tell your customers how you avoid failure, that you'll take help avoiding failure without doing the research for helping you, how do you capture, study, and learn from failure, how do you have a prompt and agile secure response to failure, and how do you contain and isolate failure. Those two measures, while they're meant to enable transparency and free market choice, even those two measures were actively resisted by the private sector for fear that it may stifle innovation. I think where we are, in order to take the reasonable steps to enable free market choice and corrective actions, we have to have the political will and the courage to take some uncomfortable solutions to rise above these uncomfortable truths.

Edna Conway, CSO, Global Value Chain, Cisco Systems, Inc.

I'm going to take you down a different road, which is a little bit of the road that recognizes that as we live today, there is no way to literally imbibe software. We need to be aware of, and completely cognizant to the reality that to date, we may live long enough to see the day where we inject software. Today, we are using devices. I think the devices are something that we are somewhat naïve about. Just yesterday, I had an interesting conversation with someone who I'm going to be

facilitating a panel with, who leads a very large effort for information security for a large healthcare organization. The exact words were, "the concept of supply chain and value chain and everybody takes risks with their third party vendors. I'm not sure that was something that I would waste my time on." That was a remarkable statement in a day and age when even as long ago as 2015, reports stated that about upwards of 80% of the breaches we see come from third-party infrastructure.

I think what we really need to consider together, and there's an importance on together, is a pervasive security approach. It's an approach that recognizes that we need an intertwined platform that really looks at collaboration, function, and security together. "Together" is a really critical emphasis for me.

I had the privilege of rowing in undergrad and law school, and it's a time when I learned that if you are in sync and organized together, you can achieve more. When there's a deviant in that, group there is chaos. That is something that we seem to have lost our way on. I urge the commission as they think about what it is that they are going to recommend to the new Administration, that there is a new opportunity to think about the reality that a comprehensive security effort really requires, in other words, an architecture that looks holistically across the value chain.

If you've ever watched five year olds play soccer, they all follow the ball, and cyber is absolutely a critical element. I've watched folks forget about the reality of operational security and physical security. They must go hand-in-hand with cybersecurity in order to have a foundational element set that allows us to move forward together. I heard Dr. Ross talk about a collective of academia and industry, as well as government.

In my written materials, I have offered a whole set of foundational elements necessary to build value chain security. I also defined what the value chain is. It's really the end-to-end life cycle for hardware, software, and services that deliver value in our global communications environment. If we can start thinking about it holistically, we can narrow it down to some of the areas that I believe you've heard both from today's panelists and probably other panelists in the other events. For me, what I'd really like to do is propose that we focus on some kind of an architecture that identifies core domains. It then allows us to set holistic goals together across the spectrum that we just talked about. We can then bring ourselves together with meaningful domains and meaningful metrics.

I'm not going to repeat the eleven domains. None of them should have shocked you. I think there are some highlights that I'd like to raise that I think connect with what I just heard Mr. Corman mention. There are two elements within a domain we call secure engineering and architecture that we absolutely must have. It's really focusing on protection at the design stage. They really building security in, recognizing that nothing will be one hundred percent secure, building it into the architecture and having checkpoints is essential.

The other piece is customer transparency, regarding what I believe is the inevitable product security incident and the mitigation methodologies and solutions that are deployed. Understanding what you're doing and being transparent about it, helps to get to the point of trustworthy products. The challenge lies in how much can be revealed in a world where trade

secret loss is something that is inevitably a goal that some of our adversaries are seeking to achieve. For us, it is a protection area that's absolutely essential.

Balancing that transparency across either requirements for a lifecycle approach to development, whether it's called a secure development lifecycle, or a product security baseline with a layered approach of physical and operational security along the entire spectrum of life cycles is absolutely essential from our perspective. It is certainly something that we've been striving to drive across the industry and as a community.

One of the things that I mentioned in the written materials was there are many good efforts out there that are public-private partnerships that have resulted in good guidance. I look at ISO 20243, which actually started with the DOD acquisition technology and logistics request. It brought in some of us to think together across industry, and across government, about how to identify whether someone was in fact a trusted provider of information and communications technology. It is very different than a view on this device, or this service, or this software. Is it actually secure, and let's look at the security enabling features, and this took a holistic approach.

What we did was try to cover three foundational areas. I had the privilege of serving as a co-chair with IBM's CTO, for the federal systems group on that and wrote something that talks about secure engineering, secure development, and what we called secure supply chain. I'd like to urge the commission to consider as you make your recommendations, a holistic approach with a narrowly defined set of core foundational domains that we need to focus on and a clear recognition that we must have a layered approach. It does not exist in isolation but recognizes that it really lives in a world where there are physical and operational practices that not only affect, but in many cases implement the cyber rationale. It can implement the security we need in the cyber arena.

Panel 3 Discussion

Commissioners of the Commission on Enhancing National Cybersecurity

Mr. Lin: *[To Mr. Corman]* You talked about complexity, and the antagonistic relationship between complexity and security. I agree. Do you have any thoughts on how decision makers, software architects and designers can make informed decisions about the tradeoffs between complexity and security. For example, could one ever come to a reasoned decision to say, "Boss, what you're asking me to do with software is too much. We shouldn't go there because there's no way I'm going to be able to make it secure. Ask me to do something less." Can you imagine a methodology that allows a defense of that kind of a statement?

