Commission on Enhancing National Cybersecurity

Established by Executive Order 13718,
Commission on Enhancing National Cybersecurity

University of California, Berkeley
International House
Chevron Auditorium
2299 Piedmont Avenue, Berkeley, CA

MEETING MINUTES

The Commission on Enhancing National Cybersecurity (Commission) was convened for its third public meeting at 9:10 a.m., Pacific Time on June 21, 2016 at the University of California, Berkeley, CA. The meeting in its entirety was open to the public. For a list of meeting participants, please see Annex A.

Welcome

Betsy Cooper, Executive Director, Center for Long-Term Cybersecurity, UC-Berkeley
Nils Gilman, Associate Chancellor, UC-Berkeley

Mr. Gilman welcomed the Commission to the University of California at Berkeley, and the Center for Long Term Cybersecurity (CLTC). It is also appropriate for the Commission to be meeting at Berkeley because of Berkeley's longstanding commitment both to basic research, to public policy, and to research in the public interest through public policy. We combine that with the fact that cybersecurity and the solutions we will develop for cybersecurity really involve a three-way collaboration between basic research, public policy, and the private sector.

The private sector is aware of many of the assets that we will need to protect with cybersecurity, and the vector to deploy the solutions we develop using cybersecurity. What this Commission is all about is precisely operating at the intersection of basic research, public policy, and private sector collaboration.

Betsy Cooper, Executive Director, Center for Long-Term Cybersecurity, UC-Berkeley

The Center for Long Term Cybersecurity was founded in 2015 with a grant from the Hewlett Foundation. We believe that cybersecurity will be the existential problem society faces in the internet age. We approach that problem by thinking about three core relationships:

- The relationship between the short and the long term; We believe that politics and the economy will change dramatically in the next five to ten years, and what cybersecurity means in that society will change as well, and we will need to prepare for those eventualities.
- The relationship between strategy, policy, and academia. We want to be an organization that brings the basic research mentioned by Mr. Gilman out into the field, whether it is

interacting with companies, other non-profits, academic institutions, or with government. It is a core part of our mission to breakdown some of the barriers that have existed so far.

- The relationship between people and technology. We are an organization that begins from the principle that we have great technology, and great technologists will be able to make technology right. The concern is with what people will do with technology once they have it. We believe this core relationship drives a lot of the research and programming we put on.

As an organization we are focused on research. We have given out over a million dollars in basic research grants to organizations all affiliated with the University of California, Berkeley. We are also focused on educational programming. Both to try to improve the pipeline problem that exists in the cybersecurity field today, but also to engage women, minorities and other under-represented groups that are not currently represented in the cybersecurity space.

Finally, and most appropriately for today, we are an organization focused on relationship building. We approach relationships broadly, whether they represent relationships with companies to improve joint research efforts, relationships with other academic organizations, or as today, with government officials to try to improve the policy pipeline for cybersecurity. We are extremely pleased to have the Commission here today.

We would like to thank the NIST staff, and the contractor staff assisting them. The event today has been successful thanks to their collaboration. We would like to thank the International House staff and the A/V staff for putting this together today. We would like especially like to thank the CLTC staff for their assistance. The CLTC will be live tweeting during the event.

Meeting Opening and Remarks

Thomas E. Donilon, Commission Chair
Samuel J. Palmisano, Commission Vice-Chair

The Chair commended the CLTC's work on cybersecurity and developing diversity in the cybersecurity workforce. He thanked the panelists for attending the meeting. The core question for today, as the digital economy experiences dramatic growth, and where Accenture estimates the digital economy represents approximately twenty-three percent of the current global economy, as that economy moves on to new technical platforms, particularly mobile and cloud computing with the security challenges that go with them, how do you think about these security challenges in the future, and how do the government, private sector, citizens and consumers meet those challenges? It is the core question facing us today.

The way we've been thinking about our challenge over all in the Commission is essentially a memo to the next President. It seeks to point to the signal ideas that will form the basis of the cybersecurity program for the country for the next few years. It is an opportune time to do this. The memo we deliver should provide the response to what the next President's priorities in cybersecurity will be. It should provide the signal ideas to form the basis of a sentinel program for the next five to ten years for everyone.

Commission Business:

Thomas E. Donilon, Commission Chair

Approving the minutes to the April 14th meeting. No corrections were noted for the April 14, 2016 minutes. Mr. Palmisano moved to approve the minutes as presented in the UC-Berkeley briefing book provided to the commissioners. The motion was seconded, and the motion was approved.

Kiersten opened the meeting officially at 9:15 a.m., Pacific Time.

Panel 1: Addressing Security Challenges to the Digital Economy

Geoff Belknap, CISO, Slack
Patrick Heim, Chief Trust Officer, Dropbox
Hemma Prafullchandra, EVP and Chief Technology Officer, Products, HyTrust
Alex Stamos, CISO, Facebook

Geoff Belknap, CISO, Slack

Mr. Belknap thanked the Commission for the opportunity to speak and noted the views presented today are his own gleaned from twenty years of working in the technology and security industries. Every day people's lives become simpler and more productive thanks to the benefits of technology. The economy is influenced by a wide array of useful technology with enormous impact on our economy and our workforce. It is important to ensure the influence of technology continues to be positive, given how much we require the ability to trust in the products, platforms, and companies supporting this change.

While there are no silver bullets, the challenge we face today, there are several policies that need to be improved:

1. Corporate boards should regularly review their governance and transparency security and privacy, including their company's cybersecurity maturity, preparedness, and effectiveness with the chief security officer. For public companies, this review could be incorporated into the SEC business and financial disclosure requirements.
2. We strongly urge companies that collect data that consumers consider to be personal, or that enterprises consider to be private and sensitive, to publish an annual review for privacy and security privacy policies. These reviews should describe the kind of data collected, uses for each type of data, and the entities the data is expected to be shared with, and how often the sharing takes place.

   Policies should be expected to explain how data is protected, whether in transit or at rest, encryption used, authentication, log in and auditing access, vulnerability assessments, penetration tests, security scanning, bug bounties, code scanning and security practices. Taken a step further, these policies should be presented in plain English in such a way to allow consumers, customers and others to make risk informed decision.

3. We can embrace secure-by-design standards and practices. The Cybersecurity Framework (CSF) was a game changer. It is accessible, flexible, and relevant in a way many security frameworks are not. In a landscape where an attacker can do more harm by exploiting poor security hygiene than perpetrating original attacks, developing communicating, and practicing good security hygiene is paramount.

Directing NIST to expand the core framework and also recommend that data security practices could improve the practices of many organizations. Updating the standards and practices would enhance the chances of more organizations to stay current and practice good security. These standards and practices should include guidance on what types of data should be considered sensitive, even if it means broadening the definition of personal and sensitive data beyond current legal definitions of protected personal information. This will help establish generally acceptable standards of caring for data.

4. We can hasten the move to a post-password world. All too often the data we entrust to our technology platforms is protected simply by a user name and password. It has proven to be a poor method of protection. Recent development of multi-factor authentication, certificates and other secure authentication technologies have already delivered products and services to market that represent progress on this issue. Encouraging the investment, development and implementation of new technologies and best practices that reduce the use of passwords for user authentication can only improve security for consumers, enterprises, and governments.

Patrick Heim, Chief Trust Officer, Dropbox

Mr. Heim thanked the Commission and introduced his background representing a spectrum of roles in the security field over twenty years.

There has been a failure of economics in security. Consistently, it appears security appears cheaper than it actually is. It drives a vicious cycle of over investment in security related opportunities. It has been noted in areas of organizations that there are not good economic models for factoring in the true long term cost for sustaining security in systems.

Mr. Heim was at a recent meeting hosted at Palo Alto, CA where there were representatives of the US military who were asking the technology industry to provide solutions to help secure event systems in various components. The focus was not to upgrade or look at the underlying systems, or building more hardened platforms, but to add new wrappers to the existing system. There was a philosophy that did not include sustainability or looking at the long term cost of embedding security or maintenance of security into these systems.

Outside the military context it is very common for CIOs to have pressure to continuously reduce operating expenses on an annual basis, which reduces the ability to continually invest in long term system maintenance or in system refreshes. We have noted there is a strong correlation between legacy and unmaintained systems and vulnerabilities.

The recommendation to the panel is that although there hasn't been any investment in looking at ROI, it should be calculated for new technology investments in the government and private sectors. It is needed to truly identify what the long term costs are for maintenance of systems, and how to budget for replacements. This discipline is currently missing. Mr. Heim believes it underlies many of the current systemic and long term vulnerabilities that exist in our environments.

From a technology company perspective this economic plays out in a slightly different way. If there were two companies who each were innovating aggressively, and one devoted more resources to make its product more secure, [that company devoting more resources to security] would very likely be at an economic disadvantage related to that product. Currently, the market rewards innovation and does not reward creating a fundamentally more secure product. This is also an opportunity for the Commission to think about how to shift this dynamic, how to create a level playing field, and how to encourage technology companies that are at the edge of innovation to place greater emphasis on creating secure products.

There is a challenge to educate citizens and consumers at a global level in good security practice. Technology providers have a role in creating this shift. There is a limit of education's ability to actually change individual behavior. When individual behavior is measured, there is a capability to change behavior for the better with more education. There is an absolute limit to the level of behavior change that can be accomplished.

When we look at the threat environment we face, many of the compromises are associated with manipulating individuals through phishing attempts and others. We have not come up with a good method to educate consumers on a large scale. Educating billions of consumers around the world, by itself, is not going to work. This is not to say that we haven’t, we've actually done a good job as yet. It is incumbent on large technology companies then, to conduct experiments, and look at how behavior is shifted, and to compensate for human weakness. In the end, human beings will be human beings. Our perceptions of risks, motivators, and drivers are based on living in the physical world, and are not going to change.

It is a function of government and large industry to determine what those weaknesses are, and invest in studying the underlying behaviors and investing technologies to compensate. It includes promoting two-factor authentication and other means. Mr. Heim noted that Dropbox has free 2-factor authentication for users worldwide. However, less than one percent of users take advantage of it.

The role of networks is diminishing today. When examining portfolios and investments, it is clear something has shifted over the last ten years. It may not be reflected yet in where money is being spent. FBI and other law enforcement authorities say the internet is going dark on them. It may be also for corporations. The cost of encryption at the network level has made it ubiquitous. At the same time, threats have evolved.

There is now tunneling content in online services. The ability of the network to act as a protective barrier has diminished over time. We need to push the thinking of security investments and drive innovations at the end points where we know what is happening. The network itself, as a means of control and monitoring is diminishing. It has been introduced as a challenge for mobile and cloud computing. It is true in the area of mobility, the network is wherever the connection exists in each distributed end point device.

Hemma Prafullchandra, EVP and Chief Technology Officer, Products, HyTrust

Cybersecurity is a very broad and complex topic. It is a global issue. There is a need for international collaboration and holistic approach when it comes to cybersecurity. Certain nations will not cooperate, but for those we need to make sure we have import regulations that require certain levels of confidence in the technologies that are offered domestically. This may include services that are based internationally and offered to Americans, or technologies coming into the country.

The biggest challenge today is how will consumers know that identity or access control implementations offered by service providers will be similarly implemented? What confidence is there that there have been no shortcuts, or not done more than the minimum for identity access control?

We should try to define a set of core protections that every service provider and technology vendor must comply with before products can be offered to Americans, whether consumers or enterprises. We understand what the core is already, but we don't have a mechanism to say they are implemented equally across the board. As the only CTO on the panel, she notes cybersecurity is added on after the fact.

The biggest investment we can make as a nation is to offer some self-service or validation of the technologies being utilized and developing this in a way that is tactical and enduring at the pace technology is evolving.

We need to apply the same creativity and innovation to solve this problem so that there is greater confidence in the technology we are all using. We have good controls over the electricity used in homes today. We need the same controls for cybersecurity. The feeling is a major event has to happen before there is real progress.

The second recommendation is we must be proactive because our already large dependencies on digital technology will only increase. We must start education early. Children start early with using digital devices. There should be education on security before kids start using devices. Our education system does not have the emphasis on digital safety being taught prior to the young age children now start using devices. We started with using these devices before thinking through possible consequences. Education can start as early as pre-K.

The third recommendation involves the definition of critical infrastructures. We have largely defined telecommunications, energy, and those classics we think of when considering critical infrastructure. We need to re-think the definition to also include cloud technologies and providers as part of this group. Many critical providers offer crucial services. They need to be identified and prioritized in terms of criticality. If large businesses are secure, the small businesses depending on them will also be secure.

Alex Stamos, CISO, Facebook

Facebook's mission is to make the world more open and connected. Essentially, the mission is based on trust. The trust the government places in us, and the trust our users place in us is very important. Facebook has applied its ideas about mission to the benefits of connecting people, and to how it does security. Mr. Stamos has identified three long-term trends that appear to be getting worse and are dragging down national cybersecurity.

1. There is a critical lack of talent in the cybersecurity field. He mentioned, mainly due to the difficultness of it. Facebook for example, offers a lot of incentives to assist with recruiting; however, the government is not as well positioned for recruiting and this is an issue that doesn't seem to be getting better.

2. There is a trickle-down effect of capabilities into a much more complex set of threats than what has been seen in the past. The level of attacks and degree of sophistication on our networks [suggest] capabilities that might be typical for top-tier cyberwarfare. Those tool capabilities and threats have trickled down into a much broader set of threat actors. As a result, there is a much larger set of companies falling victim to these threats due to the increased motivation to steal a nation's sensitive information.
3. The talent we have is not being utilized efficiently enough. We are not properly collaborating information sharing across the private sector, security research communities and the public sector. The emphasis would be to utilize the existing pool of talent across sectors and make it available to each industry.

