COMMISSION ON ENHANCING NATIONAL CYBERSECURITY

Meeting of the Commission on Enhancing National Cybersecurity

PANELIST STATEMENTS

University of California, Berkeley

Berkeley, CA

June 21, 2016

Table of Contents

Panelist Statements

Patrick Heim

Chairman Donilon, Vice‐Chairman Palmisano and Distinguished Members of the Commission, thank you for the privilege of addressing this panel.

For background, I have worked in the field of information security for over twenty years. During that time, I have had the opportunity to work as an IT engineer, penetration tester / hacker, technology auditor, security consultant, and security product leader. I have also held CISO / security leadership roles in healthcare (Kaiser Permanente and McKesson) and cloud technology (Salesforce and Dropbox), advise multiple security startup companies and sit on the board of directors of an anti-malware startup (Cylance).

As a late addition to the agenda, I have not had the time to prepare a full written statement. I would like to present the following three areas of discussion:

1. The "failure of economics" of technology and challenge of scaling security as a root cause of persistent vulnerability.
2. The challenge of educating citizens and consumers globally in good security practices and the role technology providers have.
3. The diminishing role of "the network" as a security mechanism and the resulting need to evolve security controls.

I hope these perspectives have been helpful to the commission.

Hemma Prafullchandra

Thank you for this opportunity to provide input to the Commission on Enhancing National Cybersecurity. Clearly this is a broad and complex topic and I truly appreciate the efforts of the Commission. I recognize how difficult it will be to create solutions that work globally and are enduring for some period of time, especially given this pace of technological change and as we have yet to fully understand the lasting consequences of our digital innovations.

Americans are progressively using their numerous digital/mobile devices more and more to interact with everything. Daily life is becoming extensively dependent on our digital economy, from communicating with others globally, to daily interactions with essential services in every sector, such as, financial, education, healthcare, entertainment, retail, automotive, utilities, airlines, agriculture, government, etc. Many of these sectors are actively adopting cloud-based solutions to reduce cost and become more agile.

Given the 'interconnectedness of cyber' technologies, solutions to enhancing national cybersecurity must take an internationally collaborative and holistic approach. We need to rethink what we consider as our 'national critical infrastructures' as we introduce additional smart devices and technologies, broadly leverage data analytics, and further automate our physical control systems. We need to identify and protect 'global critical infrastructures' as cloud companies, such as, Amazon, Apple, Google, IBM and Microsoft continue to grow in global footprint, and become aggregate providers of a diverse set of digital technologies that become vital to our daily lives. Also, the US Government (USG) and many global commercial companies, especially those managing key assets such as currency, payments, energy, and information, are still transitioning to cloud technologies and modern protection measures, and they remain highly vulnerable to criminal and state-sponsored attacks. As a result, there is broad variability in the security of many of these commercial and government entities that manage these global critical infrastructures.

Unlike China, Russia, Israel, and other state-led economies, 95% of the critical assets in the United States are owned and controlled by private industry and have very little or no protection directly from the USG. Today, there are a variety of consultative mechanisms between the USG and industry such as ISACs and the provisions of the newly enacted Cybersecurity Information Sharing Act (CISA) of 2015. These mechanisms represent good opportunities for interaction between the USG and industry, but funding can have a greater impact. While the USG will spend over $20 billion in 2016 to secure government systems and networks, it will barely spend any money on private industry protection either directly or indirectly, and will leave companies large and small to fend for themselves. There already is a massive mismatch between private spending in cybersecurity and the exposure of privately held assets to cyber attacks. The pace of innovation will only continue to increase, and our current protection approach and spend will no longer suffice. The ability to implement adequate protection measures exceeds the capabilities of both commercial and government entities. SMB's have even lower awareness of these issues and/or expertise to respond. Large companies typically spend 1%-4% of their budget on protection measures, but still fail to consistently implement basic controls (partly due to the dynamic nature of the IT environment and the large number of threat vectors). All sectors are struggling due to insufficient talent. Additionally, in the government sector the challenges include outdated procurement and operating processes, and a large number of legacy application and systems further reducing their ability to quickly adopt modern technology and protection measures.

Recommendations:

Cybersecurity is every ones responsibility and we only win if we work together. As a nation we have huge dependencies on suppliers and partners, who may not be implementing the same level of protections as we do, and can be taken advantage of to bypass our protections. We really must take a holistic approach to avoid any gaps leading to failures. The USG should work with private industry as cloud adoption gains momentum to prioritize the areas of most critical concern and provide leadership and funding to support the securitization of these key assets and industries in the cloud.

These key assets must be able survive attacks from nation-states, cyber-criminals and organized crime syndicates.

We must teach cybersecurity to our children before the first time they interact with anything digital. We must start as early as possible and make cybersecurity a core part of the curriculum for Pre-K through high school, as we do today for traffic safety and drugs. Personally I think we need to go further and make cybersecurity education as foundational as math and language. We should reinforce over and over such that it becomes second nature to our society.

We must develop a global standard with a minimum acceptance level of interoperable protections for all digital technology that all vendors must meet before they can be released on the market for Americans to use. These acceptance criteria must be met on all imports and services offered by/from other nations to Americans. To scale and reduce impact on the pace of innovation, the validation and certification can be self-service with a tiered model of self-assertion and/or integration testing, and/or third-party independent testing depending on the level of assurance required in the protection measures, and can be delivered as cloud services. We must fund programs to implement the infrastructure and incentivize adoption across the board. An example of an essential protection measure is identity and access management, and monitoring of data breaches. Cybersecurity requires global interoperability and standardization of these minimum protection measures allowing Americans to have confidence that they are being protected equally well as they interact with different global cyber environments. The USG should explore methods of assisting and directly or indirectly supporting commercial companies, especially those with vulnerable critical infrastructures, to augment their efforts and expedite their adoption of robust cloud security measures. We need to put programs in place for cybersecurity similar to what we have, for example, with FDA Medical Devices and FTC Bureau of Consumer Protection.

The battle for secure cyberspace is being waged across the globe every day in a rapidly changing and unpredictable way. Nevertheless, there are best in class solutions that have been or are being developed to address these threats to infrastructure, user, data, and workloads such as Virtual Machines, Containers, Mobile Applications and IoT. While the marketplace for cyber defense is large and adaptive, it needs clearer direction from the USG in the areas where it should focus investment and technological development, and encourage centers of excellence. We should collaboratively research next generation computing and protection mechanisms, such as quantum and neuromorphic computing, and quantum cryptography and automated, intelligent protection measures. With automation, orchestration, artificial intelligence, and machine learning we can help scale and provide predictive, repeatable, and traceable protection measures. Automation can remove the need for many to be experts (e.g. Cryptography/Encryption experts) by enabling the configuration of the protection measures to be done by a few experts to a tag/label associated with the data/asset classification, allowing the operational personnel/systems to simply/automatically tag, whereby the protection measures systematically get applied and enforced. Automation enables consistency across multi-cloud environments, and freedom to select different cloud environment at any time. USG should work more closely with industry to gain access to such innovative technologies and help commercial companies of all sizes become aware and gain access to best in class capabilities, technologies, and systems.