Mr Corman: This is one of those where we're going some more engineering and innovation. We haven't really stimulated enough of that in parallel implementation. One thing I can point out to you in terms of low hanging fruit is elective complexity, or elective attack service. I spent a few years as chief technology officer of Sonatype. One of the reasons I went there was, it is the largest custodian of open source in the world. I had a global view of who was consuming which Java projects, which versions of which JAVA projects; and when there were vulnerabilities, were they fixed, and how quickly that happened.

Dan Geer, the CISO of In-Q-Tel, a pillar of the industry, and I did some data analysis to look at global

hygiene. What we found, is that for open source projects, there are two questions we needed answers to. When they had a known vulnerability in their dependencies, which percentage of the time did they fix them, and how quickly did they fix them. Out of the global supply chain for all free and available open-source projects, only 41% of the security defects ever get fixed.

That means less than half ever get fixed. The mean time to mediate the ones that did get fixed was 391 days. What that meant was if you were lucky enough for a vulnerability to be fixed, it would be over a year after the vulnerability was being attacked in the wild. This is just the open source project itself. Short of making that information transparent, when you need a login framework you just go grab one. If we started to look at the hygiene of an open source project, it's possible to avoid elective attack service and risk, by choosing one that takes better care of vulnerabilities.

The second thing we looked at was some other hard stats. We looked at thousands of commercial applications, to look at how many pieces they use, how many vulnerabilities are in the pieces they use, etc. We found the average modern application is more than 90% made up of third-party and open source components, which is why I care about software supply chain transparency. What we found is 106 components were in the average application. That's 106 parts and as a ratio of defects to parts, about 23% had a known CVE. Every single one of those known CVEs had a non- vulnerable alternative available right next to it.

When I think about the fact that Hollywood Presbyterian Hospital was taken out with one known vulnerability that had a fix available, coupled with the fact there's 23% of components with known vulnerabilities that are entirely avoidable, we realize we don't need an engineering solution to start to say, if we put a bad Takata airbag in a modern vehicle maybe in our fleet, we'd be sued into oblivion. However, if we use a known vulnerable version of a crypto library or open SSL, or some other batch library it's perfectly okay.
The current state of hygiene, has about a quarter of the open-source is elective attack surface, and completely avoidable. That's why I believe political will is needed to tolerate zero known vulnerabilities, or to be transparent about the vulnerabilities being passing on. Those at least give us a minimum level of hygiene where we might not stop in the termination state but we absolutely could stop someone like Trick, who has less talent, but much more intent to use it.

Mr. Lin: What I gather from your comment, your answer to my question is no.

Mr. Corman: There is a positive trend in development operations, which is the most sought-after development methodology in Silicon Valley and elsewhere. It's starting to make its way into the Federal government through initiatives like 18F. They are realizing that complexity kills efficiency. There's a push to have less monolithic, massive applications, and more smaller micro-services that might have a chance to have less lines of code, less complexity, etc.

It does introduce some new issues, such as the "security is not composable" type issues. Is that actually out of business interests to be efficient, reliable, and innovative less so to be secure? It has some tremendous collateral benefits to security. The Rugged Dev Ops initiative is essentially injecting good security hygiene principles into security concurrent with their evolution. That is a promising area, but I think some additional love, thrust, and incentives could go further on that front. I think there's a lot more to discover.

One more point, we know very little about computer science. One thing we know is, there is a defect rate per thousand lines of code. The rate will vary from human-to-human. Microsoft's XP operating system is about 10 million lines of code. We patch it about once a month. There are several texts once a month. A motor vehicle has 10 times that. It has over a hundred million lines of code and we almost never patch them. We get this code bloat on the attack surface approaching Infinity but our ability to respond is growing linearly at best.

Mr. Chabinsky: *[To Dr. Ross]* You brought up the moon, I think the moon shot is appealing for us to think of, when the nation came together with some end in mind. One of the areas I think is difficult, is that cyber security is such a large problem. We haven't identified those areas where we want to land and return safely from. In the sixties, we said we're going to explore space and then gave that to some project. Where does it get you? I feel like a lot of times, it would be helpful if we focus on particular locations to go to. As an example of that, I look at botnet initiatives where different countries have engaged in them. We have cross-disciplines, different views of that.

The country really hasn't ever brought it together, to really have a sustained strategic view as opposed to discreet tactical levels. What I'm hoping for, are other examples of strategic views where instead of saying we want to work on authentication or something specific. We actually can break this problem down into areas. On the tactics, that if we only apply this U.S. leadership across government, the private sector, and academia; with the proper resourcing we might be able to have goals in mind that can be measured. We can then have that call to action or are there areas that each of the panelists- let's start with you, Dr. Ross, can say, "Here's a good end goal. Let's try to apply the knowledge we have in authentication and design, trustworthiness and boundaries, in policy to achieve this end. Then as a follow-up, where you see a couple of grand challenges that we should be looking for.

Dr. Ross: It's a difficult problem, but I think the one thing we can take stock in all the time is the science. We see the physics of our world have not changed. I go back to my colleague on the previous panel, Mr. McCarson from Intel, with an example of what we talked about, a holistic view of security. We have to talk about the entire system stack, that goes from hardware, to firmware, to operating systems, to middleware, to applications, and all the way out to the communications and the networks. of course on the bottom of all that's our supply chain.