   There are four recommendations in this area:

   1. American companies need to embrace modern defensive ideas, which includes the idea that moderately sized enterprises will not be able to prevent all breaches. It means accepting the fact there are many ways attackers can get in, and raising the sensitivity to attacks to the level each organization is able to respond to quickly and decisively. We need to increase the ability to block attacks immediately and defensively. The Fortune 500 must adopt this stance going forward.
   2. Information sharing can massively increase the cost for attackers. It includes attackers that are directly economically motivated (like spammers and malware, etc.) and the high-end attackers that like to invest in one set of cutting edge tools, control channels and systems to utilize against high quantity of victims at one-time.
   3. The intention is to maximize the cost of their investment. By information sharing, the cost investment can be minimized and removed from them. Facebook offers a free service called the Threat Exchange which is a machine-to-machine threat sharing platform. It consists of 350 companies, with almost all major tech companies being involved. It provides a service for all partners on the threat exchange to provide information sharing on URLs from domain and spam sites to IP addresses to top malware nation -states that have been caught in transit in the system.
   4. Improve the collaboration between corporate and the security research community to work positively together. This has been turning around but needs to continue. A majority of tech companies now have an ability for researchers to responsibly disclose bugs. A large percentage of tech companies have bug bounty programs which will pay to have bugs reported.

      Since the bug bounty program started, Facebook has fixed over 2,400 flaws based upon external bug barrier reports, and paid out 4.3 million dollars to the security research community.

      Finding ways that this type of model works for more than the technology companies would be a best practice for both America and international talent to tap into. Currently, the number one country that contributes to this program is India. The ability to utilize this talent pool would benefit American consumers, and be an untapped super power to companies.

A longer term goal would be to build a talent pipeline. Facebook has been experimenting with various programs within the middle school, high school and college levels and they are starting to pay off. Facebook has hired its first high-school engineer out of the program.
These programs have been around for years to encourage new talent. It would be beneficial and exciting to rollout cybersecurity education all the way through middle school to the university level.

Panel One Discussion

Commissioners of the Commission on Enhancing National Cybersecurity

Mr. Donilon: [*To Mr. Stamos*] You mentioned the importance of information sharing and raising the cost of units per attack against the potential benefit as well as the Facebook-sponsored threat exchange program. Can you talk about your experience with the government with respect to information sharing, how effective has it been and what ways can it be improved? Additionally, what recommendations might we be thinking of regarding government to private sector information exchange?

Mr. Stamos: Facebook does have a positive relationship with federal law enforcement when it comes to going after attackers. However, a lot of areas like outcomes from hackers and child safety are not as good because it is much more difficult to get international cooperation.

While we like having a relationship, there has not been an instance that the U.S. government has provided information that has then been used to deflect an attack. Part of that is due to receiving briefings and/or bulletin's that are not real-time (realistically, they could be 6 months after the fact). For information sharing to be meaningful, declassification of information and a more rapid response at least from machine-to-machine would be a positive step forward.

For example, once any human gets involved (by waiting for an email, phone call or sending someone to a SCIF (Sensitive Compartmented Information Facility) for a briefing), given the speed which adversaries are moving, the attack is over. If we want the government to do more than watch these attacks happen and then release to us after the fact, finding a way to communicate with the government using machines would be key.

Mr. Donilon: *[to Mr. Heim]* The concept of starting to think about security, not at the individual entities network level, but rather at the end point of increased reliance on cloud and mobile devices, where is the industry on this concept in terms of thinking about conceptually implementing effective cybersecurity measures in light of the evolution of the whole system?

Mr. Heim: The cybersecurity industry is overly invested, with an estimate of 1,500 new start-ups. There is almost too much innovation, which can make it confusing from a consumer's perspective. I'm not sure that's a sustainable state we can be in. We are seeing investment in every corner including the end-point side. There is a lot of focus on the end point but that's not saying that companies investing in innovation on the network has been diminishing. I think we need to understand why. However, this will probably play itself out naturally as the network capabilities diminish over time.

Mr. Donilon: *[to Mr. Heim]* Another question, you provided an interesting statistic on a less than 1% adoption rate of your dual-factor authentication product for consumers. How can we interpret that, is it a technical, research and development, psychological problem and / or an industrial psychology problem? Additionally, where is the thinking in regards to making these systems take into account the behavior of people and technology, and will it make technology more effective to adopt and use?

Mr. Heim: It's a complicated problem, and there are several parts to it. For technology behavior versus education, people may not know all the capabilities that exist on their technology are available, or the benefit of turning them on. They perceive these capabilities as too costly, or it simply interferes with their user experience.

Another area of focus may be to experiment with users to understand different behavioral patterns. Although the thought of running experiments with humans has some negative connotations, there is openness to running security experiments on population sets to understand how human behavior can be adjusted, as well as the design of technology to be used as a compensation mechanism.

Mr. Donilon: *[to Ms. Prafullchandra]*, In having a focus on international technology standards and core capabilities before importing into the U.S. market, what about technology vendors in U.S. standards? What kind of mechanisms can you think of where we could implement a set of programs?

Ms. Prafullchandra: Before any new technology gets to the market and initial release to Americans, standards should be applied equally, not only domestically but also on imports. This would create a certain level of cybersecurity controls and protections to be implemented, like safety measures, privacy, identity, audit logging and access controls.

The core set of controls would need to be defined, and at the very least, have a minimum set of standards. As a validation mechanism, an online service could be created depending on the size of the company. For example, there may be a self-service that allows a small business to get certified indicating that the product is good enough to be used by Americans. It is essentially requiring a baseline for all vendors across the globe.

Mr. Donilon: *[to the panel]* How do you all think of the role of government and what would be the most important thing the government can do in terms of cybersecurity to enhance your efforts in the private sector?

Mr. Heim: The government needs to clarify the role in which they intend to play. There is clearly a role in the kinetic space providing for the common defense for the U.S. However, it's not so clear, what the role of the government is in the cyberworld. The government has an opportunity to take a step back and truly define, communicate and articulate what role it intends to play and use foundational principles.

Mr. Stamos: The most important role of the government is to not deploy detailed standards from a cybersecurity perspective for the private sector to live up to. For example, probably the most widely deployed cybersecurity standard in the world is the Payment Card Industry Data Security Standard (PCI DSS). Every single company that experienced a data breach of over 100 million credit card numbers traded on the black market were PCI DSS certified. Having been breached, the assumption was that the companies attacked were not certified. However, the truth of the matter is, it's an issue staying on top of the changing canvas of cybersecurity threats and it's important that security stays relevant. It is extraordinarily difficult to come up with standards and stay relevant over time. These standards often take years to adjust to, like enterprise virtualization to cloud computing, etc. The reality is, they force companies to what they should be doing at a minimum bar, but not what they actually should be aiming for, or they would distort the industry with a huge amount of money going toward compliance.

As a recommendation instead, we need a more fine-grained decision based approach to what kind of threats companies are facing while being very careful about what gets propagated by the government. [The purpose is so that] people and companies don't aim lower in order to comply. This would be a hugely positive step.

Ms. Anton: [*To Mr. Stamos*] I agree that more information sharing is needed and anything we can do on the government side, as well as industry would be positive. Specifically, you mentioned that there has not been to date any information from the government that helped you deflect an attack.

Additionally, with the Threat Exchange Community consisting of 350 private sector companies; has the program, at any time, been able to deflect an attack and, if so, what can the government do to leverage that program concept?

Mr. Stamos: We have evidence of both. The Threat Exchange has already reduced the economic incentives for the type of attackers that try and target a widespread group of people and make money on each. We have also stopped the spread of malware, spam and intrusion attacks (from lower level to high-level attackers). There are many preventions but two examples, specifically, were from high-end attackers that were stopped by information sharing and an intrusion was detected due to a breach that was stopped by collaborating within the Threat Exchange program.

The idea behind some of the high-end attacks is to put together an attack tool kit with the intention to distribute it to multiple operational teams so all go active simultaneously and, if one, of those victims can catch that either from an automated pipeline or a manual analysis and put it on Threat Exchange and push it out to its partners then you can immunize those partners before the threat happens or catch it within minutes. Those high-level attacks can spread laterally within a network which makes them very difficult to get out.

Ms. Anton: *[to Mr. Stamos]* The Commission as a whole has discussed the need for metrics and the need to measure the cost of the real-time exchange. Is there a science that assists with capturing measurements?

Mr. Stamos: The greatest minds of our generation have been destroyed trying to figure-out security and have tried to figure out how to capture measurements and failed. For Facebook, the threat exchange is an open platform. Companies can decide what they share, and what they use for detection. However, they have to calculate their own risk on investment.

From Facebook's perspective we see it as valuable. Even if we don't stop an attack (which has not been the case), we consider ourselves as an eco-system platform that is protecting other companies, which is worth it. It is a hard to quantify, but we have significantly less customer churn rate with vulnerabilities. For smaller companies, the value is to leverage small and large businesses information on the Threat Exchange.

Facebook is usually the first to be attacked, although that is not necessarily a bad thing. Having good adversaries, is a gift which usually brings talent that can be utilized and there is knowledge gained from each attack. Meaning that when someone goes into an intelligence agency and wants to obtain Facebook information, the intelligence agency usually gives the task to their best team and that keeps us on our toes. Meanwhile, we are training ourselves against the best. Additional benefits include a trickle-down effect to lower-level teams in those organizations as well as publically. If big companies are attacked first, we have the ability to protect the smaller companies.

Now, that still means that the smaller companies need a basic level security investment regarding their network. That means some sort of Systems Insight Manager (SIM) system with integration and incident response capabilities. They essentially need to have a system in place that gathers all that data for the incident response team. Large companies have dedicated intelligence teams and/or malware analysis teams. All of these benefits are why we see this program as worth it to keep our partners and customers safe, which is why this service will remain free.

Ms. Wilderotter: *[to Mr. Heim]*, I agree with the challenges that are currently being placed on the network. Regarding ROI and investing into sustainable technology verses the network, have you thought about the idea of incentivizing companies from a policy perspective that would enable companies to continue that investment?

Mr. Heim: The thought is to change our thinking from making a security investment, to estimating the cost of security over-time as part of the original technology investment including long-term sustainability. The challenge is changing the perspective of adding security band aids. As systems age, the cost of security increases dramatically to the point of being unsustainable at some point. There needs to be more emphasis placed on the overall life-cycle of technology and have an appropriate budget built in to continuously secure it. Then, making sure the money is available to replace, update, and re-platform the environment as needed.

The hope is once the economics are understood regarding this model, to evolve a discipline of decisions around where technology investments are being placed. It appears technology is extraordinarily cheap and driving over-investment which increases the technical legacy debt that all entities will have to compensate for in the future.

Ms. Wilderotter: *[to Mr. Heim]* Would an accelerated rate of depreciation on equipment, tax benefits to companies for having a secured environment, and a tax credit for educating employees and supply chain be worth considering? Would those types of policies help the initial focus and drive the direction of thinking of security life-cycle investments?

Mr. Heim: That is an interesting idea, and directionally and absolutely going in the right direction. It is the ability to get corporations to update, replace, and re-platform to modern environments. Whether those incentives are tax credits, or preferential treatment for government contractors, I do agree it is the correct way of thinking of this problem.

Ms. Wilderotter: *[to the panel]* Regarding collaboration from a policy perspective between government and private sector research, any ideas on how government could drive a policy to encourage more collaboration that you are not seeing today?

Ms. Prafullchandra: The NIST National Cybersecurity Center of Excellence (NCCoE) in Maryland is a collaborative environment in sharing new technologies. More centers that could be available regionally that could have collaborative efforts without having to go into a SCIF, or cleared areas. It allows open access areas for collaboration and demonstration of technologies in solving specific use cases. It would be beneficial.

Mr. Stamos: If the government could get the entire Fortune 500 to at least accept bugs responsibly, and to give incentives to the security industry to act responsibly, or have even half of those companies recognize the value and pay for it.

Communicating with other CISOs and general counsels of other large companies, and additionally remove other regulatory requirements that encourage them not to know (from a see no evil, hear no evil perspective) when a bug is found. For example, if a bug is found in the network, which could potentially kick-off a 6-month investigation by the Federal Communications Commission (FCC). It is better for them to not know about the bug than deal with paper work.

There is a need to find a regulatory safe-space for companies to incentivize people to adjust and start sharing more responsibly. Software is innately flawed since it was written by humans. As a society, there should not be disincentives in reporting bugs, instead people should embrace it and recognize the value in correcting it.

Mr. Gallagher: *[to panel]* Is there a fundamental design problem regarding human behavior and technology? Meaning, is it easier to educate and correct human behavior or adjust technology?

Mr. Heim: Humans are somewhat fixed. There is a limit to what can be achieved through educating people. It is mainly incumbent on large technology providers to invest in innovation emphasizing the improvements of technology by design.

To assist with technology design efforts, conducting experiments on human behavior that are outcome oriented with the intent to understand where technology can be improved. And, building in safety nets within technology platforms to limit the damage when human behavior cannot be modified.

Dropbox is a member of the Threat Exchange, and integrates into the platform. If we notice that users' passwords have been compromised, we proactively will take those and expire those user accounts, and force a reset against the population to change passwords. This happens even if those users did not have the same password on Dropbox as other sites. One of the largest root causes today of people being compromised is linked to password re-use on multiple sites. This is a simple example of creating safety nets as a service provider. The idea is to change human behavior when possible but not rely on it as a security control. This is an area of investment that needs to be led by large IT companies.

Ms. Prafullchandra: Adjustments in human behavior and technology by design are necessary. Technology is growing at such a fast pace, we don't understand the impact and consequences of how humans will interact with it, use or not use it.

The current generation is very trusting in terms of the digital economy and technology. They have a simplistic view in that they do not believe harm will be done to them. The mind set and expectation of people is that technology is going to safeguard them.

As a society, people do not understand the impact of technology and how it can be used. Cyber-bullying was an outcome of human behavior and technology being misused. There are behaviors that are very human, but the impact of those in the digital technology world is not understood. The importance of continuing to educate people on technology while innovating and automating protections in this context.

Mr. Stamos: As a society, the need to build technology that is safe is important not when they are used perfectly. 60% of the world's population is not on the internet yet so technology companies will need to think in terms of the median new user when building their products.

Facebook has 1.65 billion users worldwide and 84% of them are outside the U.S. The median new user may have never used the internet and unlike most people in the United States may have never grown up with computers or technology. As technology providers, they need to be empathetic and build and design technology securely and do not write-off inexperienced users or users that may make simple mistakes that realistically they cannot understand.