Alex Stamos

Good morning Chairman Donilon, Vice-Chairman Palmisano and Distinguished Members of the Commission. My name is Alex Stamos, and as the Chief Security Officer of Facebook I am honored to be able to speak to you today. Our mission at Facebook is making the world more open and connected. Connecting people together and helping them share has produced huge benefits in lots of different areas: helping small businesses grow, providing a platform to publishers, giving voice to individuals, and strengthening communities. This is the starting point for all the work that we do, and we apply these lessons to our security approach as well.

As members of the Commission are aware, several long-term trends continue to complicate efforts by the private sector to significantly improve cybersecurity at a national level. On one hand, many companies are doing well in meeting obligations to customers, employees, and shareholders. These companies have dedicated security executives, large teams with diverse skill sets, and the ability to build their own security solutions or to customize off-the-shelf technology to fit their specific needs. On the other hand, it is still too difficult for all businesses, large and small, to adopt this model due to external trends, including:

- A continuing lack of entry-level and mid-level cybersecurity talent, both in terms of the number of qualified candidates as well as the skills taught in many academic programs;
- An expanding set of companies, organizations, and individuals facing criminal offensive teams with capabilities previously exclusive to nation-states;
- Deficient collaboration between private companies, the public sector, and the security research community.

At the same time, we're seeing promising success from a dedicated effort by the private sector and the emergence of an encouraging legal and regulatory environment. Continued focus and support for these initiatives could go a long way toward improving the security of American citizens and businesses.

Lessons we've learned through these efforts may be applicable to other companies and sectors:

1. **Modern defense is about more than preventing initial compromise.** An effective defense strategy depends on the correct mentality, recognizing that in 2016 any moderately sized enterprise needs to build multi-layered security architectures and be prepared to respond quickly and decisively to incidents.
2. **Information sharing greatly increases the costs to attackers.** Many types of online abusive behavior, ranging from simple spam to the most advanced attacks, can be made more expensive and less effective through timely, automated threat sharing between trusted partners. We are proud to operate a free threat sharing platform called ThreatExchange with the participation of 350 companies, and we hope that the benefits of real-time threat sharing become available to smaller organizations soon via future integrations.
3. **Better collaboration between the corporate and security research worlds is key.** In the earlier days of the security research community, it was generally dangerous to report flaws to even the largest technology companies. Over the last several years, the tech industry has led the way in reaching out to security researchers and providing them with rewards for responsibly reporting security flaws. A future in which all critical industries feel that they are able and incentivized to accept—and perhaps pay for—responsibly reported security issues is a much better future for our national cybersecurity.
4. **We need to build a pipeline of talent to improve our future.** At Facebook we have experimented with many techniques to attract young, diverse talent to the security field, starting as early as middle school. Our efforts are beginning to bear fruit with full-time hires resulting from our high-school and college programs, and we feel that a nationwide investment in cybersecurity education is critical to solving our longer-term problems.

I appreciate the opportunity to discuss these and other topics that may be useful to the Commission.

Thomas Andriola

Good morning. Thank you for the opportunity to participate on this panel and describe the University of California's (UC) current strategies for managing cyber-risk, as well as to share a few opportunities we see for securing the digital economy through stronger collaborations in cybersecurity.

Overview of UC

The University of California system – composed of ten campuses, five medical centers, and affiliations with three national laboratories – is a global leader in education, research, health care, public service, and innovation. We have more than 238,000 students, 190,000 faculty and staff, and 1.7 million alumni living and working around the world. We offer 150 academic disciplines, 600 graduate degree programs, and have produced 61 Nobel laureates.

Many of California's leading industries grew from UC research, including biotechnology, computing, semiconductors, telecommunications, and agriculture. We have 12,559 active patents, with 840 startups founded to date on UC patents. As the nation's largest recipient of federal funding for academic research, we secure $7 in federal and private dollars for every $1 in research funding provided by the state of California. And UC helps drive California's economy, generating over $46 billion in annual economic activity for the state.

The Open Research Environment

Innovation is the hallmark of any research university, and for UC, innovation defines both our past and our future. We steadily protect the core values of an open environment that we believe fuels innovation – academic freedom, the exchange of ideas, and collaboration among researchers and institutions all over the world. We are committed to maintaining this open environment not only to advance research and scholarship, but also because it serves and ultimately benefits society at large – from patients receiving the latest treatments, to farmers getting new tools to increase their yields, to private citizens breathing cleaner air. Our education, research, health care, and public service mission requires that we balance our responsibility to manage security and protect data with the need to foster a collaborative, innovative academic and research environment.

It is, though, a significant challenge. While maintaining this open environment, we have to comply with state and federal privacy regulations; we must protect our intellectual property, the foundation for our ability to help solve the world's problems; and we must adapt to their ever-changing threats that exist in today's connected world.

Our approach, therefore, is to continually prioritize risk and implement strategies across five key areas, recognizing that our needs and focus must change as the digital world evolves:

- **Governance**. We have convened a cybersecurity governance committee that includes representation from all UC locations and includes executive leaders in academia, administration, faculty, and technology. It is critical in the university culture to engage these voices in the conversations and decisions about managing security, privacy, and the open research environment.

- **Risk Management**. We have implemented a cyber-risk management approach that is based on international standards and strives for consistent methods of assessing and measuring risk across the multiple units and locations that comprise UC.

- **Modernizing Technology**. We are now leveraging our unique nature, size, and scale to bring state-of-the art technology to our locations. Higher education is one of the last industries to fully move to digital business, and until now we had not consistently been taking advantage of the latest technologies and services.

- **Developing Common Solutions**. We are adopting approaches that enable us to collaborate and more strategically work together as a single entity, rather than operating as individual campuses. Coordination translates to better protection. For example, we now can detect the same attacker profiles at multiple locations, and share warnings and strategies in timeframes much more quickly than in the past.

- **Culture Change**. We are fostering a culture where everyone is aware of their cybersecurity responsibilities. Our greatest risk comes from people not understanding today's threat environment or how to reduce risk. We have implemented training for all faculty and staff, advanced training for information security personnel, and teamed up with partners to improve our cyber awareness.

New Directions

Given the rapidly changing threat landscape and the reality that resources will always be limited, UC welcomes greater collaboration across sectors as the best means to manage cyber-risk more effectively.

- Information Sharing. Of particular importance is increased intelligence sharing to detect and respond to threats. Certainly a level of sharing occurs today, but impediments to effective communication also exist: Stale information, duplicative alerting, and classification tiers for receiving alerts may delay detection and response; not everyone is in the "circle of trust" who should be. Thus, collaborative arrangements among agencies and institutions should be developed to enable the timely, accurate sharing of threat intelligence.
- Solutions Creation. Collaboration not only enhances our ability to respond to threats but, perhaps more importantly, provides avenues to new solutions. Universities have access to some of the brightest minds in the field and adjacent fields which could add value into the cyber challenge. An example is this very Center for Long-Term Cybersecurity at UC Berkeley. Government and the private sector need to take advantage of this. Greater public-private partnership is needed to enable universities to launch joint research ventures for developing the strategies and tools to combat threats.
- Workforce Development. The current scarcity of cybersecurity professionals in the market, including the high salaries these professionals command, compounds the challenges for public and private organizations alike. By 2019, a global shortage of 2 million cybersecurity professionals is expected, according to ISACA (formerly called the Information Systems Audit and Control Association). Programs should be established to mobilize our universities to assist in the development of the cybersecurity workforce. The environment of advanced research & workforce development working hand-in-hand is essential to staying ahead of bad actors.