We don't make this an overly complicated problem. We can start doing some of the fundamentals. It's like a great football coach, whether you're talking about the Vikings or the local high school team. They have something in common. The first two weeks of practice in August they work on blocking and tackling, the fundamentals of football. Every coach has them. Even if you have the most sophisticated playbook in the world you start with the fundamentals. We have the same thing. Back in the eighties, we started to focus on the operating system. I was at NSA during that time and our whole goal was to work with industry. There were about a half a dozen companies that built a trusted operating system, and we had a delineation. There's functionality things that we value the product to do and there's also assurance, the two halves of the security coin.

Assurance had to do with more of how was the product built, and how it was designed. It involved design analysis, least functionality, minimization of functions, all the things that make more reliable software. Those operating systems were built, and then we dropped the ball on our end. When it

came time to actually require those products to be used, off the evaluated products list, we decided to give waivers because the customer, military commanders, 3 & 4 star generals, wanted the most recent version of the operating system not the one that was evaluated, which was one generation previous.

I think there is an opportunity here to go back and work with industry to put value on developing trusted components. When building a house, there had to be a good plan, a good architecture. There also must be good components. We talked this morning and this is why I really focused on Mr. McCarson's remarks because Intel is out building the trusted platform, the hardware root of trust.

They are going to write an operating system, and whether they are talking about a general-purpose operating system or one on one of our devices like an Android and iOS, that's where the nerve center is. That's why the adversary will always try to get to the lowest point in that stack they can. Building trust in the application is totally worthless if it's running on an untrusted operating system. We can start to build from the hardware route of trust to trusted operating systems but there has to be some incentive for industry to do that. We can't just say, build it and we will come. We actually have to show up if they build it.

There has to be some value in taking those steps to build a more trusted operating system because otherwise the commercial market place is going to drag us to that application that tells us the optimal time to go to the restroom in the movie we're about to see. That's where we're being pulled. The question is, can we focus work with industry to make it a value proposition for them to bring better components to our systems integrators. On top of that NIST has been working on an integration strategy. It's a systems integration standard that's been around for quite a while. It's an engineering ISO standard.

What we did is, we took the engineering standard and said, what do security people have to bring to the table, because the engineers are those who really build stuff. We have a tendency to focus and talk to ourselves in the security world. We're always around the table and we all agree among ourselves, then we run out the door and nothing happens. Now what we're doing is we're taking our expertise, our 40 years of security design principles to the systems engineers like in COCI, to the people who are running consortiums about how to build things and we're saying, here are some considerations that if you apply these things when building systems, it will increase the level of trustworthiness. It's not perfect assurance but it can be increased appropriately through doing different things. We heard this morning that the most number of lines of code that you can produce that is fully assured or highly trusted today is ten thousand. That's a state-of-the-art. When we talk about building a complex system, we're talking about doing some things on a smaller scale but a highly trusted one and that's okay.

We need to be able to have trustworthy components we need to have an engineering process which recognizes the best practices of the last 40 years, and then have a societal value placed on industry doing the right thing and also making a profit because it's good for business when customers get better security. That's what we always do, and until we can get that business model down in which we talk about the essential partnership government industry and academia.

The government has a huge procurement system and if it were to just buy the trusted technology that we currently have today, we'd be a whole lot better off than we are. We don't buy what we've

already developed and had our great industries develop. It's an unfortunate problem.

Mr. Chabinsky: If you were to take what you just said and do a proof-of-concept, I assume the government has the ability do proofs of concept in its own backyard. How would we recommend that? How do we say, here's the place that the government should show that this works. These are the technologies we actually already have that aren't being used. Let's show the world that we can create that trusted environment, and if it needs more resources it needs more resources.

I'm reminded by a colleague that the money we put into the space program was 20 billion dollars in 1960's, which equates to somewhere around 110 billion dollars in today's money. If money is the issue, and this is the problem and we all think it's as dangerous for democracy as we do, maybe it does require more resources. Maybe it's not market-based. Maybe the solutions won't be able to be driven by creating products that are purchased by the entire world. Maybe the government is going to have to put up some more funding and more money to show that it works first. Where would you start this so that it's not an experiment for the world, but that it's an experiment for one proof-of-concept, and we can show this works.

Mr. Corman: We are so blessed in this country to have so many opportunities to have those laboratories of excellence. We have one right at NIST. The National Cybersecurity Center of Excellence brings together the greatest ideas from industry to do the proofs of concept. We can think on a grander scale and bring in some of those things from the hardware platform roots of trust and get a trusted version of an operating system and running trusted applications. We don't have to focus on a sector by sector concept, because we're all using the same commercial technology. Most of the things we deploy today use the same commercial products. So we have a real opportunity through a lab based experiment like you describe, to show how a proof of concept could be widely applicable to many sectors.

Mr. Chabinsky: I'd like to see them start with IRS taxpayer data, or with OPM with top secret security clearance information. Maybe we can come up with something where we actually can test out if this works for other ideas.