Mr. Gallagher: *[to panel]* What is creating this new perspective in the technology sector and is there anything that the Commission can do to encourage it?

Mr. Stamos: Facebook's focus is on building products that work for people around the world. Facebook has a program working with other countries that we are currently not servicing, and studying these populations. Additionally, Facebook has better measurement data of undesirable outcomes that assist with forward progression. For Facebook, security is only focused on building perfectly secure products.

The truth is, even if they were perfect, people would misuse them to hurt each other and be misused by human error. Understanding the broader perspective, we have a wider set of metrics and measurements that are monitored other than the measures such as how many intrusions, malware detections and bug detections were found. Facebook has a team that actually captures human harm that happens on the platform. That team conducts a number of experiments to try and drive that harm down.

Mr. Donilon: *[to Mr. Belknap]* Would you like to add your company's perspective?

Mr. Belknap: There is very little recourse for the consumer when harm has occurred or an identity has been breached, which affects everyone including children. Technology offers the ability to damage people with no fault of their own by identity theft, and there are few antidotes to remediate the problem. While all service providers' care about their customers, how can we protect consumers and entities that have been damaged. This may be a good area to place more attention as technology progresses.

Mr. Lee: *[to Mr. Heim]* The idea of economic failure and technology appearing cheaper, what are the implications of that?

Mr. Heim: The perspective is geared toward the world where data centers and investing in purchasing systems have a large maintenance burden. The transition to cloud computing is one of the solutions. A cloud company's number one principles are trust and security. The trend is to move away from in-house infrastructures, which has those elements of unsustainability, and move towards cloud providers as a natural transition. The failure of undefined cost-model linked data center economics to the transition to cloud providers, which have the security talent and the core mission where security is embedded into the architecture in order to provide a rapid response while remaining agile in the face of threats. The game changer, in my mind, that will be recognized over time is that cloud computing is one of the most powerful enablers of getting beyond traditional data center economics.

Mr. Lee: *[to the panel]* Then, from the investments companies make, as they budget for investments and earmark funds in some way and address the cost of security, what would be the mechanisms? This may lead into my second question, mainly directed at Mr. Belknap. What faith do you have, and what mechanisms do you see to ensure those investments follow through in some meaningful way to improve security of your products?

Mr. Belknap: A common question all of us receive from others is, what would be an appropriate level of investment, and that is one of the great philosophical questions of security because it includes so many variables. I do believe that coming up with metrics to report and making it a higher level discussion and having a framework to do it in a rational fashion is extremely important. Right now, I would say there is a lot of reliance on professional judgement for risk. There is no common standard for risk assessment. We are not able to have those discussions where there is blending of economic risk with technical reality.

Mr. Heim: There are so many variables of the data scale to protect and diversity in a system while also predicting whether global or domestic. Having a framework to discuss mechanisms is important. There's a lot of reliance on professional judgement without a common standard for risks. The perspective would be blending economic risk with technology.

Mr. Belknap: The government has the incentive to encourage people to take this seriously and have people build security by design. Consumers bear the burden of leaked personal information and there has been little negative impact to the responsible companies. There needs to be other mechanisms in place to ensure boards of executives are thinking about this within an organization.

Mr. Lee: *[to Mr. Belknap]* Do you envision the NIST Cybersecurity Framework in its current form, or some evolution of the NIST framework, as being the framework to create transparency?

Mr. Belknap: There is a very good possibility that it could be. At the most recent board meeting of my company, I presented a slide based on the NIST framework. It turned out to be a very useful tool for discussion. It presented the company's maturity perspective, and five different core security-related functions.

The framework does offer positive transparency to discuss the five core functions we perform in security. It's easy to digest for investors to understand in the sense of, "why security matters", as well as what maturity level the organization has been evaluated at, and what the functions are that are being performed and accomplished. That is the bare minimum level that every board should understand.

Mr. Lee: *[to the panel]* Has there been some level of cybersecurity framework adoption across your other organizations?

Mr. Stamos: Facebook has used the NIST Framework. It is useful to have a framework to discuss the needs of each organization, and remain flexible especially for international companies.

Mr. Lin: *[to panel]* Are there any thoughts on speeding up the automated process regarding information sharing, and on taking action with respect to response time in responding to adversary attacks? Getting responses seems to be at least as difficult as sharing information initially.

Mr. Stamos: The information is useless if there is little ability to query all one's systems within a small period of time. Some helpful trends that would assist with automation would be moving to cloud computing on enterprises and mobile devices that have better security models than the traditional PC.

As an example, large email client services are the only ones qualified to provide this service. No other entity controls the code, and additionally do not understand how it reacts, nor has the ability to patch it except on maybe a quarterly basis. This can only be secured through the email client. Service providers and cloud computing providers are part of that group.

Cloud-computing will vastly assist with information sharing. Cloud providers provide protection for these groups invisibly, as well as find a way to distribute information to their customers. Facebook uses an open source agent that runs on all its systems, which can run system-wide queries and receive responses very quickly. There are some good commercial products that have the same capabilities. Peer-to-peer systems are starting to be deployed. There are exchanges like the threat exchange, and now we are starting to get those things connected so we can get alerts. When certain alerts come in, we query our systems worldwide because it comes from a trusted partner. This is the model we need to get to.

Mr. Lin: *[to panel]* As an example, if an indicator of compromise is reported (IOC) and an automated alert is unable to be sent out, will an automated patch be triggered?

Mr. Stamos: It's not an automated patch, but there are functions that happen automatically to isolate the IOC. A lot of companies are not at the capability to do this yet, but it is a direction where companies should be moving.

Mr. Lin: *[to Ms. Prafullchandra]* Can you provide insight on trade-offs between mandated standards and the impact on innovation?

Ms. Prafullchandra: Defining the minimal core standards would be key, such as identity management, how it's managed, and how access is granted. Services can go live at any time, but if a company is claiming they have access management, then the quality of identity management implementation should be measured. There should be confidence whether using Dropbox or Facebook, people's identities will be managed equally well even if people are using their Facebook account to login into another site.

Today, people are trusting blindly and that trust should be something that can be measured by developing metrics and services people can have confidence in. Cloud computing is the appropriate direction for all companies to heading in. Cloud computing offers a lot of quality measurements without degrading the pace of innovation. We have to innovate in this space as much as we do with developing new technology.

From a government perspective, incentivizing small businesses to move to cloud computing faster, rather than trying to run their own will help. Moving to Office 365 for email would be a positive step forward with filtering spam email and managing at a level that can be better protected.

Mr. Lin: As clarification, the security performance standards would be put on key infrastructure components and have companies build off those, not on regulating every application. In other words, only regulating infrastructure services on which applications rely.

Ms. Prafullchandra: Placing security standards on the infrastructures is a starting point. There is not enough maturity known to place standards on every vendor's applications. This is an area of research that needs to be explored.

Mr. Heim: We've recently seen large password dumps in the news. On the one side, there was a Russian company that stored passwords in plain text with no encryption. Then there are companies like Dropbox and Facebook that have designed their password encryption mechanisms under the assumption that they will be compromised, and how will integrity be maintained in that instance.

We can view security as a function of time. Given whatever the current standards are, in terms of compute time, passwords may have to resist attacks for a certain period of time. It is very abstract and requires some degree of interpretation. It would move as technology moves, and would be challenging to implement.

Mr. Lin: *[to the panel]* The entire discussion up to now has been focused on security as something that must be added. It would be great if the world was not like that, but it is not. Is there a way to flip that around and say, are there business opportunities that are enabled by better security? There are surveys that say people are afraid to do various things online. Would you comment on the idea that security could be an enabling factor for new business opportunities?

Mr. Heim: I would make one comment about security as a business opportunity. In those cases, it's rarely about the deep elements of security and engineering, and more about the certifications that companies invest in. There is also a danger in that because if the business is too focused on compliance and certification, then it's a zero-sum game. They may be drawing from the investment pool to do really strong engineering. As Mr. Stamos mentioned earlier, every credit card company with a major breach was PCI certified. I think you will hear a common theme from this team here, that certification has its place, it's part of a larger portfolio, but it is not a substitution for investing in real security opportunities.

Mr. Lin: I'm wondering if there are serious business opportunities that you see that could be enabled by much better business opportunities.

Mr. Belknap: I think from a consumer perspective, maintaining using trust of users is critical to having any engagement with a product if there is any kind of private information involved. Trust is more than security. When I think of trust, people must believe the maker is making decisions on their behalf that is based on the consumer's best interest. They must believe the maker has the wherewithal to stand up for those decisions. That's where security comes in, to protect the decisions companies make to do the right thing. It is critical for companies to do what they can to maintain the trust of their users. It is also important from a regulatory perspective for the United States to have an environment where the rest of the world trusts American technology companies. Currently, it is something that is generally true. It is not as true as it was five years ago. It is a durable, competitive advantage for the United States that we can grow upon, or we can throw it away if we do the wrong things in the next few years.

Mr. Sullivan: I've been thinking about these issues through the lens of a smaller business. A few of you have the luxury of large resources and board support for building security teams. For this Commission, we need to think about not just the top 100 companies that have those large budgets, but the really small companies that are getting their whole business on the internet right now. How big does a company security team need to be to participate in something like the threat exchange, or how big should the security team be for a fifteen-person law firm, or a fifteen-person real estate agency?

Mr. Heim: I think it should be zero. I think those small companies need to embrace the cloud almost entirely. Investing in infrastructure, having to have security officers in small business will not scale well. We've already mentioned that the resource availability of skilled resource professionals is the huge constraint. Small companies are at a huge disadvantage in trying to attract, retain, and compensate those types of individuals. The alternative is to create a mesh of services for small companies such as security as a service (SaaS), and others that really help provide what a small business needs located in the cloud with small business providers.

Mr. Sullivan: Do you think the enterprise products that are out there that small businesses are adopting come out of the box secure? You mentioned Dropbox offers multi-factor authentication to consumers and they adopt it one percent of the time. When a small business decides to put their business in the cloud, does it come secure by default?

Mr. Heim: I think we need to examine what the product is. One of the things we have consistently identified is products that have a consumer foundation like Facebooks' and others are under continuous attack. However, there is an element of "Darwinian" evolution of security in play here. Our systems are reasonably secure because we are under continuous attacks. When there are products that are younger in age, and not as broadly exposed, it's not really known until something is attacked. The true measure of security is the ability of the teams to respond, adapt, and to recover.

It seems most of the products that service small business currently, do have great standards. It makes it easy for companies to focus on authentication across a large variety of cloud services. We're seeing that the underlying ability to piece together services for companies without infrastructure has evolved and is evolving in a very positive direction. The real problem becomes one of authentication, not perimeter control. This is one of the supporting points for the earlier discussion the network is disappearing. When we think about small companies today, they are accessing services. There is no data center. The concept of a corporate network, or a production network doesn't exist because everything is accessible from anywhere. The real problem becomes one of authentication, not perimeter control.

Ms. Prafullchandra: There is a challenge with small businesses adopting cloud-based services. It is something they are embracing but the smallest businesses don't have the skill sets to evaluate the different providers that are available. It goes back to quality. How do they go about evaluating hosted email services or productivity tools they may want to use? They may not necessarily have the skills to choose, so they may rely on local consultants where there is a trust relationship. However, those consultants may also not have criteria to judge. There is no trusted relationship in this situation.

Mr. Belknap: To use an analogy, and turn back the clock a bit. People gave up horses and buggies and started using cars. I think technology is advancing quickly, and we are putting automotive products on the market that have seatbelts. This may be an unpopular opinion, but the auto industry is not required to put them in cars even today. For myself and others making platforms, it seems it should be important. While platforms are advancing quickly, and we're putting seatbelts and other things to keep people safe, consumers have not yet exercised the demand in the market to only by products with advanced safety features. It is something the government can influence. Strict regulation may not be the way to do that, but there is room to influence consumers in this direction.

Mr. Sullivan: Getting a little deeper on that, and the PCI example that was given. I know from experience, it is hard for a standard to keep up with technology now. What are the places we could be looking at right now? Is federated identity something to pursue? Is focusing on the network level something we should pursue? What are areas to pursue in the near term?

Mr. Belknap: This where I'm convinced technology is not the problem. There are a number of fantastic technologic advances that have dramatically improved outcomes. This is where education becomes the problem. Not enough has been done to educate consumers on how to make good choices. It's easy to go into an appliance store and find a refrigerator that meets the needs of the person buying it. Consumers have enough information to make an informed choice on the appliances they buy.

Consumer information to make informed decisions on cybersecurity is not really available today. Even if we go home today and implement fantastic advances in cybersecurity, and force consumers to use them, it's not enough if consumers don't know to use them. It may be a differentiator competitively. However, it doesn't improve the state of cybersecurity for the nation or the world.

Mr. Stamos: The panel hit on something interesting when talking about the ability of people to make judgements on cybersecurity. In my opinion, one of the most ridiculous wastes of money is the vendor risk management process. Is there a way to standardize the threat information process to make it more efficient? It would save a lot of money on the high end, and open up the ability to look at a standard set of judgements for smaller companies to use. There would then be a means to look at the set of information to aid in decision making.

Dealing with standards very quickly becomes too complicated. Is there a mechanism by which only the largest companies that have the most buying power have the ability to get real questions out of their vendors, in order to make a reasonable judgement? There have been a couple of efforts in the private sector that have failed to make the process more efficient. It could make the process more efficient and save money at least at the high end. There would then be more of a basis for intelligent decision making. Availability of standards for small business and consumers is critical.

Mr. Banga: I think your point about standards, and enabling transparency about using those for people choose what they are buying is critical. We've gotten used to it in food labels and electrical devices. We need to think about the digital world as an extension of the physical world, instead of it being a new world. The worlds are converging at a rapid pace. Yet, our dialogue tends to be "either-or". It is not "either-or", it's a unified world. That's part of one topic. I think the topic of small business deserves a lot of attention from all of us. We need to protect the weakest link in the chain.

I have a question on a different topic that anyone can answer. My belief is human beings prefer to be recognized for who they are, not what they remember. Our problem is, all our systems are built on what we remember and not who we are. The problem with using "who we are" is, we come very close to a debate on privacy and personal identity in so many ways. How do we frame that issue? It is a tough question for policy makers and government to consider.