For UC, managing cyber-risk is simply the new norm. We supported California through its agrarian, industrial, and information periods. We continue to evolve and support it in the digital age. Cyber-risk is here for the long haul. It is a long-term game. We will continually revise and refine our approaches as threats and technologies evolve. But our best, long-term strategy will always be to work together – across universities, governmental agencies, and the private sector.

Dr. Cynthia Dwork

I will talk about Differential Privacy, a definition of privacy, and a collection of supporting algorithmic techniques, tailored for privacy-preserving statistical analysis of large datasets.

I will begin with an example of the kind of problem the concept was designed to address, called a "differencing attack." Suppose a data analyst is told the number of Microsoft employees with the sickle cell trait, that is, one gene for sickle cell disease. This quantity "feels" non-disclosive, and seems safe to release. Let's say the answer is 298 (this number is made up). If the analyst also obtains the exact number of Microsoft employees – other than distinguished scientists with very curly hair – who have the sickle cell trait, then my sickle cell status can be deduced.

This is a special case of the *Fundamental Law of Information Recovery*: overly accurate estimates of too many statistics can completely destroy privacy. The differencing attack does not involve "tracing a value back to the owner" or "de-anonymizing" data. The notion of "personally identifiable information" does not arise. The attack works because statistics combine in unfortunate ways.

Differential privacy is a promise that an individual data contributor will not be affected, adversely or otherwise, by allowing her data to be used in any study or analysis, no matter what other studies, data sets, or information sources, are available. At their best, differentially private algorithms can make confidential data widely available for accurate data analysis, without resorting to data clean rooms, data usage agreements, data protection plans, or restricted views. Nonetheless, data utility will eventually be consumed: the Fundamental Law of Information Recovery can no more be circumvented than can the laws of physics. The goal of algorithmic research on differential privacy is to postpone this inevitability as long as possible.

Differential privacy is the only known approach to privacy-preserving data analysis that can measure and control privacy loss accumulating over multiple analyses (as in the differencing attack above) and participation in multiple datasets. This signal capability makes it possible to "program" in a differentially private fashion. In ordinary, non-private computation, anything computable can be computed using only addition and multiplication, but this is not how programmers work. Algorithm design is the creative combining of appropriate computational primitives to carry out a sophisticated computational task, while minimizing the consumption of key resources, such as time and space. Similarly, differentially private algorithm design is the creative combining of simple differentially private primitives to perform a sophisticated analytical task, while also minimizing privacy loss and inaccuracy, in addition to the usual resources. As a rule, the inaccuracy is independent of the size of the database, so, speaking intuitively, when the dataset is large the signal dominates the noise; when the dataset is small this is not the case. This is precisely what we desire; think of the case of a dataset of size one: to ensure privacy the noise *must* drown the signal.

Differential privacy is the *wrong* technique for finding a needle in a haystack, searching out the terrorist. Designed to preserve the privacy of everybody – even the needles – the goal is to solicit participation, without fear of repercussion, for a public good, such as learning that smoking causes cancer, and other facts of life. Indeed, it is often the outliers who most need protection.

There are two popularly studied modes of operation. In the "local" model, differential privacy is applied to the data themselves, generalizing a 1965 technique, randomized response, used in the social sciences to study the prevalence of embarrassing or illegal behaviors. In the consumer setting this is described as "pushing the trust boundary out to the client." The "trusted center," or simply "centralized," model is exemplified by a federal statistical agency, such as the census. Here, raw data are collected and differential privacy is used to create summary statistics, synthetic data, histograms, etc., and to respond to specific statistical queries.

Differential privacy adopts a traditional cybersecurity mindset: adversarial "data analysts" are assumed to be sophisticated cyber actors, with access to large troves of side information easily accessed in a networked world – perhaps owned by the very companies or government agencies that employ the adversary – and that can be brought to bear to exploit vulnerabilities in a privacy-protective information system.

Google uses differential privacy in the local model to identify dangerous websites that are popular among the users of Chrome. At the 2016 Apple World Wide Developers Conference, Apple announced the deployment of differential privacy, again in the local model, in iOS 10 for a variety of data analytics, such as learning new terms for QuickType suggestions. The common factor in these two examples – one for cybersecurity and the other for a competitive user experience – is compliance with a strong non-technical privacy promise via adherence to a rigorous mathematical guarantee.

The US Census Bureau uses a variant of differential privacy in the centralized model in its OnTheMap website to provide statistics about where people work and where workers live. Projects and prototypes for other centralized model systems are under construction in several places, including the Privacy Tools for Sharing Research Data project at Harvard and a pilot reporting system for aggregated smartgrid data as an approach to compliance with a ruling of the California Public Utilities Commission (a joint effort between Microsoft and a California power company).

Differential privacy can have applications in the context of finding “bad actors” or “patients zero”. First, it can provide the means for learning “normal” or “typical” behavioral patterns, in a privacy-preserving fashion. In other words, it can be used to *define* the needles by contrasting them with “normal”. Second, the concept can be modified to distinguish between parties for whom privacy is explicitly protected, and a targeted subgroup for whom it is not. (This direction has been raised in a 2010 patent and a 2016 PNAS paper, but has not yet been widely studied.)

Originally designed with applications in mind such as traditional census uses, privacy-preserving early detection of epidemics from over-the-counter drug purchases, and discovery of systematic racial discrimination in home lending reports, differential privacy has also been suggested by the Defense Manpower Data Center (the central repository of Department of Defense (DoD) Human Resource Information), to enlist non-traditional data sources such as social media data to obtain insights relevant to improving personnel readiness and retention.

I close with three policy recommendations. First, *Publish Your Epsilons*. Differentially private algorithms are equipped with a privacy parameter, usually called epsilon, specifying an upper limit on permitted privacy loss in the execution of the algorithm. Algorithms that do not satisfy differential privacy have a bound of ∞ (infinity). By maintaining a registry of privacy loss, akin to a toxic release registry, we provide a path to determining the human value of the mathematical measurement, just we have learned the human value of a fixed unit of time; we stimulate competition to obtain better analyses at lower privacy costs; and we engage those who traffic in the data of individuals in the effort to protect their privacy.

Second, *Establish and Maintain a list of approved private data analysis techniques and appropriate applications*. To remain current, to evolve toward being comprehensive, to accommodate contexts that were not previously anticipated, and to take into account new developments in the scientific community’s constantly evolving understanding of data privacy risks and countermeasures (which may lead to either additions or deletions from the list), the list should be maintained by a periodically convened task force including data privacy experts from computer science, statistics, and law, as well as ethicists, members of Institutional Review Boards, and researchers who do various kinds of human-subjects research.

Third, *Consider Restraint*. In a data-rich world, the challenges revolve around the trade-off between what can be done and acceptance of the fundamental truth that overly accurate estimates of too many statistics can destroy privacy. If we are interested in privacy, sometimes restraint might be the right approach.

Eric Grosse

Good morning Chairman Donilon and members of the Commission on Enhancing National Cybersecurity. I appreciate the opportunity to participate in this discussion regarding collaboration models for addressing cybersecurity challenges.