Mr. Corman: I'll give you two that are somewhat arbitrarily chosen, including one of the things that I left out of the testimonies. Dr. Rosekind opens up almost every speech by quoting that there were 32,675 deaths in the U.S. due to car accidents in 2014. It's up 8% and if you do the math that means, about a hundred citizens a day in the U.S. die in car accidents. Ninety-four percent of those are due to human error or human choice. This is why he and his staff are mercilessly trying to get to the semi-autonomous and autonomous vehicles to dampen the hundred or so citizens per day who die due to human error.

My fear, which as you know we've shared with them, is that an exotic attack that leads to loss of life will postpone that promise and that opportunity by 5 to 10 years. My mother-in-law will not trust a connected vehicle. The first thing we see when someone says there's a car hack on a Jeep is, thank goodness I have a 1997 Civic. The problem is their 1997 Civic is significantly less safe than the modern cars are for a whole bunch of reasons. As soon as they add a Verizon hum dongle to it they just made their un-hackable Civic, a hackable Civic. I would love to see a grand project that says, can we make vehicles that can be can operated safely while compromised. The notion of resilience and survivable systems is that there can be a degraded performance that's still safe to operate.

An issue with current hacking of cars is not that they are hackable. Cars will be hackable forever. The issue is that if one hacks the infotainment system, they can also shut off the brakes or the steering wheel. It is incredibly poor segmentation isolation. I would love to see a reference architecture for a defensible resilient connected vehicle, because if we shatter that trust we're saving a hundred humans a day that we could be saving with existing available technology.

The second one is shorter in its description is the clinical healthcare environment. One of the previous testimonies in New York was from Greg Rattray. He testified that they have over 2,000 full-time security staff members at JPMorgan Chase. They have an over 600 million dollar security budget. Despite those resources they still get breached routinely. How then, can a health delivery organization with zero security staff have a fighting chance?

The second grand project I'd like to see is how to really easy to design and implement segmentation and isolation of clinical medical systems, so that they are on a need-to-know basis in a way that does not require a massive staff of security professionals. We have prototypes and ideas in the private sector on how to do this. However, we have a dearth of future talent and workforce that could actually go look in those hospitals. An environmental constraint is we want the benefits of connected and precision medicine. We want to solve and cure diseases with machine learning and AI, and have more information sharing. None of that's going to happen if chief medical officers are afraid of getting hacked weekly due to ransomware or other ideological attackers. The two areas that I would focus on are public safety and to preserve the promise of these connected technologies would be vehicles and healthcare.

Mr. Modeste: I'll take a different tack. We've looked at it for the last 2 or 3 years. I've been engaged in that process. As I've looked at it there's a similarity in the problem. If you look at it from healthcare, transportation, industrial control systems, or just the consumer view, the problem is what Mr. Corman pointed out, namely, software. Software is a significant issue. Right now today, it seems we throw up our hands and just accept it. We seem to accept we will always have poorly written software. We accept that after ten thousand lines of code, we will have poorly written software.

That is the challenge. It is one of the big challenges the commission should look at. Where can you start to have secure software? How can you build a foundation to start having secure software? Because that software resides in a car, in a smoke detector, in an oven that can be turned on remotely. It's the same software in medical devices. The challenge is, how do you set up and build secure software. Mr. Corman gave out some really interesting statistics that we've seen regarding vulnerability issues. The challenge is people know they are putting software into their products that have flaws in it.

We are a safety company that has been around for 120 years. No one can come to us today with a device that catches fire. No one can come to us today with a component in their device that could probably electrocute someone. However, from a software perspective it seems that it's ok and acceptable to allow questionable software to continue.

That was the premise behind our program, to start with something that's reachable and attainable while also recognizing there are different bad actors. If you mention the hacker from Syria, you have some guys who have the ability and the tools to go after companies and their products. What

are they doing? They're going to go after the low-hanging fruit. If I want to rob your house, first I'm going to walk up to the door and try the door. If it just so happens that that the door is open and the car is not there, there is no need to try to circumvent the security system. I think that's a problem.

It is important to look at the fundamental tenants of software for good security practices. These have been mentioned by Mr. Corman and Ms. Conway. We look at software weaknesses. We've had the same top 25 software weaknesses that have existed time and again over the last decade. One of the objectives of this commission is to make that top twenty-five obsolete in ten years. There may be another top twenty-five in the future, but the present list should be obsolete. It makes it hard for the bad actors to go after those systems. In this way, a foundation can be built for smart cities, smart homes, or smart cars. That's where I would take a different tack and go after something significant.

Mr. Corman: We know how to stop SQL injection. We could eliminate SQL injection if we chose to. We can forget the top 10 or 25, let's talk about the top one. We haven't comprehensively eliminated SQL injection. We can, but we have no incentive to do so. Therefore, we haven't done it. That's why I believe both of us led with the idea that while we have engineering challenges, the primary bottleneck right now is the incentive structure to motivate people to avail themselves. I was really moved by the Intel testimony in the second panel, because the trusted platform module and roots of trust was very, very promising and nobody adopted it. I don't want to create this battle chest of really cool technical innovations that doesn't have the incentive to do so.

One of the reasons we get to software liability as a concept isn't telling every innovator how to achieve a certain outcome, but let them make their own risk decisions. If they want to be really sloppy with chain and have millions of lines of code because they think that no one would ever attack their goods, let them make that risk decision. However, if they get it wrong there should be some sort of consequence for doing so. To me it's less about what's available in terms of engineering innovations. We have and more, why should anyone bother looking at them becomes the issue. The current state of affairs is a software developer can make a risk decision on behalf of their customers without telling them what decision they made. As they pass that risk on to the customers, the customer is under no obligation to know the risk they are inheriting from their software provider. Then, when harm is caused on the customer there's no legal recourse to do anything about it. The thinking is, it's none of my business what you did, I'm not allowed to know what you did, and I can't come after you for what you did. That's a failed market.