Mr. Heim: Biometrics is an area that has evolved very positively. It has primarily due to smart phones. What we're seeing now with the new generation of smartphones is nearly all have the ability to have a fingerprint-reader built in, or in some cases the ability for facial recognition. But if you were to ask me what is the future of authentication, and what would it look like in a perfect world, five years from now. I think the smart phone will be used as a portable biometric and be used as a gateway. The authentication device becomes a gateway to bridge into one's PC, and other systems. The rise of smartphones has created the opportunity for a portable biometric device that is controlled by the individual. It is an amazing opportunity to utilize this consumer technology to actually step up the quality of user authentication, as long as we have the protocols to integrate those devices into the back-end systems we all provide.

Mr. Heim: The funny thing is, authentication is not that hard. We have a lot of options available for various threat scenarios, and various levels of risk, and there are good ways to authenticate oneself. The real problem, especially for consumer businesses, is account lifecycle management. Meaning, how do we tell customer accounts are created for good purposes, and matching identities on those accounts? How do we handle all the things that happen to consumers at scale? If someone loses a computer, or their phone, and their SIM changes, how will they be able to get back into their account? It is extraordinarily difficult. It is easier for people with a large physical plant. The bank can freeze the money, and eventually the owner will get back in. As people interact more and more with international organizations without local presences, it becomes much more difficult. It is a larger challenge than authentication itself.

Mr. Banga: The issue of having different aspects to use for authentication is easier to comprehend. The phone, fingerprint, or a selfie, or a heartbeat monitor recognition system that comes off an available device. However, if we go past that, all of those cross over into who one shares that information with. After all, one's fingerprints, or heart beat pattern are being given to a lot of people. I want to frame that debate, because that debate could bring all those ideas to a halt very quickly. They are terrific ideas because they seem to answer the consumer need for being recognized for who they are, vs. what they remember. There still is the issue of people's privacy. I'd like to know how you feel about it as this industry evolves.

Mr. Heim: I support that thinking, but I view it as an engineering detail. If one were to do a fingerprint verification on a local device, why could that not unlock a set of keys stored on hardware. The provider on the other side, never has to have the biometric information. The authentication occurs at the device level. The data does not need to be passed on to providers as part of the authentication protocol.

Mr. Banga: You are recommending the manufacturer become the keeper of personal identities. I'm just pushing on that part a little bit.

Mr. Heim: There must be transparency in engineering these devices, as well as standards that reassure consumers when they use biometrics, the implementation will not abuse them from a privacy perspective, and will comply with various standards. It should integrate broadly and have been securely engineered.

Mr. Stamos: Talking to the people at the Fast Identity Online Alliance (FIDO) is a good idea. They've done a lot of work on using biometrics in a way that preserves privacy.

Ms. Prafullchandra: It is an evolving situation as far as our openness in using technology, and using biometrics. As security practitioners, we are highly sensitized to the kind of information we share. But in terms of usability, using a single thumbprint to access apps is simple. We must recognize that our attitude and approach is changing in these matters. We trust manufacturers and services they render. It becomes about trusting services and providers because breaches can still happen and biometric identities can also be stolen. That's one part, the other is, especially for small businesses, the use of data is highly sensitive. Usability and convenience will always win. We must educate them on the consequences of using these things.

Mr. Stamos: When we talk about these trade-offs, I'm afraid as a society we may end up accepting the horrible status quo because people are afraid to try new things. As Mr. Heim pointed out, the last two weeks have been some of the most extraordinary in our industry in that hundreds of millions of passwords have been dumped out on the black market. It has been pretty much invisible to consumers, but there has been a mass of frantic activity happening in consumer businesses to keep our information safe. Despite the fact that anyone with access to those dumps, which is a lot of cybercriminals, now have the ability to impersonate people. If there are trade-offs to be made, they should be made openly and transparently, while being weighed against the current status quo, which is absolutely horrendous.

Ms. Murren: This question relates to consumers. If we look at some other industries, such as healthcare and financial services, they've been able to encourage changes in consumer behavior, but they typically relate to having a mandated risk disclosure in certain instances either on packaging, or in conjunction with education. Certain entities, such as mortgages, require disclosures that are understandable to the average consumer that must be read prior to entering into an agreement. Do you think this something technology companies should adopt as well?

Mr. Heim: There is a long history of click-through terms and agreements for various technology products, which unfortunately no one reads. I'm not sure that embedding security risk statements is helpful. That is my initial reaction, but I would need to consider further.

Ms. Murren: The corollary would be mortgages, where before the financial crisis people signed pages of financial documents without reading them. Now, there is a statement at the front outlining terms, and presenting risks for entering the agreement. It is a short summary to allow people to understand what they're doing.

Mr. Stamos: We've experimented a lot with this. If you look at our privacy policy, you'll see it's written to be humanly understandable. On the security side, there is less focus on internet hazards in general, than if there are specific threats. Specific advice to consumers on possible scenarios may be more helpful than warning statements up front. We warn Facebook users when they have been attacked by a nation-state not only that an account has been compromised, but it was done by attackers related to some government, and we are working to decide what kind of advice we give people and what situational help should be offered.

Mr. Heim: One the elements that may support this from an enterprise perspective, is in the emerging ISO standard 27017 that explicitly defines consumer responsibilities when purchasing from a company vs. the cloud provider. It is very healthy because everything is defined and there are no gray areas. It is difficult to reach consumers and explain their accountability and potential risks. It is a difficult proposition.

Mr. Alexander: It would be nice for security as an industry to stop scaring people. We're really good at that. I think we've almost done too much of it. It's time to move towards admitting it's scary, but emphasize what to do about the threats. WE can get to a point with consumers, where given their particular situations, they can be given what they need. If we can get to a point where those here on the panel, and other platform providers can provide a clear, easy to understand means for consumers to understand everything they need to know, it would be progress. Simply understanding risks is not enough, because it's easy to accept risk at a corporate level and just sign-off on something and hope nothing bad happens. It's much harder to maintain good hygiene.

Ms. Prafullchandra: A one-time statement up front may not be all that is needed. Practices may change for any provider. It is a good thought but I think it needs to be iterative and continuous.

Mr. Alexander: I agree with your comments on cloud computing and especially pushing small companies there. It is something regulators need to look at. My question is, what do you see as the "cyber Pearl Harbor", and what should government and industry do to work together to prevent it?

Mr. Heim: There is great concern about the internet of things, primarily because there isn't any evidence that we've changed the behaviors of how we build and sustain technology components attached to durable goods that actually impact people's lives. The pattern we've seen is when looking at a technology component is the lifespan is maybe two or three years, and then there is a new component. But if we look at the underlying tangible asset, or the component it's attached to, those appliances have life spans of ten or more years. My own car, a 2011 Ford Explorer no longer receives updates after only a few years, no longer receives updates. I feel I am at risk in that area. It is something that may be fixed by regulation. As we move more into the internet of things, technology components need to be secured for the lifetime of the vehicle or appliance it is attached to. It is a powerful principle to consider here.

The reason I think back to that doomsday scenario is, we have to consider the balance of innovation vs. risk. I think this is an area where we've been able to deal with losses in the past, whether privacy losses, or fiscal losses. Those are things that can be compensated for. But as we start moving into a deeper and deeper dependence on machines that control our lives, keep us alive, safe, and sane, future breaches will be ones that directly impact people's lives in the future. I believe that it will force a reaction on the part of voting populations to see changes in cybersecurity.

Mr. Stamos: The "cyber Pearl Harbor" should be of most concern to those running power grids, hospitals, and others. For the rest of us, we should not let the idea of that one horrible day distract us from the reality that software and the internet are not as safe, usable, and trustworthy as it should be right now. Focusing positively on the day-to-day problems, can have a long-term positive effect.

I'd like to see a change in law enforcement and the intelligence communities away from information sharing as something that enables their eventual mission, which could be enablement of actual action, or enabling law enforcement to be able to make arrests where needed, and have information sharing be the outcome. With the cyber-CISA omnibus bill, one of the reasons it wasn't supported by the technology industry, was that it had a huge focus on law enforcement as being the outcome of information sharing. That is not why IOCs get shared. We share IOCs with each other to make it difficult for attackers to attack, fast response to threats, and reduce economic impacts. The government becoming a clearinghouse that has greater ways and means than ours, to get information on threat actors, and to willingly share, even when they are not part of the outcome. It is still a success if American companies can be immunized against threat actors, even if there are no arrests.

Ms. Prafullchandra: We are pretty good at detection. We struggle with how to share what we have discovered. The areas we should look at going forward, is what are the critical infrastructures in our society? Is Facebook a critical infrastructure? It is used by people to share their current state in an emergency. We need to think some of these digital technologies that have come into widespread use. If something is a critical infrastructure, the government should provide adequate funding for those entities to survive disasters.

We need to think differently about openness and transparency in cybersecurity. For a long time, cybersecurity has been a topic where the perception is sharing cannot occur. We need to be confident in the controls we have in order to be able to share.

Panel 2: Collaborating to Secure the Digital Economy

Thomas Andriola, Vice President & CIO, University of California System
Dr. Cynthia Dwork, Distinguished Scientist, Microsoft Research
Eric Grosse, Vice President, Security Engineering, Google
Eli Sugarman, Cyber Initiative Program Officer, The William and Flora Hewlett Foundation

Thomas Andriola, Vice President & CIO, University of California System

Mr. Andriola speaks from the perspective of being a chief information officer, and trying to protect the university from cyber-attacks. He considers himself in the role of understanding cyber risk. In his role of being a chief information officer, it covers technology in a range of areas from the mundane to keeping the openness of the research environment of a group of research universities, and protecting from attacks.

The University of California (UC) system has ten campuses, educating 240,000 students annually, five medical centers serving fourteen million patients every year, and relationships with three national laboratories. We are in health care, higher education, and research and development, all areas of high activity for cyber-attacks against high value assets. The university also has the talent to look at problems in these domains. The university system has a rich history in dealing with many kinds of problems as society has progressed.

There are challenges for a CIO in the university's openness to maintain exchange of ideas, etc. The nature of the university is such that openness and an atmosphere of collaboration must be nurtured and maintained, while maintaining security at the same time. At same time, there must be balances between openness, privacy and the need for security. These are significant challenges.

The university has many types of assets. It's not just personal identity, but also research data, and other things. Actors may keep information they obtain to act on possibly ten or fifteen years later. It is something the university must consider now. There was a very public attack last year that necessitated a public statement about what might have happened. There is a continuum from an under-appreciation of these risks to an over-reactive sense of urgency, and back to a place where we acknowledge it is a long term problem that needs a long term mindset.

There is a need to understand the level of risk that exists. The university has set up a governance structure that encompasses academic administration, business administration, faculty and technology. Prior to last year's very public event, it was only a technology conversation. It needed to become an institutional risk conversation. The university has adopted some international standards for assessing risk, measuring risk, defining the metrics we want to use, and placing values on assets. All assets are not equal. We are taking advantage of modern technology.

One reason higher education and health care attacks are more visible, is the way the industries are designed. They are more fragmented by nature, which makes them more difficult to protect. Technology has helped with coordinating intelligence sharing across locations. The university is moving away from thinking about campuses as separate locations, and thinking of the university system as a coordinated front. It has created great improvement in defending and responding against attacks. When there is a bad actor, there is visibility at all locations in the system. In an academic environment, or healthcare, where information sharing is natural, it is daunting but we're getting better at it.

The most difficult part is the cultural change. Raising awareness of everyone in the system from top to bottom is a challenge. Students today expect to have greater ability to be able to interact with the university digitally. They expect a trusted environment in which to conduct those transactions. Training programs at the university have helped with student understanding of security. There is information sharing in the university.

The university is a living laboratory of multiple organizations under one umbrella. We are doing a better job of information sharing. Intelligence information sharing is at a certain level today, but there needs to be a greater level of trust across the board. There are too many rules at an organizational level. The university has great relationships with local law enforcement, but it is not seamless. Trust exists during particular incidents, but not after.

We see information sharing as something that can be greatly improved on. It is the seminal challenge of the economy today. How do we think about challenges? How can universities around the country be used as part of the solution? How can we utilize the brilliant minds in security and adjacent fields to solve problems? Information sharing healthcare has grown tremendously in the last 15 years. Policy changes have fostered more exchanges of information. It has pushed everyone to be more innovative. Cybersecurity is not just a game of defense but also developing offensive strategies.

Universities can be at the forefront of offensive strategies in this area. Universities can take the challenge of developing talent for the workforce of tomorrow. Universities can play a big role in long term talent development. Cyber risk and cybersecurity is the new norm. The university has been in CA for a hundred fifty years and has seen evolution from agrarian society to the present time. We are continuing to evolve as an organization. It is a long term game for the university. We must have protection and response strategies, and social research strategies. Preparing the workforce of tomorrow is a crucial part of innovation and growth.

Dr. Cynthia Dwork, Distinguished Scientist, Microsoft Research

Differential privacy is a definition of privacy, together with a collection of supporting algorithmic techniques tailored to privacy-preserving statistical analysis of very large data sets. Differential privacy is a mathematical guarantee that an individual data contributor will not be affected adversely or otherwise by allowing his/her data to be used in any study or analysis no matter what other studies, data sets or information sources are available, now or in the future. At their best, differential privacy algorithms can make 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, which says over-accurate estimates of too many statistics can completely destroy privacy is a mathematical truth. It cannot be circumvented any more than can the laws of physics.

The goal of algorithmic research on differential privacy is to postpone this inevitability for as long as possible. Differential privacy measures and controls privacy loss accumulating over multiple analyses. This signal capability makes it possible to program in a differentially private fashion. In ordinary, non-private computation anything that can be computed, can be computed from multiplication and addition. But, that is not how programmers work. Algorithm design is the creative combination 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 combination of simple differentially private primitives to perform a sophisticated analytical task while also minimizing privacy loss and inaccuracy. As a rule, when the data set is large, the signal dominates the noise injected for privacy.