My name is Eric Grosse and I am a Vice President Security Engineering at Google. Over the past decade I built up the core team of over 500 people in security and privacy at Google. Our work includes expanding the use of network encryption, strengthening consumer authentication technology, detection and blocking of foreign espionage, transparency on government requests for data, sophisticated malware analysis, and creating tools and frameworks for safer building of web applications. Recently, I have stepped down from overseeing the entire security team, and have returned to day-to-day security engineering work.

Today I would like to talk about two themes that undergird important advances in securing the digital economy: collaboration and transparency.

<u>Collaboration and the Digital Economy</u>

A safe Internet is essential not just for any one company, but for everyone who connects to it. When I first began working on security research, networks were often relatively small, and comprised trusted entities. Now we see over three million new smartphones coming online each day, and the picture of who is connected to whom is rapidly evolving. And so are the threats.

At Google, while we believe that it is important to keep our own users and systems secure, we also use our resources to collaborate with others in ways that we hope can help all of the Internet's users. I will discuss two important collaborations here.

Vulnerability Reporting: Google has for years helped to lead discussion and progress in the practice of vulnerability reporting and disclosure. Online security is a difficult task and as the people looking to exploit vulnerabilities become more sophisticated, the defenses must keep pace. We take very seriously the idea that vulnerabilities should be reported promptly to the impacted entities so that the problems can also be addressed promptly. We have spent significant sums in money and human resources to encourage this.

Of course our focus is not limited to our code and products. In 2014, a team at Google created Project Zero, which looks at the software and systems that we use everyday, not just our own. When the Project Zero researchers discover a vulnerability, they do the responsible thing and inform the people who maintain the impacted technology, so they can fix it. While we have found and reported vulnerabilities to many different companies (some of them well known), this work is especially useful when it comes to the open source projects that are essential for the Internet, and which are maintained by just a few dedicated people.

Governments, of course, also have researchers that uncover vulnerabilities and in the US there is a process through which these vulnerabilities are reviewed and recommendations are made on how to handle them. At the beginning of 2014—after a review and comment process—the President's Review Group on Intelligence and Communications Technologies pledged that the government would rebalance its assessment toward favoring disclosure of zero-day vulnerabilities to vendors. The President repeated this pledge, noting exceptions for national security and law enforcement.

I have been watching and trying to understand how the new policy compares with the comparable Google-related efforts I just described. I wish it were easier to assess. Collaboration requires an accumulation of trust over time, and the government is missing an opportunity here. As an example of the sort of thing I admire, in the early days of Android, NSA's Information Assurance Directorate shared with us important vulnerability findings, which we fixed. The government should say more about how much of this zero-day reporting it does.

Threat Sharing. Reporting zero-day vulnerabilities to the software author is simple compared to the challenges of sharing threat signals, another hot area of interest in public/private cooperation. It may be helpful to mention one method I've observed work well. Google participates in a Bay Area CSO Council that has a working group of a dozen or so companies that share threat signals. We're pretty good these days at detection of threats and attribution. In this group we're comfortable sharing at the incident responder level with a few other trustworthy individuals. However sharing at a wider scale would not be productive, as leaks render the information useless as adversaries can leverage it to hide better. Threat sharing is challenging.

Transparency and the Digital Economy

In addition to collaboration, transparency is an important element of successful collaboration for security and it exists in many forms. To take one example, some of the foundational code that underpins the current state-of-the-art for encryption is open source code, meaning anyone who wants can examine the code and take comfort in knowing how it operates. This transparency is precisely what has helped to make some of these popular standards so ubiquitous.

Of course it's not only open source code in our, or any major company's, systems. But the larger point gives an important insight into how transparency helps with the work we do. Opening up details—whether it's code or other information—so they can be seen and understood by others can be a useful and powerful tool.

To illustrate further, I'll share three examples that show some of the ways transparency operates across the Internet's different constituencies, from end users to other companies, researchers, and government actors.

Android Permissions Model. First, at a base level, when assessing the security of a system, it is useful to know who has access to the system and to have control over the various access points. With this knowledge and control it is easier to audit or understand the scope of access. Processes like our updated Android Permissions model and the corresponding model in iOS let users see when an application is asking for permission to obtain specific kinds of data from their device or account and they can grant (or limit) that permission.

Certificate Transparency. Second, we have also helped to pioneer an open framework for monitoring and auditing TLS certificates in nearly real time. Certificate Transparency makes it possible to detect TLS certificates that have been mistakenly issued by a certificate authority or maliciously acquired from an otherwise unimpeachable certificate authority. End users may not be interested in directly reviewing this information themselves, but it is valuable for domain owners, certificate authorities, and browser manufacturers, all of whom have a vested interest in maintaining the health and integrity of the TLS certificate system.

Transparency Report. Finally, beginning in 2010, Google launched the Transparency Report, which in its first instantiation provided details about requests to access or remove data on our services. The Transparency Report has since grown.

While the Report doesn't work against malware or vulnerabilities in quite the same way that other code disclosures or reporting do, it is an important force that has helped us and others to speak more openly about security and data integrity on the Internet. The discourse enabled by this data has also allowed some additional transparency around requests made under the Foreign Intelligence Surveillance Act and National Security Letters. There is still a long way to go, but information like what you find in the Transparency Report from Google—and increasingly more and more companies—can lead to better Internet policies because we can see how laws play out on the ground.

In this vein, Google also has worked to be able to tell particular users when the government has made requests for their data. There are times when we are gagged from doing so, and in some cases it's easy to understand why. But systemic, indiscriminate and perpetual use of gag orders is corrosive of trust over time. Providers should be silenced from telling users about requests only when there is truly a need to do so, and not forever. The government too should be more transparent with those users. In the long run, this will bring greater legitimacy to the laws and confidence in the system.

Conclusion

The principles of collaboration and transparency have evolved over time while their importance as tools in our work to secure the Internet has grown. I appreciate this Commission's work to investigate this topic as I think understanding the complex ways these themes operate across many sectors—with varying degrees of modern and legacy systems to secure—is essential to approaching the tasks you have set out to address.

I would be happy to answer questions if you have any.

Eli Sugarman

I. Introduction

Thank you for inviting me today to address the Commission on Enhancing National Cybersecurity. It's a privilege to do so, especially on the campus of UC Berkeley, a long-standing partner of the Hewlett Foundation. Our Cyber Initiative, which I manage, made a $15 million grant in 2014 to establish the university's Center for Long-Term Cybersecurity (CLTC) – the host of today's meeting. CLTC's innovative approach to cybersecurity research and education is helping to build a more capable and interdisciplinary cybersecurity policy field.

I will focus my remarks on the role of philanthropy supporting collaboration among government, the private sector, and civil society to address cybersecurity challenges. Before doing so, a few words of context: The William and Flora Hewlett Foundation is a private charitable foundation headquartered across the bay in Menlo Park. It was established 50 years ago to serve the public interest, and since that time has made more than $5.5 billion in grants on issues ranging from education to the environment to cybersecurity. We address complex public policy problems with long-term, strategic grantmaking approaches.[1] The foundation has a long-standing interest in national security, including prior initiatives focused on conflict prevention and nuclear security.