If you wanted to get people interested in either funding some of these engineering innovations, or funding R&D, or removing elective complexity, or adding fast secure over-the-air updates that came up in a prior panel, there must be an incentive structure that makes us want to consider and adopt and experiment with them.

Mr. Chabinsky: I particularly like the comment you made about the SQL injections, when you said we know how to do it but we just haven't done it. To the extent as you consider what would you normally do in your daily life anyway, the more examples that you can forward to us about those areas where it's really just a matter of will and someone needs to take a leadership role, just say we've been having sequel injection attacks and losing entire databases of private information for 15 years, it will end within one year. Those are very, ears and eyes wide open and so are the grand

challenges. Those are things that I would love to see some short term movement to pull all that together.

Ms. Conway: A few comments in answer to your questions. I very much resonate with everything that has been said. I think some of it is already out there, as Mr. Corman has said. He offered two industry areas where we can target some things as proofs of concept. I want to go back to the fact that there is a body of work out there on the secure development life cycle. He talked about things like segmentation in healthcare. How to segment information is well known, just like SQL injections. If people aren't doing it then the answer is, in certain critical infrastructure environments and in health care, we need to make decisions on what we're going to permit or not permit with government-funded dollars. I think that's the solution. You only are going to get what you pay for.

The concept of secure development life cycles, and how to deploy it is out there. With software and hardware, if you want to reach some really innovative areas you ask Mr. Chabinsky. I didn't have the privilege of listening to Intel this morning, but I think if you remember that integrated circuits are the heartbeat of all electronics.

I want to focus on three areas that I think we can work on together: There are some fun things that can be done at the hardware level with secure integrated circuit design whether it's doing something like key base hardware obfuscation, or deriving polynomial expressions as a fingerprint. These things can help us determine as procurers what is, and is not secure. Determine if vendors meet them or don't need them and then make an educated decision on what you're buying.

I think this goes back to the free market, and a set of requirements on purchasing and utilization of a secure development lifecycle capacity, as well as techniques that are already well-documented in industry and academia and just need to be embedded in procurement processes.

Mr. Gallagher: I wanted to follow up on something that I heard from everybody at some level, and that was the question of liability issues and enhancing the professional standard of care. I wanted to ask you specifically what you think the commission can do to support any recommendations. The two issues I want to raise are, to what extent do we understand the base level of care that would be applied in a liability situation, and the second one is the difference between things happening in cyber and kinetically, which is the unseen nature of the harm or damage. In other words, we've seen it happen before where the inability to describe the harm becomes a barrier. Would you comment, and try to point us in the right direction.

Mr. Corman: Software liability is a third rail topic. But, if we don’t' talk about it now, we will be talking about it after we've implemented it poorly. On the Health and Human Services task force, one of my first observations, and this will sound like a contradiction, I carry some cognitive dissonance here and I'm sure this group can figure out the tension. When you look at how hackable medical devices are, and how hot packable hospital clinical environments are, it's very, very bad.

Billy Rios looked at a single device and it had over at 1400 known vulnerabilities in it. Fourteen hundred vulnerabilities, and it wasn't really an anomaly. That's pretty much par for the course. It's a reminder it takes only one to harm patient care. When you look at this kind of stuff, one of my observations was it was actually true that "meaningful use" was our original sin. We wanted to dramatically accelerate the availability of electronic health records. These devices were never

threat model designed or architected to ever be connected to anything else, we slapped the connection on to everything else in a big hurry.

That was an example where when we want something badly we get it done badly. I'm loath to introduce another perverse incentive with the idea to go to software liability. That said, I believe we're going to have a crisis of confidence moment in a car or medical device and through the court system will going to have case law introducing that the EULA does not waive all responsibility.

The family that's suing for the loss of a loved one is going to have a reasonable expectation that whether it's a physical brake pad failure, or software failure, in the patchy struts it's still negligence. Accidental case law is very malformed and could do serious damage to the software industry. One of the older ideas I've been socializing for a while now is vendors are not responsible for zero day vulnerabilities and exotic attacks and writing perfect software. Perhaps there is responsibility for known vulnerabilities in products, or at least passing along transparency about them. One of the things Ms. Zatko said this morning was that food labels don't tell you it's not junk food. You can still buy and eat junk food. Lack of informed consent and use of known vulnerabilities doesn't fly anywhere else.

If we wait for the case law to happen, we will have whatever software liability actually happens and it could kill the software industry. As an example, if the liability was put on the developer who introduced Heartbleed, no one would ever write open source software again. It's my belief that if we know failure is coming, we should design deliberately where to place the liability, and where to limit the liability. The software industry hates the idea of this supply chain transparency. If you think about that rubric for 30 more seconds right now, if you flip the switch to software liability and someone like a software provider is responsible for all harm that could be very untenable. Whereas, if vendors are responsible for a bill of materials and offering a patch and the customer chooses to use your product in spite of bad hygiene, or fails to apply the patch that's their problem. I'm taking unbounded liability. We have made it really a two-legged relay race at least. I think we're going to need to dig this well before we're thirsty. That's just a grossly oversimplified rubric, but if we can define what a reasonable expectation is for liability, it might be something in between the Draconian measure that could hurt things and "a come as you are do as you please" attitude and an untenable situation as it is right now.