When the data set is small, this is not the case. This is correct. Think of the case of a data set of size one. To ensure privacy, the noise must dominate the signal. 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 the networked world and perhaps owned by the very companies or government agencies that have employed the adversary and that can be brought to bear in a privacy-protected information system. Differentially private algorithms are future-proof, even against such actors. Differential privacy is the wrong technique for finding a needle in a haystack, or for searching out terrorists.

These techniques are designed to preserve the privacy of everyone, even the needles in the stack. The goal is to solicit participation without fear of repercussion. Indeed, it is often the outliers that need the most protection. Nonetheless, the techniques can have applications in the context of finding bad actors, or patient zeros. First, it can provide the means for finding normal or typical behavior patterns in a privacy-preserving fashion. In other words, it can be used to define the "needles" by contrasting them with normal. Second, the approach can be modified to distinguish between parties for whom privacy is explicitly protected, and a targeted subgroup for whom it is not.

Google uses differential privacy to identify dangerous websites that are popular among Chrome users. Apple has deployed differential privacy in IOS 10 for a variety of data analytics, such as learning new terms for quick-type suggestions. The common factor for 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.
Dr. Dwork closed with three policy recommendations:

1. Publish the epsilons. Differentially private algorithms are equipped with a privacy parameter, usually called "epsilon"; that caps the privacy loss. In a non-private algorithm, epsilon is infinite. By maintaining a registry of privacy loss similar to release registries, we stimulate competition to obtain better analyses at lower privacy costs we engage those who traffic in the data of individuals in the effort to protect the privacy of their subjects.
2. Establish a list of approved private data analysis techniques, and appropriate applications, and keep it current.
3. Consider restraint. In a data rich world, the challenges revolve around the tradeoff between what can be done and acceptance of the fundamental truth that overly accurate estimates of many statistics can destroy privacy. If we are interested in privacy, sometimes restraint might be the right approach.

Eric Grosse, Vice President, Security Engineering, Google

Over the past decade Mr. Grosse has built up a core team of over five hundred experts in security and privacy at Google. They have deployed comprehensive network encryption systems, usable consumer authentication systems, and have observed that they have been successful in stopping even high level actors from hijacking accounts. They have also conducted malware analysis that enables better detection and attribution at a level that not long ago would not have seemed possible. Mr. Grosse recently stepped down from leading that team to work with hardening open source software, to bring it to the same level of capability.

Today, we will talk about two themes. We can all agree a safe internet is good for everyone. We've seen how it has changed from a few dozen trusted machines sitting behind a firewall, to now there are 3 million smart phones added daily with complicated threats happening all the time. There are very complicated trust relationships and evolving threats. At Google, it is important to keep our users protected, but we also believe it is important to use our resources to help others.

Google has tried to lead the discussion of fixing vulnerabilities when they are discovered, and create and implement fixes to prevent further harm. There has been an evolution in the practice of vulnerability reporting from those who find vulnerabilities to those who can make the proper fixes and deploy them in time to minimize harm to users. It is a very challenging problem. We are looking for a way to get the word out without causing harm. Google is prepared to spend significant monetary resources on bug bounty programs. The money spent on those programs is larger than the amount of the bounty checks that get written. It takes many skilled engineers to process incoming reports. Google also does a lot of internal research looking for vulnerabilities.

Google spends a great deal of money investing in vulnerability research. Money is also invested in looking for vulnerabilities in other software. We think the vendor disclosure and repair process is important, and time is of the essence in these cases. Acceleration of the time scale in these cases has improved greatly in the last few years. Governments also have processes to uncover vulnerabilities, and there are processes in place to handle them.

In the first part of 2014, the President's review group on intelligence and communication technologies made a recommendation, and the President pledged to rebalance its assessment regarding favorable disclosure of zero day vulnerabilities to vendors. There are exceptions made for law enforcement and national security purposes. It has not been easy to assess the progress made by the government since 2014 vs what Google has been able to accomplish. Collaboration requires an accumulation of trust over time.

The government is missing an opportunity. The Information Assurance Directorate (IAD) approached Google when Android first came out and made them aware of some flaws within Android. The flaws were fixed. This is the type of relationship we'd like to see more of. These types of things may be happening now, but we don't hear about it happening. If the government is doing it, the government should take public credit for it. It may help cure the lack of trust that poisons the atmosphere today.

In public-private threat sharing, having the full context of the attack has been helpful. The best example, was Rob Joyce's talk at the Enigma Conference. He laid out rules of defense against attacks and what to do against them. His advice went beyond threat indicators, and was very helpful.

In addition to sharing these types of signals, transparency should be emphasized. It is a very important topic. In 2010, Google launched a transparency report that reported requests to Google from various governments around the world to remove or disclose user data. That type of transparency report, now being emulated by other companies, is very healthy as it gives people an understanding what is actually happening. It keeps things out of the shadows. People tend to be either oblivious and make the wrong risk decisions; or they over-exaggerate what the risks to them are. There is still a long way to go. It is helpful to have aggregate numbers, but we would like to see more.

Google has also worked to tell particular users when the government has made a request for their data. There are times when Google is gagged from doing so, and some cases it is easy to understand why. We don't want to tip off criminals who may be a flight risk. However, systemic, indiscriminate, and perpetual use of gag orders is corrosive to trust over time. Providers should be silenced from telling users about requests only when there is a need to do so, and not forever. I would urge the government to be more transparent to those users. This will bring more transparency to laws and bring more confidence in the system.

Eli Sugarman, Cyber Initiative Program Officer, The William and Flora Hewlett Foundation

Mr. Sugarman discussed the role of philanthropy and collaboration in the context of cybersecurity. The William and Flora Hewlett Foundation has made over 5.5 billion dollars in grants in complex policy issues including education, climate change and cybersecurity. The current cyber grant effort started two years ago. It is a five year, sixty-five-million-dollar grant making effort to build a more capable cyber policy field that can offer solutions to the complex problems being discussed today.

Technology alone will not solve the cybersecurity challenges confronting the US and the world at large. As the current debate on encryption highlights, we need smart policy to frame critical choices and manage institutional networks and behaviors that operate in cyberspace. Policies frameworks help solve today's problems. They also help plan for the future. They must look forward and identify where the road we're on is going. So, despite the urgent need for these cybersecurity policy frameworks, universities, think tanks, and non-profits are starved for resources. One might then look to the government to fill the gap, but it may be difficult. Appropriations become difficult in the current political environment, and there are two other reasons the government is not the ideal primary actor.

However, government should be a partner. It is focused on day to day crises and is focused on protecting the nation, and certain classes of enterprises. Senior officials often want to play a longer term role, but often cannot due to the pressing demands of their positions. The government also faces a trust deficit with certain companies and stakeholders located both here in the Silicon Valley and elsewhere. The lack of trust makes it difficult for it to be the sole funder of certain types of policy research. Ideas and frameworks funded solely by the government in those areas would be suspect because of their origin.

Companies are driven by profit and commercial imperative. Some do try to serve the public interest, but are limited in their capability to do so. The private sector does fund some work on the broader internet issue set, often it is linked to government relations and other commercial imperatives. Internet and funding entrepreneurs are largely absent from this funding landscape. It used to be that individuals would spend large sums to support the public interest in order to mitigate the effect on U.S. society from the industrialization that they benefited from financially. Today, there are few leading innovators and entrepreneurs doing something similar and investing in a secure internet. Foundations have played a role in shoring up U.S. security in the past. A private foundation helped the U.S. invest in radar, which ultimately helped to win the war. This illustration points to the fact that there is an alarming gap in our ability to deal with cybersecurity challenges in part because the correct policy framework really does not exist.

There is an important role for foundations, philanthropists, and other donors to step in and collaborate. Many foundations are aware of the importance of cybersecurity but are unsure of what to do. A handful have made tentative beginnings by focusing on human rights and civil liberties issues, others focus on smaller pieces of the whole. The Hewlett Foundation Cyber Initiative is the largest foundation effort in cybersecurity. It is alarming to consider in the context of the need. An additional order of magnitude of funding is needed at a minimum to deal with cyber policy issues.

In conclusion, Mr. Sugarman offered some concrete suggestions:

1. The Commission is uniquely positioned to help the government engage philanthropic funders. It can make clear how acute the need is, what roles foundations can play, share information with foundations so that they can clearly identify risks, and help them identify with whom and how to collaborate. The Commission should be commended on its willingness to engage foundations in this arena.

2. Encourage the government on how to involve the private sector more creatively. Engaging civil society so that it builds trust, and encouraging collaborative effort is needed. It may be outside government's tool box, or its traditional comfort zone but it is needed.
3. There is a need to be transparent. We understand why law enforcement and government are reluctant to be transparent, due to the sensitive nature of their work.

More is still needed to increase transparency and dig into the issues together. The government can also assist with funding. The government can give mandates to the National Science Foundation and others to engage in more multi-disciplinary research in cybersecurity policy, to really make it clear that the technical disciplines and the humanities must be part of the solutions together. Given the way certain government funding is structured, it becomes unnecessarily difficult to make these types of projects happen. It can be one of the goals of the Commission to bring these two different funding streams together.

Panel Two Discussion

Commissioners of the Commission on Enhancing National Cybersecurity

Mr. Sullivan: Differential privacy is exciting. Not many people may say that but not many people really understand it. It excites me because it feels like every company is becoming a data company. Companies are gathering and storing more and more data about their customers to develop insights for targeting advertisements or for other reasons. We're seeing more and more situations around the world where companies are aggregating large data sets about people. It leads to two things – one, people inside organizations are accessing that data in its raw form, and it becomes difficult to have good security.

The second is, governments also want that information once it's been accumulated. One of the solutions we talk about is, as has been in the messaging context is encryption. But in the absence of that context where companies want to have the data because it can add value to the products. It seems like there should be a role for differential privacy getting standardized and broadly adopted in how companies are translating and storing data in ways that is privacy protected for the consumer. Can you speak to that a little more?

Dr. Dwork: Differential privacy is a tool for statistical analysis. It's not necessarily the right tool for storing information that allows some users to be stored in a different fashion from others and personalize that approach. The kinds of things it can do in personalization, is to ensure that the information of one person does not affect how other people's information is treated. As an example, think about a movie recommendation system. If I'm going to recommend movies to you, I can have those recommendations appropriately reflect your tastes. After all there is no need to keep your recommendations private from you. However, the recommendations I make to you should not be affected by anyone else's preferences. That would be an inappropriate spilling of information. Those are the kinds that differential privacy can help with.

It's also the case that the approaches that Google and Apple use inject differential privacy into the data before it is collected. No matter how much anyone investigates that modified data, it will be impossible for anyone to learn anything about individuals who provided that randomized data. There are also techniques that involve processing data and then destroying it. It involves maintaining some local state of information that measures statistical state that represents statistical properties without actually keeping raw data around. Does this help at all?

Mr. Sullivan: Where do you see it developing next, and becoming something that's adopted only by a couple leading companies?

Dr. Dwork: There are several projects working on particular sets of usage scenarios sharing a common theme, such as statistical analysis of social research data, for example. They are developing libraries for carrying out analyses for research being done in that field. Harvard is carrying out one such study in this area. Scientists, statisticians, legal experts, and social scientists would be able to work together. A long term library would evolve to include a collection of scenarios or settings.

Mr. Sullivan: There have been challenges in collaborating with academia, but conflicts exist in the self-imposed data collection rules. There have been cases where data limitations created shortcomings in research, and prevented full utilization of research and talent in research settings. It was unfortunate that academia was not really able to work with companies to really get a profound result.

Dr. Dwork: That would be a perfect setting for differential privacy. The data could be made available in a differentially private fashion. There would then be certainty the data is correct. When I spoke about libraries being constructed of various topic-specific unit, there would be one that would be specific to the type of online auctions people are interested in carrying out.

Mr. Sullivan: *[to Mr. Grosse]* You mentioned you spend a lot of your time working on hardening open source. I think we've seen a lot of really interesting work and investment through things like analytic foundation efforts, or what you've been doing at Google. What role do you see the government playing in getting involved and helping push this work forward?

Mr. Grosse: One way Google has tried to help in the open source world, is that Google extended the bug bounty program to include open source. But not in the obvious way, by just sending a check if a real vulnerability was reported. My sense was that since open source is done by volunteers, and it was unfair to impose the same time constraints on volunteers. We re-structured the bug bounty program in that area so that whenever a bug is found, fixed, and verified, then a check is sent. It has not really taken off as yet. It is something that government could have been funding, because all of us use open source widely in our systems including the government. It might be one more concrete thing the government could do - put more attention and money into programs of that type.

The government has a people with unique understandings of where the vulnerabilities in the world and where they are. Some must be classified, of necessity, but others could be shared with the people would are in positions to fix vulnerabilities. We encourage information sharing, not only with software vendors but also with the open source community to fix these problems.

Mr. Sullivan: One last question on a different problem. One of the things in the Commission's mandate is to focus on defense. I was excited about that, and then the DNC stories from the last week reminded me, there are frequently situations where nation-state conflicts spill over into private systems. It raised the question of what should the government be doing to secure private systems. To some extent the entire digital economy is critical infrastructure (CI) and that's possibly just semantics. What role should the government have in helping private enterprise have a minimum of security?

Mr. Grosse: A couple of interesting points there. I have modest expectations of what the government should do to raise the security of the private sector. It's a huge problem, and probably the best thing the government can do is set a better example itself. It doesn't involve a lot of collaboration; it doesn't involve any risk of companies feeling over-regulated. If the government sets a really good example, and talks about that good example, that would be a healthy start.

I believe the role of the private sector is not to go on offense. This "hack-back" stuff is a bad idea. Vigilantes over the years have caused a lot more harm than good. The offensive role should be played by the government, and the responsibility should stay there. On the other hand, we can't have an effective defense, without running offense against ourselves. Defenses can get trained against our own offenses. Simulations can be an effective means of doing this. Red teams will need to be supervised. There needs to be a defined set of rules, to call the exercise at the right time. There needs to be follow up to these activities, and commit the resources to do what is necessary. Then there is a report, and the defense does nothing with the information. Often years later, the same methods work that would have been thwarted if report findings had been followed up on.