Two years ago, we launched the Cyber Initiative, a 5-year $65 million effort to cultivate a field that develops thoughtful, multidisciplinary solutions to complex cyber policy challenges. We make grants focused around five core objectives:

- Building the capacity of civil society organizations;
- Building the capacity of decision-makers and influencers;
- Building a robust network of experts;
- Generating policy-driven research and thought leadership; and,
- Catalyzing additional funding.

The Hewlett Foundation is a non-partisan funder with a diverse set of grantees – including think tanks representing a range of political and ideological perspectives and research universities such as UC Berkeley. We strive to support a more informed, inclusive, and open conversation about cybersecurity policy issues. We purposely fund grantees with different viewpoints who disagree with one another in service to building a true marketplace of ideas on cybersecurity. We pursue this approach because, while we seek better policy outcomes, we're agnostic as to what they are. We're also interested in helping to bridge key trust deficits in the field, like those between Washington and Silicon Valley, or between those who view cyber policy primarily through the lens of national security and those for whom privacy and civil rights are paramount, to take just two examples.

We believe that our Cyber Initiative has an important role to play, but cannot succeed by itself. We are trying to show other private foundations what can be done while encouraging other funders, including government and industry, to widen their focus.

II. The Cybersecurity Challenge

Decision-makers in and out of government are struggling to make informed and sophisticated decisions about cyber policy and security matters in part because of long-trusted Industrial Age norms and laws that may be ill-suited for an information era. They are uncertain about the nature of the key problems; how to properly balance competing values, such as national security and civil liberties; or

[1] In accordance with limitations imposed by federal law, the Hewlett Foundation does not engage in lobbying or earmark its funds for lobbying activities. The foundation's funding for policy work is limited to permissible forms of support only, such as general operating support grants that grantees can allocate at their discretion and project support grants for non-lobbying activities (e.g., public education and nonpartisan research).

grasp the long-term impacts or tradeoffs embodied in their decisions. In crucial respects the field is still embryonic: too underdeveloped to provide the information, policy frameworks, venues for dialogue, and leadership required to drive more effective policy decisions and strategies.

In the meantime, global Internet traffic continues its explosive growth, as does the number of Internet-connected devices and sensors (the "Internet of Things"). Digital technologies promise greater access to information, increased efficiency and economic growth, opportunities for creativity and expression, and new forms of social interaction. Balanced against this progress, we know that there can be a variety of unintended, often negative, societal implications associated with new technologies and complex systems.

People need to be able to count on the digital tools of their everyday lives even though every new Internet user and/or device is another potential vector for malicious actors to exploit. They need trustworthy devices and systems that function as expected. Disruptions to such trustworthiness—whether due to the purposeful actions of an adversary or an unexpected, emergent property of a complex system—could give rise to serious threats to national security, commerce, societies and individuals alike. The decisions policymakers make about how to manage these risks, moreover, will likely have enormous consequences for the public interest, privacy and civil liberties, the economy, and international relations in the future.

Our views are premised on the firm belief that technology alone cannot protect us from cybersecurity threats. As the controversy over encryption illustrates all too clearly, we need smart policy to frame critical choices and manage the institutions, networks, and behaviors that operate in cyberspace. Such policy frameworks do more than help to resolve the crises of the moment: they set a path that shapes future decisions and events. They must, as such, be formed with the future, as well as the present, in mind. It is dangerous to build a road without a clear idea of where you want to go.

Yet funding to develop long-term cybersecurity policy for the benefit of the broad public is practically non-existent. Private companies underwrite cybersecurity efforts focused on their own commercial interests and the defense of their own networks, while public funding from the Department of Homeland Security, the National Science Foundation, the Defense Advanced Research Projects Agency, and other government sources focuses almost entirely on technical cybersecurity research and education.

Philanthropic institutions can help to fill this gap. They are neutral players without a direct interest in the outcomes of debates about cyber policy, with flexible resources and the latitude to take a long-term, strategic approach to the issue. But they need to be activated. Among foundations and other donors, there is presently little appreciation for the pivotal role philanthropy can play and even less understanding of why it is needed. This Commission is uniquely positioned to call upon foundations and individual donors to step in. Engaging philanthropy is a low-cost but potentially effective way to unlock new funds, create much-needed policy frameworks, and develop a pipeline of experts to support cybersecurity both in the United States and globally.

III. The Potential of Philanthropy

Despite the urgent need for cybersecurity policy work, the universities, think tanks, civil society organizations, and other institutions most capable of doing it receive paltry support for the purpose. One might normally look to the national government to fill this funding gap. But even apart from the difficulty of generating new resources through congressional appropriations, the US government is ill suited to step in for at least two reasons. First, the government is (as it should be) principally focused on day-to-day cybersecurity imperatives, as opposed to long-term frameworks. Senior officials who want to take a more long-term, strategic approach oftentimes cannot do so, given the pressing demands of their positions and the need to extinguish recurrent cybersecurity "fires."

Second, the government faces a trust deficit with critical players whose participation is essential, as well as with segments of the American public and international community. This lack of trust makes it difficult to get full participation and buy-in from the technology community and other stakeholders. The credibility of policy frameworks developed exclusively with government funding could also be called into question, potentially undermining the impact of such frameworks.

Companies, meanwhile, are mostly animated by commercial imperatives and short-term profits, not maximizing societal benefit over the long term. Not surprisingly, private sector funding focuses on developing new technologies and products and protecting immediate interests. The policy-oriented funding that the business community provides thus tends to be modest and focused on serving the government relations goals of individual companies.

Internet and technology entrepreneurs are, unfortunately, largely absent from the funding landscape. In an earlier era, individuals like Andrew Carnegie and John D. Rockefeller dedicated significant funds to help American society adapt to the industrialization that provided the basis for their fortunes. Today, very few if any leading Internet innovators or individual philanthropists are funding efforts to help American society understand and adapt to the security environment produced by the technologies they created and from which they profited.

Further, at many critical points throughout the United States' history, philanthropies have stepped in and provided critical resources to shore up the country's national security. For example, Alfred Lee Loomis funded groundbreaking research into radar detection systems and helped the U.S. government deploy them during World War II. He overcame bureaucratic obstacles to deliver a critical military capability.

The upshot is an alarming gap in our ability to deal with cybersecurity risks—a gap whose importance and peril will grow over time. There is work that must be done, and soon: work the government cannot fund and the private sector will not fund. It is here that philanthropy can make a difference.

Many foundations acknowledge the importance of cybersecurity and have expressed a desire to engage. But most shy away, uncertain what they have to contribute to a problem this complex and difficult. A handful of large foundations have dipped their toes into the water, but largely to support open Internet and human rights-focused advocacy and research. Other foundations dedicate a portion of their more modest resources to studying national security dimensions of cybersecurity. The Hewlett Foundation's Cyber Initiative is the largest foundation effort to create long-term cybersecurity policy frameworks and educate well-rounded experts to apply them. Even taking all this together, it is far too little. Funding at the level of an order or magnitude larger (or more) is needed.