Mr. Ross: I think the answer to your question is we don't know enough yet about where to set the bar. Setting up prematurely as Mr. Corman said may have a catastrophic effect on our industry. We have the best anywhere, and we don't want to do that. I do think there's an opportunity I talked earlier, this notion of functionality and assurance. Functionality means all the features that the developers load up in the products. The assurance clarifies how much to trust the product to do what it is supposed to do, and not do things it's not supposed to do. That assurance can be defined on a continuum for everything from low insurance to very high assurance.

Vendors have to work a lot harder to get high assurance. We typically find in high assurance products a reduced set of functionality. It kind of goes back to something that's simpler to define and to build is also easier expect greater trustworthiness because there are less things to worry about. When we talk about testing and evaluating, we can never test 60 million lines in an operating system. It is just too many pads in that software. We talked about the notion of a kernel-based

operating system. It's a very small piece of code that can be highly trusted. We know how to do that. Maybe one of the solutions is that we develop a continuum of assurance type of criteria and let the software industry define where they want to come down on that level of assurance.

In some sense if I'm building a widget and this widget can perform up to a certain level of trustworthiness, I'm going to work a certain length of time to make sure I reach that bar. There's some ways to define it. In our business, there may be other high assurance there so that you will never trust a garage door opener. It does one thing, but it does it every time. It's highly assured. They can go on record as saying they build a trusted garage door opener and build it to a higher level of assurance. They can present the higher level of assurance. We already have these international standards.

The common criteria has functionality requirements and assurance requirements it's been around for a couple of decades now and we just don't use it like we could. It's one area where we can give industry an opportunity and a way in however they feel comfortable. Then incentivize companies through government procurement for elevating that bar over time. We can reward companies that build more trustworthy products. I'm going to favor that project and that's a good thing. It generates competition outside of regulating the whole industry. Competition does wonders. We saw this in the eighties with the operating system developers they were all competing to build the first trusted operating system. Had we not dropped the ball, we might have been a different place today. That's one aspect of how we could do it.

Mr. Lee: I've been a little indecisive here because I don't really have a question. It's more of a reaction or a philosophical reflection. Maybe one or more of you may have a reaction. One thing I haven't heard too much is the word, "network". There has been a lot of focus on software single systems. It strikes me that much of the real vulnerabilities and the large dangers are in networks and interconnected systems. The real tension, when you talk about things like liability, is the fact that at least today, much of our nation's economic growth is based on the exploitation of network effects and that is the fundamental conflict and so I was just reflecting here about why we're hearing a lot of assurance of software systems but much less about the complexities of network systems and the economic growth imperative.

Dr. Ross: I mentioned that the engineering publication that we're working on now will be out in September and the final in December. We have a concept of a system boundary that is composed of 1 to N system elements, where an element could be a hardware platform, operating system, application, person, or policy. We talk about networking. A network in some sense is a collection of system elements. The thing that we address is that every one of those system elements should have a defined level of trustworthiness to some transparency mechanism.

We're never going to have a world where every element is going to be at the highest levels of assurance. We're going to operate the way we always do. It's critical as we build the internet of things that it's really a system of systems. We have to have a paradigm where everyone who contributes an element to that system of systems, we're able to determine the level of trustworthiness they bring to the table. We then have the ability to assess risk. When we start to have that kind of incentive, for companies to compete for those trusted elements, the bar raises a little at a time. It will never be a perfect world. We are running at warp speed with technology and

innovation, and we never want that to stop. We want to be able to understand what we're building and how we're building it, and how much trust to put into all of it. That is what the guideline is attempting to bring to the process.

Mr. Corman: The Cavalry has made significant strides with the Food and Drug Administration on raising the bar on pre-market and post-market guidance for devices atomically. There is still a long way to go. The example in the clinical environment is a segmentation problem. It can be done in a device. I think one of our assumptions is that everything must be connected to everything else.

I think we need to go to more need-to-know, or mesh, or cohort-based trusted networks. We often start with devices because security is not compose-able. If we are not starting with defensible end points, it makes it worse. Now that we are making strides on medical devices, the concern shifts to how to make scalable, manageable network segmentation isolation or isolate cohorts. The internet benefits so many parts of the private sector, but it is the bane of security. We want the free openness of everything, but there are no good neighborhoods on the internet. The idea we can connect safety-critical industries on the open internet is probably going to be challenged at some point. I would rather see higher assurance networks, or alternate principles embraced. It's not so much that we don't know how to do it, but we don't know how to do it at scale. On the vehicle front, it's not the software in the car, it's the amount and type of attack surfaces we allow.

Following 9/11, the most important change that probably prevented attacks was hardening the cockpit door in aircraft. We have to think about the 80/20 rule and apply it to networking. The level of exposure probably merits more attention than how attackable they are.

Public Comment

Kent Pankratz, American Family Insurance

Mr. Pankratz spoke about consolidating security controls. He recommends different sets of security controls specific to industry, including risk management. How is PCI implemented and HIPAA? Metrics should provide answers to how security posture is quantifiable. He talked about consolidating security controls; and recommended to maintain the separation of control.