Ms. Wilderotter: I want to ask Mr. Andriola and Mr. Sugarman book-end questions on collaboration. You are involved in one of the largest education systems in the world. You also have a feeder education system called the Community Colleges System here in California. You are also in the heartbeat of technology and innovation all around you, especially here on this campus. Are there things you could be doing with the two school systems to really drive workforce development in this area? There is a shortage in this area. Are there policy incentives the government could put in place that would allow you to do more of that?

Mr. Andriola: The answer is yes, and we are just starting to talk about it. We can use policy incentives from either the state or federal government to help us to do that. When we look at the combined population of the three segments, let's not leave out the population of the Cal State system. There are approximately 2.5 million students from all different backgrounds, not just traditional aged learners and the opportunity to create awareness and an evolving workforce to address this challenge. We are in conversations now to bring this into the forefront on our campuses. Having dedicated programs would be most helpful.

Ms. Wilderotter: It would be interesting if for transfers into the UC system from the community colleges, there were some requirements for a computer science or network engineering degrees so that classes can be taken prior to students arriving on campus.

Mr. Andriola: The outcome doesn't always have to be a degree. Certificate-based programs can be used to get people into early positions in cybersecurity. These positions are also well paid, even at early experience levels. This can also be part of the workforce development initiatives.

Ms. Wilderotter: *[To Mr. Sugarman]* The concept of philanthropic funders is very interesting in the whole area of cybersecurity. Has the Hewlett Foundation thought at all about reaching out to other foundations to work collectively, and is there some government accelerator that can be put in place to help encourage it?

Mr. Sugarman: It is a great idea, and yes, The Hewlett Foundation is actively engaged with other foundations to try to show them the salience of these issues, and concrete opportunities to make a difference with funding to fill gaps in the workforce. It depends on where one is trying to address needs. We are also talking to parties in Washington to utilize other messaging platforms and pulpits to call upon other philanthropies.

We feel called upon to be one of the voices saying we're doing this and here is the impact we're trying to achieve. We, of course, need more resources. One of the challenges is every foundation and government agency has reasons for doing what it's doing. It takes time to create convincing arguments. It takes time to get to know individual institutions, because there is no one size fits all solution. It is very individualized. There have been a few instances where we have been able to bring in other funders to partner on grants to specific grantees. We are thinking about how to make it scalable.

Ms. Wilderotter: Is there anything the government can do from a tax incentive perspective?

Mr. Sugarman: It highlights this area and makes it a call to action. In the past, the White House and others have highlighted policy challenges that are a national imperative and called on everyone in society, and particularly called out foundations asking for assistance. This is one way.

A second way is to helping to educate funders. These are complex issues. For foundation funders who are used to funding in a different area, the complexity can feel daunting. Information sharing in this area can assist. Giving examples of areas where specific funding is needed can be a big help. Education for foundations is worthwhile. Brokering relationships is also worthwhile. It can be fruitful to renew relationships in this area.

Mr. Alexander: Mr. Stamos talked about Facebook having 1.65 billion users. Contrast that to the population of the United States being about 300 million people, it's apparent that 80 percent of Facebook users are outside the U.S. Yet, the discussion we principally have about collaboration is set as U.S.-entity to U.S.-entity, when it seems what we really need to set is, how does the United States help create an international set of engagements on how we share here and abroad for companies that are global.

We can start the discussion here, but our government and this industry must work together to set this framework. I'm interested in your thoughts on how we should go about doing that nationally, and internationally, to help solve this problem that increasingly has become more difficult for commercial entities and our government. Any thoughts?

Mr. Grosse: When we talk about collaborating with government, we need to remember more than half of our users are outside the United States and that we must be even handed in our treatment of them. We are looking for collaborations on a basis where everyone who agrees to play by a certain set of rules has a seat at the table. It should not be politically motivated.

The US government has a lot of relationships internationally, and is in a better position than private companies typically are to handle these matters. There should be some recognition of legitimacy from people around the world. However, there are sovereignty issues. It is difficult for us really understand what other government sensitivities may really be. We have tried to help with the

Mutual Legal Assistance Treaty (MLAT) reform. This is one of the hot items, when we talk about public-private relationships.

Law enforcement is one of the places where it gets to be the hottest issue. If you think it's difficult for U.S. law enforcement to get what it wants when it wants, law enforcement outside the U.S. has a much more difficult time. Google has tried to assist with improvement to the MLAT process with some success. More improvement is needed. To go beyond law enforcement relationships to a broader sense of security, is a tremendously important topic.

Mr. Alexander: It seems that everyone has a different standard for what's private. Some countries say an IP address is private. Sharing IP addresses of attackers can raise privacy issues. There needs to be a standard to define what can and should be shared for government and industry, national and international, and either proscribe a path to such a working group or move that along. NATO recently declared cyber as a situational domain. It presupposes everyone has the same definition of what is going to be done in that domain.

Our government can't do it without industry support, and shouldn't without international support. The real issue is how do government and industry start this discussion in a more reasoned way to help move it forward with the best intentions.

The internet is now truly global. We need to understand how that happened. It seems to make the most sense to frame this in terms of economic growth around the world. There is another piece that needs to be mentioned. It seems at times to be a protectionist move, vs a civil liberties and privacy move. The playing field needs to be leveled by setting the framework correctly.

The biggest threats against the healthcare industry seem this year to be ransomware. It is the balancing test of investing to protect information vs how much we are willing to invest to protect assets. We make sure we know where our valuable assets are, how we protect them. We are not sure there is anything government can do, that it is not doing today. It is a serious issue.

Mr. Grosse: There are several research projects going on working on an international, multi-stakeholder approach. One of them is the Internet and Jurisdiction project. It is an international non-profit based in Paris. It is trying together the main corporate partners, governments in Europe and the United States, and the developing world. They are trying to identify use cases to share information between governments and companies while respecting constitutions and laws. It is an effort in its early stages and goes with academic research going on.

Ms. Murren: The discussion today points up the power a multi-disciplinary approach could have to solve some of these problems. There is a unique role that research universities and university-affiliated research centers can play in convening the government, the private sector, and philanthropy. What are the barriers to expanding collaborative efforts in these areas? Privacy may be one of the concerns slowing collaboration in these areas. Other things include concerns about intellectual property rights and conflicts of interest that may exist with multiple parties working in the same area. Also, how can we identify work going on in other fields, while not technical, that may have applicability here.

Mr. Sugarman: Based on what I've seen at the foundation, in looking at universities and what we fund and why, and what are some of the barriers to their success, privacy is an issue. Good data, for whatever reason it is not shared, is often not available to academic researchers who are trying to connect it to policy frameworks. Representatives from companies may be better able to explain how to be more open with that information.

Government has started to see more openness, and acknowledgement it is the only one with certain types of information. It has been more willing to release some information in without compromising security. It is an ongoing challenge. It requires academics to seek out friends and experts and look outside their particular discipline. Attempts to bridge disciplines are often frowned upon. The Foundation seeks to fund those efforts that involve multi-disciplinary work.

Mr. Andriola: The research universities are getting better at multi-disciplinary research. It is being pushed by the philanthropic community, and government funding agencies are more interested in multi-disciplinary work. The trend for the university is it is a necessity to become better at it. There are many examples on the university's campuses where multi-disciplinary research is how to get ahead. The big societal problems are solved through multi-disciplinary initiatives. More multi-disciplinary research in the future will be key to solving the big problems that society faces.

Ms. Murren: *[to Mr. Sugarman]* You talked about ways to unlock data. Privacy-preserving data analysis is exactly what that's all about. When we're talking about what role the government can play, investing more research in building the tools, and investing in educating people not only to develop the technology, but also to use the technology. People who have experience analyzing data have methods they use, and procedures they follow. When they now have to interact with the data through a privacy-preserving interface, it can be very challenging and disconcerting. There is now a fair amount of movement in the statistics community toward embracing these technologies, but it is slow. People need to be educated in how to use it and how to build it.

Mr. Sugarman: It is fair that multi-disciplinary research is becoming more mainstream. However, it remains a luxury of mid-career and more senior faculty members. For junior faculty members, PhD students, and post-doctorates, it is very difficult to engage in multi-disciplinary research because there are no jobs available at those levels. There are very few, if any, junior faculty jobs at leading research universities that entail research in cybersecurity.

Where can research in cybersecurity be published? There are two journals only just established in the last year. They are not well known yet because they are new. It is worth noting that the government can bridge the gap between the up and coming experts and getting them into a career trajectory that allows them to move up the ladder and ultimately become the department heads. They will be able to ensure multi-disciplinary research becomes inculcated from day one.

Ms. Murren: There are some interesting points being raised here on solving the problem. It may be worth exploring reframing the issue to incorporate the human element more effectively, then the philanthropic community and the messaging from foundations, to people that can participate in funding would start to expand dramatically. There might then be more interest from that part of the potential funding universe.

Mr. Gallagher: We've been talking about collaboration and the areas of collaboration mentioned today: research, policy, threat mitigation and detection. Have we forgotten any areas of collaboration? We have not discussed response and recovery. That is usually a very broad area of collaboration. Is there a "cyber Red Cross" opportunity that we may be missing?

Ms. Murren: One area in the private data analysis setting that comes up is eventually the data can no longer be used, or reduce its utility. Collaboration in deciding the questions to be investigated in the data so that as many people can get as much benefit from it as possible before its utility runs out is necessary.

Mr. Gallagher: The tricky thing for the government to consider regarding collaboration on incident response is a perception in the private sector that if the government comes in, it is adding collateral damage on top of dealing with aftermath of an incident. The problem for the government right now in order to be able to participate more is getting rid of the history. In aviation there are good safety reporting systems that avoid that damage. It takes the bad things revealed in the information it receives without blaming, and tries to make something better out of it. The cyber world needs some sort of similar mechanism. In previous workshops when this was discussed, it foundered because there were classified elements involved. Trust has not been able to evolve in that environment. We have not been able to find a way to go forward from that past.

Mr. Andriola: The word collaboration has been thrown out a lot today. In the community at the University of California, there are two words that go with the word "collaboration". One is "trust", and the other is "interdependency". We can trust each other, but if we don't have something in common, a shared goal or objective, collaboration doesn't need to happen. Whether in the policy framework or in the incentive programs or funding, create the interdependency we need around collaboration. If there is greater interdependency for people to work together, and there are incentives to do it, the collaboration will happen. The Commission can think about creating interdependency around these issues, and the incentives are there. Trust plus interdependency leads to better collaboration.

Ms. Anton: Universities are struggling with how open the university network is, with the thousands of faculty and researchers who use the network in a variety of ways, without them ever having been taught to deal with privacy and security. There are number of empirical studies taking place on campuses where they receive IRB approval without any real understanding what it means to secure the data, or what it means to preserve the privacy of sensitive data. We are not sure where those conversations need to take place. We have a huge university system. Where should those conversations take place? Companies do empirical studies. They have IRBs. Are there a set of best practices that should be shared across the nation for protecting sensitive data?

Mr. Andriola: When firewalls first came in, students and universities could not use firewalls because they needed to do research. Graduate students needed to have their machines directly on the internet to do experiments. We have moved past this fortunately, or perhaps unfortunately. We now assume all our networks are compromised, or malicious even behind the firewall.

There is not as big a gap now in companies as existed ten or fifteen years ago. We assume when someone comes into Google and plugs into the wall, there is no access to anything. It's like plugging into the internet anywhere in a coffee shop. We don't see the problem we used to see. We've given up trying to solve the security problem at the network level. Now, endpoints need to defend themselves from a hostile network. That means the university can run its operation at the same level as we are.

Ms. Anton: I'm not sure that's at all comforting. What then is an ethical practice? If we expect our universities to train the future workforce in America, and the people are doing research at our universities don't know how to protect our information or don't even think about the fact there's a potential for the data they're collecting. Which can be extremely sensitive at times. They are oblivious to the consequences of that. I think we're talking about a broader conversation about that and who is ultimately responsible.

Mr. Andriola: There is a journey we're on. I won't say we're perfect. We had the crisis that was the opportunity for us to elevate this conversation. There are certainly mistakes along the way. It starts with having a multi-disciplinary conversation. We've defined this as the academic and business administrations, direct faculty members, because they are the ones who influence this problem not the administration, and the IT community. The IT community is so happy when I make the statement, I talk IT last. The fact we create those conversations, and we hash through very difficult conversations about how to weigh risk, and balancing risk, and how we balance privacy against protection. It is a very robust dialog that happens at each campus. There is a cyber risk executive at each location who is responsible to the chancellor for that topic. The CIO really owns and drives the conversation locally.

I was in a cross-functional meeting with faculty and other members of the administration, and one of the faculty members said, he got an email from the library document repository, and he wondered if it was fake. It means we made a little progress, so it was momentum for us to keep going.

Ms. Anton: What recommendation would you have for the Commission in terms of what we can do to make a difference nationally? Some universities have hospitals, some don't. There are many varying levels of security around the country.

Mr. Andriola: The report should deal with the economy at large. There doesn't need to be anything specifically dealing with universities and medical centers. When we talk about networks and open access, we're not that different than we were fifteen years ago.

Dr. Dwork: Aside from the security questions, there are questions about how the data are used and how they are treated. I think there is an enormous need for education along these lines. If we are going to be training people who handle lots of data, there are things they need to know that are not covered in a standard security class. The IRBs present a very delicate point here. One would not expect amateurs to roll their own encryption schemes. So, why would we expect them to understand the subtleties of working with data?

Mr. Lee: In listening to the discussion and the many references to workforce development and education. It strikes me that policy makers and legislators need education too. There is a famous course still taught at Berkeley on physics for future presidents. It involves the physics a policy maker or a president need to know. There might need to be a cybersecurity course for future presidents.

Mr Sugarman: Several of the universities we support, including Berkeley and Stanford in particular, have tried to create boot camps, and training modules targeted at decision makers in and out of government. It is a huge priority, and as more universities start to do that we will start to see modular curricula available online and some great resources. There are courses on cryptography at Stanford. The University of Maryland just did a boot camp for journalists and newspaper editors to educate them because they play a key role in the policy debate. It is a great area where the Commission can call on universities. There is an appetite from policy makers for that training. There are several efforts underway to train congressional staff and members of Congress. It is hard to make sound policy without an understanding the technical and non-technical dimensions of an issue.