IV. Suggestions for the Commission

The Commission is uniquely positioned to engage funders, focus attention on the importance cyber policy issues, and catalyze an even more informed cybersecurity policy debate. Its mandate allows it to take a strategic, long-term perspective that typically eludes government. I encourage the Commission to consider the following ideas for its future work as well as its final report. The Commission should consider encouraging the U.S. government:

- Via the National Science Foundation and/or other grant-making/research institutions – to fund multidisciplinary cybersecurity policy research (drawing upon both technical and social sciences disciplines) by universities, think-tanks, and other non-profit organizations;
- To engage philanthropic funders by: (i) sharing information about the high stakes involved in cybersecurity; (ii) exchanging views on key cybersecurity policy topics; and, (iii) identifying opportunities for collaboration, including funding of cybersecurity policy efforts;
- Especially the intelligence and law enforcement communities, to be more transparent and open about key dimensions of cybersecurity, thereby informing the public debate with facts and data and encouraging new voices to participate; and,

- To partner with civil society organizations and other stakeholders to pursue creative ways to build trust, recognizing that the U.S. government cannot do so alone and needs the advice, support, and relationships with other stakeholders to arrive at optimal policy outcomes.

Gilman Louie

The United States needs to treat the Internet as a global resource and thus cyber security as a common interest for all responsible nation states. The United States needs to continue to engage with other countries in both bilaterally and multilaterally discussions. We cannot view Cyber Security as a domestic issue. We must work with other nation states and discourage a Balkanizing of the Internet. While each country has their own views as to what they need to have a safe and secure internet, we need to find common ground as it relates to critical infrastructure, financial transactions, commerce, criminal activities, intellectual and digital property, data, IoT and safety. The US must take a global leadership position in protecting this critical resource. The State Department, Commerce and FCC have major roles to play on cyber security.

Cyber security is not just a security issue, it's also a quality of service issue. Cyber threats and the need for ever increasing cyber security measures at each layer of the internet, reduces performance, reliability and trust while increasing cost, complexity, and vulnerability. The lack of trust and security leaves each institution, corporation, and citizen on their own. The lack of a secure Internet, materially negatively affects global productivity, trade, innovation, performance, trust and safety.

While law enforcement, intelligence and military have roles to play, a non-law enforcement, non-military, non-intelligence, trusted agency needs to be the principal federal agency in charge. While there are great expertise and capabilities within the DHS, NSA and FBI, they are not appropriate lead agencies if we believe that cyber security is a global issue and that the Internet is a global resource. The current construct is not trusted globally and it is seen as adversarial by many in Industry. We need to find other solutions that involve our international partners and create public-private partnerships.

Cyber security requires information sharing between industry and governments. We must lower the barriers that inhibit information sharing and we need to develop solutions that allow threat sharing to be done at Internet speed. Industry needs to be viewed not only as a user of threat data and intelligence, but as an important source of threat data and intelligence. For many, Industry is the primary target of bad actors, which means that Industry is an important provider of threat intel. Unless we provide incentives, safe harbors and infrastructure for Industry to share, we will continue to have an incomplete awareness of the threats. It is difficult for Industry to share with federal agencies that can prosecute or have the mission to penetrate information security networks. It is also difficult for global companies, which almost all Internet companies are, to legally be required to share with one nation state while legally ignoring the legal requirements of another.

The National Commission for Review of the Research and Development Programs of the United States Intelligence Community (2013) published a special topic white paper entitled: The IC's Role within U.S. Cyber R&D. This paper pointed out the need for a new approach for U.S. cyber R&D. It outlined three guiding principals for US cyber R&D Investments:

1) Cyber R&D must be informed by full threat and vulnerability assessments.
2) A Cyber R&D framework must respect privacy and civil liberties.
3) Cyber R&D must be informed by information exchange.

It made the following recommendations:

1) Establish a national Cyber R&D agenda.
2) Determine what Cyber R&D is being done.
3) Examine and evaluate approaches to public-private partnerships for Cyber R&D.

The 2016 Federal Cybersecurity Research and Development Strategic Plan listed five recommendations:

1) Prioritize basic and long-term research in Federal Cybersecurity R&D.

2) Lower barriers and strengthen incentives for public and private organizations that would broaden participation in Cybersecurity R&D.
3) Assess barriers and identify incentives that could accelerate the transition of evidence-validated effective and efficient Cybersecurity research results into adopted technologies, especially for emerging technologies and threats.
4) Expand the diversity of expertise in the Cybersecurity research community.
5) Expand diversity in the Cybersecurity workforce.

These reports as well as many others have made similar actionable recommendations for Federal Cyber R&D but progress has been slow, uncoordinated, and underfunded. We need the cooperation of both academia and industry. It is academia that develops the talent and research and industry that develops and sells the solutions. We need leadership and organization to execute a national R&D strategy.

The United States created the Internet. Our country is a global leader in making the Internet a global communications and information platform. Everyday, with new innovations, products and services, the world increases its dependency on the Internet. The United States must continue to be the leader in keeping the Internet open, safe and secure with a global, not just with a domestic, policy.

Mark McLaughlin

Good afternoon. My name is Mark McLaughlin. I'd like to thank Chair Donilon, Vice Chair Palmisano and the Commission for the opportunity to speak to you today about innovation and collaboration for the future of the digital economy.

Drawing on my experience as chairman, president and CEO of Palo Alto Networks, and as chairman of the President's National Security Telecommunications Advisory Committee (NSTAC), I'd like to talk about how I believe innovation is essential to reversing the current dynamic in cyberspace, where increasingly automated adversaries are dramatically outpacing manual defense. Innovation must be thought about holistically because, as this Commission understands well, innovation in isolation is meaningless. If we want to regain leverage against our adversaries and reverse the unsustainable, current dynamic, we must ensure that innovative technologies operate together in an automated fashion, within a broader cybersecurity ecosystem, coupled with educated people and refined processes.

Let me start by applauding the Commission's focus on innovation and collaboration and your effort to come to Silicon Valley for this critical conversation. This workshop represents just the latest example of a sustained effort that began with last year's White House Summit on Cybersecurity and Consumer Protection and which recognizes the importance of an enhanced partnership between the U.S. government and private industry in addressing these existential cybersecurity challenges.

As this Commission continues to tackle difficult cybersecurity questions, I am confident that the work of the NSTAC can serve as a valuable resource to inform your upcoming report. Drawing on the expertise of 30 presidentially appointed senior executives from private industry, who advise the President on national security, emergency preparedness, and communications issues, the NSTAC has an important mission that complements the broader cybersecurity charter of this Commission. Just last month, the NSTAC, which has existed for 30 years, hosted its first-ever meeting in Silicon Valley with tremendous engagement from senior U.S. government officials, including three Cabinet secretaries. That meeting focused on exploring potential ways for Silicon Valley to contribute expertise to specific national security issues. For example, in recent years at the direction of the White House, the NSTAC has produced reports with recommendations on the national security implications of such issues as emerging technologies, big data analytics, IT mobilization, and the internet of things (IoT).

Let me step back from the NSTAC work, and speak more generally about the cyberthreat landscape, addressing how I believe we can collaboratively innovate to restore the trust in our digital age that comes into question with each successive cyber breach and attack. As this Commission knows well, these increasingly frequent and sophisticated cyber incidents are leading many to question whether the technological foundation on which we are building our future of smart homes, self-driving cars, and the new global, digital economy may have deeper structural flaws.