Eileen Manning, Cybersecurity Summit coordinator

Ms. Manning runs focus groups for CEOs She urged the commission to remember small and medium sized organizations in its deliberations. Big companies are aware of cyber security, but medium to small entities don't feel cybersecurity is their issue. They have said they will address if they ever get hacked. Whatever we can do to heighten that awareness to make sure people realize cybersecurity is everyone's concern.

George Wells, Imaging and Pictures, Inc.

Mr. Wells thanked Dr. Ross and Mr. Corman for bringing the commission back to a strategic point of view. He noted the problem with cybersecurity that happened in 2010 as a direct result of Hurricane Katrina. The southern backbone was knocked out as a result of the storm, and the middle internet backbone of the country was severely taxed. We need to increase redundancy. A northern backbone would decrease potential strain on the rest of the system. Cybersecurity baked in to PC smartphones and tablets. Mission critical infrastructure should be protected by the civil version of

SIPRNet. Hubris is not a viable security option.

Adjournment

The meeting adjourned at 4:07 p.m., Central Time.

Annex A: List of Participants

Last Name	First Name	Affiliation	Role
Todt	Kiersten	NIST	Executive Director, Commission on Enhancing National Cybersecurity
Donilon	Thomas, E.	O'Melveny & Myers, Vice Chair, Former U.S. National Security Advisor to President Obama	Commission Chair
Palmisano	Samuel, J.	Retired Chairman and CEO, IBM Corporation	Commission Vice Chair
Anton	Annie	Professor and Chair of Interactive Computing at the Georgia Institute of Technology	Commissioner
Banga	Ajay	President and CEO of MasterCard	Commissioner
Chabinsky	Steve	General Council and Chief Risk Officer, CrowdStrike	Commissioner
Gallagher	Pat	Chancellor, University of Pittsburgh	Commissioner
Lee	Peter	Microsoft Research Corporate Vice President	Commissioner
Lin	Herb	Senior Research Scholar, Stanford University	Commissioner
Murren	Heather	Former commissioner on the Financial Crisis Inquiry Commission	Commissioner
Sullivan	Joseph	Chief Security Officer at Uber	Commissioner
Harman	Michelle	NIST	Designated Federal Officer (DFO), Commission on Enhancing National Cybersecurity
Amin	Dr. Massoud	Dr. Massoud Amin, Director, Chair, Technological Leadership Institute; Distinguished University Professor, University of Minnesota	Presenter
Booker	Robert	Senior VP, Chief ISO, UnitedHealth Group, Optum, Inc.	Presenter

Last Name	First Name	Affiliation	Role
Conway	Edna	CSO, Global Value Chain, Cisco Systems, Inc.	Presenter
Corman	Joshua	Director, Cyber Statecraft Initiative; Former CTO, Sonatype; Co-Founder, I am The Cavalry and Rugged Software	Presenter
Grant	Susan	Director, Consumer Protection and Privacy, Consumer Federation of America	Presenter
Johnson	Mike	Director of Graduate Studies in Security Technologies, Technological Leadership Institute, University of Minnesota	Presenter
McCarson	Brian	CTO, Intel IoT Strategy; Sr. Principal Engineer, Chief Architect, Intel IoT Platform	Presenter
Modeste	Ken	Global Cybersecurity Technical and Strategy Lead, Underwriters Laboratories, Inc. (UL)	Presenter
Moriarty	Kevin	Senior Attorney, Division of Privacy and Identity Protection, Bureau of Consumer Protection, Federal Trade Commission (FTC)	Presenter
Ross	Ron	Computer Scientist, National Institute of Standards and Technology (NIST)	Presenter
Toretti	Gary	Chief ISO, Sabre Corporation	Presenter
Zatko	Sarah	Cyber Independent Testing Lab	Presenter
Manning	Eileen	Cyber Security Summit	Presenter/Public Participation
Pankratz	Kent	American Family Insurance	Presenter/Public Participation

Last Name	First Name	Affiliation	Role
Welles	George	Imaging and Pictures, Inc.	Presenter/Public Participation
Barrett	Mark	Exeter Government Services	Event Staff
Chalpin	JP	Exeter Government Services	Event Staff
Salisbury	Warren	Exeter Government Services	Event Staff
Aerts	Bill	Medtronic	Attendee
Crooks	James	O'Melveny & Myers	Attendee
Daggett	Doug	CICS	Attendee
Dajani-Brown	Samur	Honeywell	Attendee
Danda	Durga	N/A	Attendee
Dandar	David	MITRE	Attendee
Debrouvier	Hemille	UMN	Attendee
Dennis	Charles	UMN TLI	Attendee
Dodson	Donna	NIST	Attendee
Dufresne	Joe	UMN	Attendee
Dutt	Brian	St. Jude Medical	Attendee
Edlund	Dawn	St. Jude Medical	Attendee
Eggers	Matthew	US Chamber of Commerce	Attendee
Englund	Tyler	CICS	Attendee
Fancher	Angelique	UMN	Attendee
Fenten	Mike	Legislative Audit	Attendee
Fries	Joel	N/A	Attendee
Grat	Susan	CFA	Attendee
Greenauer	Derek	UL	Attendee
Hanson	Michael	Sabre	Attendee
Haroian	Kevin	UMN	Attendee
Hawkins	Steve	UMN/TLI	Attendee