Ms. Todt: One of the tasks of the Commission is to formulate an R&D agenda. There has one that was created by the government, but focusing on collaboration. As a follow on to the points made by Ms. Murren and Mr. Gallagher, one of the reasons we have asked the four of you here is because you represent these sectors that when collaborative, what could we produce? What would you identify as priorities across these entities for the Commission to put forth as a recommendation and an action?

Mr. Sugarman: I think it's tough to prioritize because of the challenges here. On the educational front, we are trying to think about how to empower multi-disciplinary research and engage and provide the data and the experts, and all the connectivity there that is really required to generate relevant research. We are talking about real world challenges here, and that means we don't want to entrust academics to always toil away without having a conversation with those on the front lines about what to research. Having more of that conversation about how the Commission can frame the key tasks, and then the universities can really go after the research is a priority.

Another priority is rebuilding trust. Lack of trust has been an impediment to collaboration. Focusing on the trust piece, and focusing on citizens, companies and government. There needs to be more sophisticated conversations. Creativity can be applied here to find new ways to approach this issue.

Mr. Grosse: My top priority would have to be setting time bounds on gag orders. If we don't get that, we will not earn the trust of users domestically or worldwide. It is the most important thing I would ask of government.

Dr. Dwork: My top priority would be trying to expose what is being done with data, why, how often, where and by whom, both in research and in industry.

Mr. Andriola: I would say my top two would be how we move from university sponsored research into applied research, and then, this gets to the immense nature of this challenge: How we build agility in the ecosystem. Five years from now things will be different than they are today.

Panel 3: Innovating to Secure the Future of the Digital Economy

Gilman Louie, Partner, Alsop Louie Partners, former CEO, In-Q-Tel
Mark McLaughlin, Chair, National Security Telecommunications Advisory Committee (NSTAC); Chairman, President and CEO, Palo Alto Networks
Ted Schlein, Managing Partner, Kleiner Perkins Caufield & Byers (KPCB)

Gilman Louie, Partner, Alsop Louie Partners, former CEO, In-Q-Tel

Before there can be innovation, the right mental framework must exist for cybersecurity. We have either looked at cybersecurity either as an opportunity, or in a national security advisor capacity. Those mindsets at the extremes of the spectrum are the wrong mindsets. It focuses us on a very domestic series of solutions. However, the internet is not a domestic thing. There cannot be cybersecurity of any framework without international cooperation. It is not us vs. another nation-state, but focuses on the ability of other nation-states to have a common interest, to understand that cyberspace should be treated like any other resource. It impacts commerce, life and safety, critical infrastructure, the ability for nation-states and corporations and individuals.

The challenge is that there are many different points of view about what the future looks like. Privacy, definitions of what constitutes a national security issue, and what constitutes criminal activity all fall into this mix. There are many debates on these topics. Companies are left to guess what the future looks likes.

There is a common misbelief that an entrepreneur based in venture capital operates at internet speeds. But the reality is that it takes five or ten years to build a great enterprise. We're not investing to solve today's problems; we're investing to solve problems we project out five to ten years from now. Understanding the policy framework, and what the international view looks like, and the policy view are critical to making things happen.

There are a couple of important things to think about regarding innovation: First, innovation starts from a strong R&D base. If we look at previous studies in this area, all the people who study these things point to the fact that we need a national R&D agenda. There have been a couple attempts to create such an agenda. Historically, they have been underfunded and uncoordinated. Everyone has "cyber" in their name today. The word "cyber" has been hijacked, particularly in R&D circles, into a way to keep doing the same things. This will not work.

Many recommendations have been made on how to do this. It is critical for an R&D agenda to be based on a view of tomorrow's problems and consider what the world might look like in that tomorrow. It then can back into, what should our national priorities be that are shared common interests with other nation-states. This separates are military and intelligence activities from what we need to do to make it a safer and more secure place for operators to actually live in.

In speaking with some attendees prior to the meeting today about the idea that perimeters are really where defense should happen. The internet was designed to be unreliable and unprotected and the internet figures it out. IP addresses and packet routing get to the right place, and it doesn't matter how messy it gets in the middle. Today, given what has happened particularly in the last month, it's like telling everyone in the physical world that everyone should have guns and armored vests. Nothing else is needed in the middle. It is ludicrous to think we should live like we are in the wild, wild, west. Yet, this is the way scientists and policy makers assume things should be. Other nation-states use various strategies to protect their populations from the internet. Some of them are very, very dangerous. The Chinese strategy is to have the master kill switch and create an alternative to the internet. It creates a vulcanization of the internet.

If nation-states try to take control over their little piece of what they think their internet should be, this global resource gets broken up into these little pockets of nation-state advantages. We will not be able to operate in such an environment, much less have commerce. All the things we worry about, trade protection and barriers, go away in this vulcanization model where every rule is different and every company that plugs into the net has to figure out what that matrix looks like. It is an impossibility. This Commission is very important. It is very important because we need to reframe the discussion. We need to clearly state and figure out activities and clearly organize those activities around responsible nation-states to clean the mess up. We're not in it alone.

Second, there are great federal agencies that are all trying to do the best job they know how to do. The reality is, the agencies we have chosen are not necessarily the right agencies to lead the charge if we want to have the United States be a trusted provider of technologies to make the internet safe. It should not be military or law enforcement agencies, but we should not use a strategy that says we're here to protect, but we're also here to break in. There is great expertise in those agencies, but they are the wrong choice for international engagement. We need to rethink how we think about lead agencies. We need to reframe commercial activities and the importance of information sharing in such a way that companies are incentivized and to remove the disincentives for sharing information.

Major financial institutions in the U.S. asked Mr. Louie to remove the cybersecurity check box because they do not want to have a reportable event. There are local, state, and federal rules that step on top of each other aiming at different objectives. We don't want to know too much. We don't want to have to report to shareholders, state attorneys-general or the federal government.

Everyone is in it for themselves, and everyone is incapable of protecting themselves.
On the R&D front, there are great universities with great research grants. However, a more coordinated effort is required if we really want to put out a research agenda that is going to move the needle which starts the talent pool that enterprise can tap into, and finally move the ball forward. When we see hundreds of cybersecurity start-ups all pitching the same thing. This week it's "orchestration", but it's the same stuff, just renamed. We need to think about what the power of big machines can do against the cybersecurity threats we have.

Finally, the most important thing is to have international engagement. We might not get global agreement, but without bilateral agreements from allies on key issues, there is no hope of agreement across the board. We cannot bury critical cyber-issues, and big trade agreements that stand no chance of passing. The issues need to be separated from each other, and engage, and give this all our energy and focus. What the Commission writes about this will set the agenda going forward.

Mark McLaughlin, Chair, National Security Telecommunications Advisory Committee (NSTAC); Chairman, President and CEO, Palo Alto Networks

It's important for us all to be focused on innovation to reverse the current dynamic in cyberspace where increasingly automated adversaries are dramatically outpacing what is increasingly manual defense.

If we want to regain leverage here against our adversaries, and try to reverse the unsustainable dynamic that we're facing today, I think we have to ensure that innovation is happening and innovative technologies are meant to operate together in very automated fashion within a big ecosystem and at the same time, do a lot more education for everyone starting with our kids, and also with highly refined processes from today.

So if I think generally about the cyber threat landscape, I want to talk about how we can collaboratively innovate to restore the trust in the digital age that comes more and more into question every time we see a successful breach or cyber-attack. As this Commission knows full well increasingly frequent and sophisticated attacks are leading some to question whether the technological foundation on which we're building our future of smart homes and self-driving cars is the new global digital economy may have some very deep structural flaws.

This is ultimately just a matter of trust. More and more we're living in the digital age which is fundamental I think for gross domestic product growth on a global basis. We're all relying on that. From retail transactions, to the operation of the financial system to the generation and transmission of electricity, these are increasingly interconnected through the internet and only really exist any longer as bits and bytes and there's not a lot of physical stuff left. That digital age is bringing an enormous amount of productivity increases in all these areas. However, it also brings new challenges and vulnerabilities. I think business, government, and military leaders know there is a very fine line separating the smoothly functioning digital society that's built on trust, and chaos.

At the heart of the cybersecurity battle, ultimately it is a math problem and one that's pretty easy to understand but challenging to correct. Unfortunately, today the math problem overwhelmingly favors the adversary. That's simply because the cost of compute power required for malicious actors to launch successful cyber-attacks has been decreasing dramatically for decades. I think we should assume that will be the case for the rest of our lives.

Couple that with widespread availability of black market malware, our adversaries are increasingly able to conduct automated successful attacks at decreasing to almost no cost. In the face of that automated onslaught, network defenders are generally relying on decades old technologies often cobbled together as multiple layers of point products. None of which are really designed to work together or communicate together, and that lack of automation and interoperability has become increasingly problematic as networks continue to grow in complexity.

This is only getting harder with virtualization, SaaS, cloud mobility, and the internet of things which were mentioned earlier. That increased complexity of enterprise architecture and independent security controls really create a dependence on one of the least scalable resources that any organization has, and that's people. We're doing a lot of manual fighting against a highly automated, machine generated attacker. As a result, we're simply losing on the economics of the cybersecurity problem. So, how do we how do we change that paradigm today?

Innovative approaches effectively applied to people, processes, and technology are one of the key principles in trying to drive a stronger prevention orientation. We can establish security as the default and try to regain some leverage against our adversaries. Prevention, ultimately, is about significantly decreasing the likelihood and increasing the cost for an attack.

We should not assume that attacks are going to go away, or that they're going to be stopped. They won't be. However, we should assume and be very diligent ensuring that the cost of a successful attack can be dramatically increased to the point where the likelihood of a successful attack will decline over time. If we're going to maintain our trust in the digital infrastructure and restore the loss, we have to focus on getting leverage from the attackers to make it more expensive in terms of resources, time, and personal impact, to launch successful attacks.

That leverage can be built into a few categories of innovation principles, and as you focus on innovation with the Commission as a means to enhance our security, I would recommend establishing a clear definition of what constitutes an innovator, applied to the following categories:

1. The first is technology. Innovators have to develop technologies that work seamlessly to enhance the security of individuals, enterprises, and a broader ecosystem. In other words, cybersecurity innovation in isolation is inherently less effective because a single technology that's built to solve one discrete problem does not solve what has to happen in a highly automated environment, where networks are at stake.

   Simplification and automation are essential for making networks adequately defensible. Security technologies must be used as part of native platforms capable of automatic reprogramming based on new threat information, to prevent threats across all points of an attack lifecycle. It includes on the network, in the cloud, and at endpoints. The capability to deploy these preventive countermeasures automatically has to be consistent as well, no matter where data may reside. It could be in a data center, perimeter, at an endpoint, on a cloud, a public environment, cloud environment, private cloud environment, it really doesn't matter. What matters is, it has to be consistent.

   Innovators also have understood that security technologies need to be fully integrated as part of a larger global ecosystem. More specifically, the innovators should work within the ecosystem to utilize information sharing, leverage open source integration APIs, and develop interoperable technologies capable of high automation, including through partnerships with complementary technologies from other third party companies, including their competitors.
2. Innovators must recognize that technology is not going to solve everything. However, if we're not also educating our people and executing processes in the right way we're still going to have a problem. We have to double down on increasing cyber-awareness and education for employees, for our children, ourselves, or anybody we have responsibility for, so we can reduce human vulnerabilities and ensure we’re good on the next generation of cyber savvy citizens.

I would recommend educating children at the earliest possible age, so that cybersecurity is fundamental. They really don't realize the value of their information and what people are going to do to take it from them. That's just going to get worse and worse from a generational perspective.

Hands-on training with innovative security technologies being engrained in educational curriculum, is something that I would recommend. We have to leverage innovative technologies like long distance virtualized learning to educate more people and do it faster.

The space, unfortunately, is very uncertain as we forward. What's clear, is we can expect really radical changes in our digital lives in the not too distant future. Technologies that are currently breaking new ground or just over the rise, like big data analytics, quantum computing, artificial intelligence, virtual reality, very global Internet, digital money, and nano-scale computing are going to shape our world in the next three to five years at the outside in ways it's hard to imagine, and will definitely increase the complexity of the security challenges we face today. It's going to get going to get worse before it gets better. Keeping in mind a few network defender design principles are going to help us navigate that world, and would be something that I highly recommend.

Ted Schlein, Managing Partner, Kleiner Perkins Caufield & Byers (KPCB)

While I'm here today as managing partner of Kleiner Perkins, the views I'm representing are my own, based on over thirty years of working in the cybersecurity industry.

It's my view that the management of technology risks, in particular cybersecurity, has become critical to our increasingly digitized and connected society and economy. It's imperative for both national and international security and there will continue to ever be more a foundational requirement in other domains. I have five areas I'd like to discuss, with recommendations that I ask you to consider

My first recommendations are in the area of the measurement of corporate cyber risk. As we know in business, if we don't measure a program or a person, we never really know how we're doing versus our goals. I think the country should consider creating a risk preparedness index, or an RPI. It systematically measures the people, processes, policy, and technology configurations by each critical infrastructure sector of our country. This can be accomplished by using a NIST-based standard for each sector, and creating an independent entity that issues ratings much like Standards and Poor, or Moody's does for bonds. We would assign every commercial company an RPI score. These would be publicly available, and the belief is that consumer awareness will drive the necessary behaviors by corporate entities to increase the risk preparedness that's appropriate for their industry sector.

Public companies are also increasingly understanding risk, and thus forced to deal with their company's cyber posture. We should consider the 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. There should be at least a requirement that some subset of the board needs to be briefed on the company's security requirements and deficiencies on a quarterly basis. Finally, I believe that it should be required to report a security breach and all the necessary information about that breach. Who any entity reports this information to and how it's handled are going to govern in a future section.

Over the next decade, I believe some of the most defining issues that we're going to face as a nation are how we evolve our approach to dealing with cyber-attacks in both the private and public sectors. 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'd like to propose a series of changes we make to our national security apparatus. We need to put in one place an 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 the U.S. Cyber Command from the NSA and using it to create a combined U.S. cyber command that includes the FBI, the 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 the Secretary of Defense, with additional reporting to both the FBI and the DHS. I realize that the authorities of these various entities are quite different and that's going to 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 U.S. This agency would be at the disposal of the DOD for offensive purposes, FBI for domestic law enforcement issues, and DHS for the protection of private U.S. industry. In the case where this has international implications, these actions would need to be coordinated with the DOD. It would be the main interface with our international allies on cyber-issues as I could see a cyber NATO forthcoming.