This is not hyperbole. More and more, we live in a digital age in which the fundamental elements of the economy—from retail transactions to the operation of the financial system to the generation and transmission of electricity – are increasingly interconnected via the internet or only exist as bits and bytes. This digital age brings with it incredible efficiencies and productivity, but it also brings new challenges and potential vulnerabilities—and business, government and military leaders know that there is a very fine line separating the smoothly functioning digital society built on trust and the chaotic breakdown in society that would result from the erosion of that trust.

I believe at the heart of this cybersecurity battle is a math problem—one that's relatively simple to understand but challenging to correct. Unfortunately, today, this math problem overwhelmingly favors our adversaries. Here's why: The cost of computing power required for malicious actors to launch successful cyberattacks has been decreasing dramatically for decades. Coupled with the widespread availability of black market malware and exploits, our adversaries are able to conduct increasingly automated, successful attacks at little to no cost.

In the face of this automated onslaught, the network defender is generally relying on decades- old security technologies, often cobbled together as multiple layers of point products that are not designed to communicate with each other. This lack of automation and interoperability has become increasingly problematic as networks grow in complexity due to macro technology trends like the adoption of virtualization, software as a service (SaaS) technologies, cloud computing, mobility, and the internet of things. This increased complexity of enterprise architecture and independent security controls creates a dependence on one of the least scalable resources organizations have—people—to manually fight automated, machine- generated attacks. As defenders, we are simply losing the economics of the cybersecurity problem.

This daunting threat environment has led many to conclude that cyberthreat prevention or protection is impossible, and we must simply focus on detecting and responding to intrusions after the compromise has occurred. But this perspective is fundamentally flawed. If our only response is to clean up after compromises have occurred, then attackers will continue to win. No executive, whether a Cabinet official or a CEO, should simply strive to report promptly that their organization's sensitive employee or customer data—or intellectual property—has been stolen by a cyber criminal. And as cyberattacks become increasingly destructive, and the potential for physical damage to industrial control systems and hardware proliferates, it becomes clear that only by persistently driving for better prevention can organizations avoid these untenable scenarios.

So how do we prevent successful attacks and restore the digital trust we all require for our global economy? First, because cybersecurity is an inherently distributed problem, I think it's critical that we approach this question with a shared lexicon. Under the direction of President Obama's Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," the National Institute of Standards and Technology (NIST) commendably led a process that brought together public and private sector experts to establish this collaborative baseline of cybersecurity priorities and best practices. The resulting Cybersecurity Framework featured five core functions governing how organizations can manage and reduce their cyber risk: Identify, Protect, Detect, Respond and Recover. While all five functions enhance security, focus on effective identification and protection, in particular, is critical for actually preventing successful attacks, limiting an organization's need to focus on the ways in which it must detect, respond and recover after a compromise has already occurred.

Innovative approaches—effectively applied to people, process and technology—can be one of the key principles in achieving prevention, establishing security as the default and regaining leverage against our adversaries. But before I detail the innovation imperatives behind achieving prevention, let me first clarify what I mean by prevention. Prevention is about significantly decreasing the likelihood, and increasing the cost required, for an attacker to perform a successful attack. We should not assume that attacks are going away or that all attacks can be stopped. However, we should assume, and be very diligent in ensuring, that the cost of a successful attack can be dramatically increased to the point where the likelihood of a successful attack declines. This is the outcome we should strive for—not to eliminate all risk, but to reduce and compartmentalize the risk to something acceptable and understood.

If we are going to maintain the trust in our digital infrastructure and restore what has been lost, we must focus on regaining leverage from attackers by making it more expensive in terms of resources, time and personal impact to launch a successful attack. This leverage can be built on a few categories of innovation principles. As this Commission focuses on innovation as a means to enhance cybersecurity, I recommend establishing a clear definition of what constitutes an innovator, applied to the following categories:

- Technology: Innovators must develop technologies that work together seamlessly to enhance the security of individuals, enterprises, and the broader ecosystem. In other words, cybersecurity innovation in isolation is inherently less effective because a single technology built to solve one discrete problem does not solve the job of a network defender.

Simplification and automation are essential for making networks adequately defensible. Security technologies must be leveraged as part of natively integrated platforms, capable of automatic reprogramming based on new threat information, to prevent threats across all points of the attack lifecycle—on the network, in the cloud, and at the endpoint. This capability to deploy preventive countermeasures automatically must be consistent regardless of where data resides, or the deployment model of the network, whether on premises, in the cloud, or stored in third-party applications. By automating prevention technologies, we can dramatically reduce the workload on security personnel, allowing them to prioritize only the most significant incidents that are worthy of human intervention.

Innovators must also understand that security technologies need to be fully integrated as part of a larger, global ecosystem. More specifically, innovators should work within this ecosystem to utilize information sharing, leverage open source integration APIs, and develop interoperable technologies capable of automated security—including through partnership with complementary technologies from third-party companies.

Integration should be embraced with an eye toward three primary objectives: 1) protect against all known cyberthreats, 2) turn unknown threats into known threats on a near- real-time basis, and 3) translate this new threat knowledge into preventive countermeasures and share them broadly within the ecosystem to protect against other organizations falling victim to the same or similar attacks.

- People and Process: Innovators must recognize that technology is irrelevant if we aren't educating people and executing process in the right way. We must double down on increasing cyber awareness and education for our employees, children and ourselves to reduce human vulnerabilities and ensure we are growing the next generation of cyber- savvy citizens.

  We need to start educating children at the earliest possible age so that cybersecurity is fundamental. We must ensure that hands-on training with innovative security technologies is ingrained in educational curriculum. And we must leverage innovative technologies, like those that enable long-distance virtualized learning, to educate more people, and faster.

  We all know there is a major shortage of qualified cybersecurity personnel. But if we build our workforce development plans on a foundation of automated technology, we can ensure that we are recruiting and training people in a more targeted way for only those jobs that require a human's sophistication and critical thinking. As our adversaries become increasingly automated, it is simply unscalable as a defense model to manually combat functions that could be more effectively addressed by automated technology.

The future technology space is uncertain in this Internet age. What is clear is that we can expect radical changes to our digital lives in the very near future. Technologies that are currently breaking new ground or just over the horizon—like big data analytics, quantum computing, artificial intelligence, virtual reality, a truly global Internet, digital money, and nanoscale computing—will shape our world in ways that we cannot possibly imagine. Defending that space seems daunting, but it does not have to be. Keeping in mind a few network defender design principles will help us navigate whatever digital security challenges may surface in the future.

Adopting these innovation principles across technology, people and process is a critical first step in changing the economics of the cybersecurity problem and achieving prevention. But fundamentally changing the current dynamic requires collective action across the cybersecurity ecosystem. With the combination of next-generation technology and our joint efforts, we can vastly reduce the number of successful cyberattacks and restore the trust we all require to preserve the promise of our digital age.

Ted Schlein

Chairman Donilon, Vice-Chairman Palmisano and Distinguished Members of the Commission, thank you for the opportunity to serve on this panel and to address critical security issues related to the digital economy. We appreciate the thought the Commission is putting into formulating its recommendations for the report to the President.

I'm Ted Schlein and while here today as a Managing Partner at Kleiner Perkins Caufield & Byers, the views I'm representing are my own based on over 30 years of working in the cyber- security industry as a commercial operator at Symantec, as an investor in many cyber security technology companies, and a cleared advisor to various US national security initiatives

It is my view that the management of technology risks, in particular cyber-security, has become critical to our increasingly digitized and connected society and economy. It is imperative for national and international security and will continue to be ever more a foundational requirement in other domains.