Last Name	First Name	Affiliation	Role
Hildebrand	Nicholas	Best Buy	Attendee
Huerte	Yeeth	UMN	Attendee
Hydrie	Waris	St. Jude Medical	Attendee
Isle	Brian	UMN	Attendee
Jackson	Caprice	UMN	Attendee
Jackson	Jay	3M	Attendee
Jenn	Helen	UMN	Attendee
Jeries	John	St Catherine University	Attendee
Johnson	Clete	Department of Commerce	Attendee
Jones	Alex	Best Buy	Attendee
Kaveh	Mos	UMN	Attendee
Kinstad	Brian	Midwest Reliability Organization	Attendee
Klein	Joseph	Emergent Networks	Attendee
Knake	Rob	Orkestrel	Attendee
Knether	Katherine	N/A	Attendee
Koepsell	Keith	UTC	Attendee
Korgeu	Tim	Absolute Software, Inc.	Attendee
Kors	Veronica	City of Roseville	Attendee
Kosten	Chris	Kroll	Attendee
Kozak	Mark	On Semiconductor	Attendee
Kroth	Alan	Optum	Attendee
Landfield	Kent	Intel	Attendee
Larson	Kevin	Honeywell	Attendee
Larson	Judd	UMN	Attendee
Latin	Brenden	UMN	Attendee
Lawinger	Larry	LCI	Attendee
Lentz	Chris	Centerra Group	Attendee

Last Name	First Name	Affiliation	Role
Liban	Mohammed	SIM	Attendee
Livon	Eli	UMN	Attendee
Madson	Kirk	UMN Foundation	Attendee
Mahn	Amy	DHS/NIST	Attendee
Malone	Denice	Auditor	Attendee
Martinez	Richard	Robins Kaplan	Attendee
Mayfield	Mark	City of Roseville	Attendee
McHugh	Brandon	UMN	Attendee
McLane	Shane	Multifeeder Technology	Attendee
Meeker	Tina	BestBuy	Attendee
Miller	Galom	CICS	Attendee
Min	Derek	UMN	Attendee
Montoya	Jerrod	OATI / InfraGuard	Attendee
Morris	Ken	KnectiQ	Attendee
Morse	James	CenturyLink / ITT Tech	Attendee
Mulder	Tiffanea	Frederickson & Byron	Attendee
Murawski	Paul	Valspar	Attendee
Niejelow	Alex	MasterCard	Attendee
Nolan	James	UMN	Attendee
Oberhelman	Amy	Target	Attendee
Ostaffe	Mike	Iteris, Inc.	Attendee
Parry	Mark	Mayo Clinic	Attendee
Parsons	Brenna	UMN	Attendee
Payne	Charles	Adventium Labs	Attendee
Peluso	Maria	UMN	Attendee
Peretti	Gary	Sabre	Attendee
Peters	Mark	MITRE	Attendee
Peters	Marcia	US Bank	Attendee

Last Name	First Name	Affiliation	Role
Peterson	Richard	Uponor, Inc.	Attendee
Pierson	Jim	N/A	Attendee
Radzak	Lisa	APMG	Attendee
Regenreif	Dillon	UMN	Attendee
Reikes	Anaj	CICS	Attendee
Romine	Charles	NIST	Attendee
Rushemeyer	Joel	Valspar	Attendee
Scholl	Matthew	NIST	Attendee
Schultz	Brenda	N/A	Attendee
Schwamberger	Benjamin	UMN	Attendee
Sedgewick	Adam	NIST	Attendee
Seeberger	Michael	BSC	Attendee
Seierop	Scott	St. Jude Medical Center	Attendee
Singh	Pramod	UMN	Attendee
Sivagnanam	Mangaya	MSST	Attendee
Skeglund	Benjamin	N/A	Attendee
Smith	Angela	NIST	Attendee
Smith	David	US Bank	Attendee
Soderquist	Jeff	MN-DHS	Attendee
Souppaya	Murugiah	NIST	Attendee
Stegall	Rachna	UL LLC	Attendee
Stine	Kevin	NIST	Attendee
Strobel	Sylvia	APMG	Attendee
Surine	James	Smiths Medical	Attendee
Swenson	Jeremy	TLI / Optum	Attendee
Tabor	Daniel	Optum	Attendee
Tan	Eduardo	TK	Attendee
Titiner	Aaron	N/A	Attendee

Last Name	First Name	Affiliation	Role
Truong	Hung	SIM	Attendee
Tschider	Charlotte	Mitchell Hamline School of Law	Attendee
Ubel	Andy	Valspar	Attendee
Vold	Tim	Lawinger Consulting	Attendee
Waggoner	Joseph	Optum	Attendee
Wampach	Aaron	Health Partners	Attendee
Warhol	Erin	Black Opal	Attendee
Whelan	Ted	Clifton, Larson, Allen LLP	Attendee
Williams	Jeff	UMN	Attendee
Wu	Winnifred	Consultant, Medical Devices	Attendee
Young	Bill	Valspar	Attendee
Zuidema	Liz	Microsoft	Attendee
Mitchell	Charlie	Inside Cyber	Media