We as a country need to evolve our thinking and thus our policies to take into account that the digital domain is very different then the physical domain and therefore many of the laws we currently enforce are not applicable when applied to this new networked world.

I have 5 areas that I'd like to discuss with recommendations that I ask you to consider.

1. Measuring Corporate Cyber Risk
2. Changes in National Security Apparatus & the Need for Talent
3. The Role of Government Purchasing Power
4. Legal Landscape Around Breaches
5. Combatting Cyber Criminals

My first recommendations are in the area of measurement of corporate cyber risk. As we know in business if we don't measure a program or person, you never know how we are doing versus our goals.

- The country should consider creating a Risk Preparedness Index (RPI) that systematically measures the people, processes, policy and technology configurations by each critical infrastructure sector of our country. By using a NIST (National Institute of Standards and Technology) standard for each sector and creating an independent entity that issues these ratings, much like Standard and Poor's and Moody's does for bonds, we would assign every commercial company a RPI score. These would be publically available and the belief is that consumer awareness will drive the necessary behaviors by the corporate entities to increase their risk preparedness that is appropriate for their industry sector.
- Public companies are increasingly understanding, and thus forced to deal with their company's cyber posture. We should consider that companies in certain sectors, be required to have a security expert on their board much like we have financial experts as part of the Audit Committees. At least, a requirement that some subset of the board needs to be briefed on the company's security requirements and deficiencies on quarterly basis.
- Finally, I believe that it should be a requirement to report a security breach and the necessary information around that breach. Who any entity reports this information to and how it is handled I will cover in a future section.

Over the next decade, some of the most defining issues we will face as a nation are how we evolve our approach to dealing with cyber attacks in both the private and public sector. In order for us to properly execute in the event of an attack as well as to evolve policies in Congress in real-time, I would like to propose a series of changes that we make to our national security apparatus.

- We need to put in one place and under one management team the country's best and brightest security minds and technologists in order to effectively defend the country's interests. I would propose, removing US Cyber Command from the NSA and using it to create a combined US Cyber Command that includes FBI, DHS, and other military branch cyber assets and personnel into one unified command. This agency should be run by a Secretary of Cyber that reports to the Secretary of Defense with additional reporting to FBI and DHS. I realize that the authorities of these various entities are quite different and that will need to be addressed. We should create one campus for this new Agency and its purpose is to both defend and attack on behalf of the US. This agency would be at the disposal of DoD for offensive purposes, FBI for domestic law enforcement issues and DHS for the protection of private US industry, of course in the case where this has international implications these actions would need to be coordinated with DoD. It would be the main interface with our international allies on cyber issues, as I could see a CyberNATO forthcoming. We must recognize that in the world of cyber there are no borders. We should also encourage and make the security clearance process easier to enable private citizens to rotate thru this agency to establish a place where the best and brightest are able to shine on behalf of the nation. As we have huge amounts of talent not currently employed by the federal government, who could be very helpful to this cause if harnessed properly.
- By creating this Agency, we get our best talent working on our hardest issues over-layed with the appropriate laws for each group's actions. This will also be a great advisor to Congress about future policy changes that should be debated and decided. Because you will have defense and offense, national and international all represented in one place, you will get an actual representation what we deal with from a cyber security perspective as a country and also by private industry and how to update it in real-time circumstances.
- Like many, I believe that our best defense is going to be a good offense, the FBI and DHS sector of this group would be responsible for helping private industry fight back if needed, authorized and warranted. This would be the group that would be the recipient of the breach notifications by private industry and also be able to disseminate the appropriate information out to them as needed.
- Inherent in the ability for the above, is to continue to hone our ability to get better and better attribution for attacks against both the private and public sector. This will be a key ingredient for deterrence as well as for deciding on proportional response. It should also play a part in assisting victim companies in dealing with potential liabilities.
- Finally, as part of this initiative we should mobilize the higher level education system in the country to produce more cyber aware and trained graduates. In fact, we should put out the challenge that we want to create 50,000 new cyber security graduates per year. This means you cannot be a computer science graduate unless you understand secure coding. You cannot be a network design graduate unless you understand secure network design and architecture, etc. And in order to effect this the government will pay for any student who decides on the appropriate major in this area, as long as when they graduate they work for at least 4 years at this new Cyber Command. This way the government gets great new talent and we help train a workforce for the private sector that they will desperately need.

Lets face it, we have a dilution of expertise issue in the public sector, we have a trust issue with the private sector and we have rapidly expanding national and international security issues that require more forward thinking policy. We also have a talent shortage in both government and private sectors and this will only increase over time.

The next area I'd like to comment on the federal government using its purchasing power to effect change. The public sector is the largest buyer of technology in the country with the DoD being the single largest. This is a powerful tool and could used to promote safer computing.

- I would propose that the federal government not allow the purchase of third party technology by any of its agencies unless that commercial entity provides a detailed secure code audit report that adheres to NIST standards. This will drive commercial software vendors to fix security holes before providing that technology to the market, which will in term benefit all customers.
- Further, no internally developed software by a government agency will be allowed to be deploy if it has not undergone a secure code audit and is signed off by the appropriate level CISO.
- Finally, in this area, I think the federal acquisition rules around the purchasing and deployment of security technology should be reviewed for streamlining purposes so that our front line agencies are able to deploy state of the art capabilities at a pace that is relevant to the demands of cyber space and not the confines of the physical domain.

Another area of comments are around potential concern with the evolving legal landscape due to cyber security breaches. There are two main areas that I think bear mentioning.

- First, class action lawsuits aimed at a private enterprise for not being able to defend themselves against a cyber attack by a foreign nation state, are unrealistic. Most of our federal networks cannot defend themselves against similar attacks yet the financial burden as well as the public shaming that goes along with such a case, calls out for tort reform in this area to create a safe harbor in certain situations.
- Second, the FTC is currently chartered to be a consumer advocacy policeman of sorts. Having the power to investigate and extract large fines from private enterprises they deem not properly protecting consumer's privacy information. The Commission may not be the group that has the expertise to make these judgments nor would they be the ones to make a determination, but you do have the ability to speak to the undue burden placed on these small businesses – often privately held – by an ongoing FTC inquiry. These decisions should end up in a better prepared and equipped part of the federal apparatus.

My final area for comments are around combatting cyber criminals and thoughts on how the United States may be adjusting our thinking and approach toward curbing this ever increasing issue. At the core, being a cyber bad guy is just too good of a business model. One can wake up, not change from their pajamas, go into their living room and make a few million dollars by lunch time. It is a highly scalable business with great margins. We need to fundamentally change the economics of how good a business this is and we should do this with a mix of technology and policy changes.

- We need a call for international cooperation to combat ransom ware and cyber extortion. Any country that harbor these perpetrators needs to be called out and appropriate action taken against them, including trade sanctions.
- The penalties on an international level for those caught conducting these crimes needs to be severe and strictly enforced.

Commissioners, thank you for listening, and your time and dedication to this extremely important set of issues our country faces. I hope I've provided you with a few ideas that you find interesting and potentially useful as you finalize your recommendations. I look forward to answering any of your questions.