We must recognize 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 through this agency to establish a place for 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, it could be very helpful to this cause if harnessed properly. By creating this agency, we get our best talent working on our hardest issues overlaid with the appropriate laws for each group's actions.

It will also be a great advisor to Congress about future policy changes that should be debated and decided. Because you’ll have defense and offense, national and international, all represented in one place, you'll get an actual representation of what we deal with from a cybersecurity perspective as a country and also by private industry and how to update in real time circumstances. Like many I believe our best defense is going to be a good offense.

The FBI and the DHS sector of this group would be responsible for helping private industry fight back if needed, authorized, and warranted. This is 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. Continuing to hone our ability to get better and better attribution for attacks against both the private and public sector is inherent for this capability to function. This will be a key ingredient for deterrence as well as for deciding on a 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 education system in the country to produce more cyber-aware and trained graduates. In fact, we should put out the challenge that we want twenty-five to fifty thousand new cybersecurity graduates per year. This means students cannot be a computer science graduate unless they understand secure coding. Students cannot be network design graduates unless they understand secure network design and architecture, etc.

In order to effect this, the government will pay for any student who decides on the appropriate major, as long as when they graduate they work for at least four 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 desperately need. We have a dilution of expertise 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 that will only increase over time.

The federal government should be using its purchasing power to bring about 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 be used to promote safer computing. I propose that the federal government not allow the purchase of any 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 in turn benefits all customers. Further, no internally developed software by a government agency will be allowed to be deployed if it has not undergone a secure could audit, and is signed off on by the appropriate a chief information security officer. Finally, in this area, the federal acquisition rules covering purchasing and point of security technology should be reviewed for streamlining purposes so that our frontline agencies are able to deploy state of the art capabilities at a pace that is relevant to the demand of cyberspace, and not the confines of the physical domain.

One thing bears mentioning about the potential concerns with the evolving legal landscape due to cybersecurity breaches. Class action lawsuits aimed at private enterprises for not being able to defend themselves against a cyber-attack by a foreign nation-state are completely 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.

Finally, regarding combating 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 a living room, and make a few million dollars by lunchtime. It's 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 both a mix of technology and policy changes. We need a call for international cooperation to combat ransomware and cyber-extortion. Any country that harbors 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.

Panel Three Discussion

Mr. Sullivan: I noticed one kind of conflict in ideas is the right way to frame it. Mr. Louie posited the idea that the current agencies involved in cyber are not the right agencies to enable trusted technology, is a little bit inconsistent with the idea of unifying everything under a cyber command.

This is something I've also been thinking about because in the private sector, when something bad happens, there are two thoughts: One, who can help right now; and two, who can help prevent this from happening. Currently, there aren't any government agencies out there that are performing either function well. So, how does one think more deeply about the kind of conflict between these two approaches of creating a trusted technology organization that's separated from the attack world, versus putting it all together just so there can be one set of smart people in one place?

Mr. Louie: First of all, whichever approach we use, it's not going be easy, starting with framing cyber as an international resource, and cybersecurity as an international dilemma and crisis. That must be the starting point because if we don't start there we can't feel good about a domestic solution. It would be very difficult to implement at a global level without everybody going for what is in their best interests.

If each nation-state goes for what's in their best interests, we will not affect the changes that we need. It doesn't mean that we shouldn't have a coordinated military capability to deal with adversaries that are using military nation-state resources against us. If a nation-state moves on our critical infrastructure, it is clearly a military issue. If a nation-state’s military moves on our commerce, it is also a military issue for the United States. The same is true for law enforcement.

The challenge lies in a world where everybody's dependent upon everybody else's pieces of equipment and little bits of chips and software that protects the world. There needs to be a foundation of trust. There is a reason why the words in my write-up were chosen as they were. Cybersecurity is a quality of service issue; we need to think about it that way. Yes, it has critical military implications, and it has criminal and law enforcement implications. However, if our first goal is to make the internet clean to allow for faster communications or lower latency, more trusted communications and transactions, and to be able to actually trust a block of code or an information stream that controls a physical device like a car, an airplane, the power grid, or a nuclear reactor; we need to make that quality of service high, not just for the U.S. but for everybody.

Here's a set of framings to think about: Nation-states should not pass rules for its companies doing business internationally that they would not want other nation-states to pass for doing business internationally. As Mr. Schlein has stated, we see the same sorts of gaps that we have around federal agencies. It's really hard to risk sharing information with federal law enforcement, if later they can come back and have the power of arrest.

It is very difficult to share your global technologies with the National Security Agency to make sure that those vulnerabilities are sealed, if potentially they're being exploited for nation-state advantage. It is very difficult to share information with law enforcement on the legal framework in the United States and not do the same thing with another nation-state which may not be an American ally.

All these agencies have a role. However, the organizing agency designated to protect this global resource needs to be non-military, non-law enforcement, and needs to focus on the global quality of service and the trust necessary to allow the Internet to function for the global economy to boost productivity and to move nation states forward.

Mr. Schlein: I'm not convinced that Mr. Louie and I are saying two completely different things. I come at this from the perspective of being the best in the world of both protection and offensive strategies. We can consolidate and put the best technologists and the most knowledgeable people in the same organization overlaid by the rules of the road, rules of our country and the rules of engagement. There's no doubt in my mind that there's going to be some version of a cyber NATO, regardless of how it's going back and forth today. We're going to have to interact with our allies on these issues.

Who's going to do it? Who's going to represent all aspects of our nation to that group, to our allies? We are going to need one place to do it. It is very frustrating to see the inefficiencies that take place when one group in the government could solve a problem for another group in the government. But it doesn't happen because it's either politics or a set of rules and laws that are getting in the way. We need to create an organization and a system and a framework so that we would be able to deal with things in a much more streamlined fashion. I put forth one recommendation to do it, it needs a huge amount of modifications to make sure that we don't break any international laws or domestic laws.

Mr. Sullivan: I love the idea of an agency that's promoting a global quality of service around technology. I personally have trouble with that being a shared mission with an offensive component.

Mr. Louie: That's why they need to be separate. We have to have the world's best offensive capabilities. We have to have the world's best capabilities at breaking crypto. We all know the history. We need the best quality of law enforcement to protect our citizens from attack. It's true, we need to build those capabilities.

It's a completely different attitude than when going to an intelligence service of another country who knows my association with other intelligence agencies within the U.S., there's this cloud of doubt. It exists even with companies I invest in. As long as there's a cloud of doubt over U.S. companies which provide the technology used to protect everyone, there will not be progress.

We have to remove that cloud of distrust and separate those activities. The DOD, FBI, local law enforcement all need to have the best. However, they're not in charge and should not be in charge of positioning the U.S. and signing frameworks and standards for what safe, secure, quality service and trust on the Internet on a global scale should be.

Mr. Sullivan: In your mind, is there an agency that's carrying that mission right now?

Mr. Louie: If I couldn't create a new agency, I would look at the FCC, Commerce, or State, as better places to engage from using the resources of the other agencies and expertise to start as a building place. But again, I wouldn't start with DOD, and I wouldn't start with existing agencies that are currently considered lead agencies. Even DHS, as many of us inside the beltway don't consider DHS as a law enforcement agency. Unfortunately, the rest of the world has the perception it is.

Mr. Sullivan: Another topic I want to touch on that I think you all covered, was the concept of removing disincentives to sharing. I heard one concrete idea from Mr. Schlein regarding safe harbor tort reform, but what are some of the other ideas that you have? Assuming we do want to remove the disincentives to sharing and promote more sharing, what are the concrete things we should push forward?

Mr. McLaughlin: I think Mr. Schlein mentioned he wanted tort reform, some have already begun with removal of antitrust concerns, so there's been some progress on those lines. Removing stigmas that come if there has been a breach, and what happens as a result is important. I bring up the tort idea and other non-tort actions as well. But government actions against an entity who confesses and says something's wrong, will that then be used against them later? The balance needs to be there between allowing people to come forward and say an event occurred because we want to encourage that sharing to happen, while at the same time not allowing negligence to pass without consequences. I think that's the balance we need to strike.

Mr. Schlein: One thing we would ask ourselves, and I'm taking a little bit of a chapter from the FAA here, if an airline or an owner of a private aircraft, flies that aircraft, there's a set of rules that must be followed. If there's sort of a near miss in the skies, usually the pilots are grounded and a full investigation is done. So why if there is a breach in some area of critical infrastructure is that investigation optional?

I may not be using the right analogies here, but if by having that information we'd make ourselves safer, presumably that's why the FAA does it, using these investigations to make the skies safer. If investigations of critical infrastructure breaches end up making people safer, would people really want it to be optional? I just wanted to put that in people's minds to think about.

The other side of it though, is to make it worth their while. What do they get by sharing? If it's a one way street, it doesn't do a whole lot of good. While we're still early into the information sharing bill, we'll see how that turns out. If that benefit doesn't flow both ways, rest assured there would be very little information shared.

Mr. Louie: First of all, I love the FAA model. There's a lot of goodness in the FAA model which is not just about figuring out what's wrong, it’s also about taking precautions after figuring it out and passing those bulletins out to every aviator, every airline, and every aircraft manufacturer as the most immediate best practice. I think we could do something like that in cybersecurity. Who we can share with is important in creating a neutral third party, and that third party could be an agency, it could be a nonprofit, it could be a 501(c)(3). If people are worried that if they share information, somehow it's going to be misused by a government institution in this country or another. Possibly they may not want to disclose something that they might be liable with; they need to be able to share anonymously.

There are other issues that relates to sharing, such as being to be able to get something from it in return, meaning best practices. For banks, one thing financial ISACs do extremely well is the big banks protecting the small banks. As soon the big banks get hit, they immediately contact the small banks. It is in nobody's interest to have small banks get attacked when big banks can protect themselves. They figured it out for themselves. However, we can't allow it to be on a case-by-case basis. The rest of the world doesn't have the financial resources that some of our bigger financial institutions have.

There is a broken mindset in the federal community regarding cybersecurity, and that is they alone have the good stuff. They have the TS, SCI, and classified material on cyber, and they can't let anybody know how they got that. They have to protect sources and methods. It's a problem, not because that information isn't good, but that mindset doesn't recognize that private industry in many cases has better information. Why? Because it's money. People go after money a lot more than they go after national security secrets.

We don't know how our big institutions and our commercial organizations with their surface attack areas, are being attacked globally because they won't share with us. We don't make ourselves approachable, since we think we've already got the best information. If this is true, our trust is greatly misplaced and we're leaving a huge gap in that information sharing regime. I'm not suggesting that classified information suddenly be unclassified, but we need a framework and a mechanism for everybody to throw their stuff in the pot at machine speed; so we can immediately protect critical infrastructure. That includes not only our national interest, but everybody who is a good and fair player globally.

Mr. Sullivan: All right I've got one last question and I don't want to miss this chance to ask. You used a phrase about solving future problems. As venture capitalists, security companies, and people looking at building products to solve future problems, we want to solve future problems as well. You've spent a lot of time looking at the technology landscape and where it's going. Too frequently, security involves bolting on after the fact. Someone comes up with a great idea then we think about safety after the fact.

What are the areas that we should be thinking about in terms of looking at general technology, and platforms and where they're going so that we're not continuing to bolt it on in six years? Right now, in the enterprise we've been talking about, suddenly we're in a borderless world and now our network level security program doesn't help us anymore. What are the areas that you think we should be looking at going forward?

Mr. Louie: Machine intelligence is one area. We have algorithms running machines that we depend on, or are part of the kill chain. Those algorithms and money are going to be huge vulnerabilities. We have machines controlling machines, and if there is no trust in that linkage because that code, those data streams, and packets, then really bad things are going to happen at the global scale. We are racing as fast as we can down that freeway to automate and put machine intelligence in everything.

Doing machine intelligence is like back in 1999 when everybody was putting ".com" on three letter words. Now, let's put machine learning on everything. I'm not saying machine learning isn't really transformational, but it's going to be a huge attack surface vector that we need to start working and investing in now,, and figure out how to protect that flow.

Mr. McLaughlin: Machine learning I think specifically is associated with the internet of things as well. That is another buzz term. With the ten billion more devices that can go get data that were conveniently put in the cloud in one place, we to have to figure that out as well.

Then, I think another area that is fast approaching is quantum computing. It is moving very quickly and has a lot of pros, both in the sense of machine learning, for what can be done with it; and a lot of ideas that will change things for encryption as an example. It will change the utility of those things in the future.

Mr. Schlein: Of course the issue with Mr. Sullivan's question is, as we attempt to repeatedly predict what may come true, the line keeps moving. I do think we're moving into a signature-less world where we're not focusing on detecting known bad signatures, which is kind of what we've done for the last twenty years. The focus will be on the data. The group that's able to get the most important data, process it, run it through the right behavioral models, figure out the anomalies, and doing that at line speed will win.

That process will not beholden to some sort of signature, and it will happen. I also think, as an industry, we will start to expand the DMZ. Meaning, that we will start to do a little bit more preemption of attacks. Most of what we've done as a security industry is just deflection, deflection, deflection. I actually think we'll start to lean forward more, and we will start to invent technologies that allow us to lean forward and bring the fight a little bit more to the bad guys, which gets at the cost issues that we were talking about earlier, namely raising the cost for being a bad guy, so it's not so scalable. I think that falls into this area of preemption.

However, I'm not so sure anything replaces education. The reason why I say this, I started a company a zillion years ago called Fortify Software. It was the very first time anyone thought to use secure code auditing and look at the source code. The reason to do it was to get to the root vulnerability at the source code level and remove those vulnerabilities, the result would be a piece of software that is far more secure. There's not a lot of debate about that. It should be engrained. It just should just be that way, and not thought of as an add-on. As a vice president of engineering. How could unsecure code be allowed? We are slowly progressing to the idea security must be built-in from the beginning, so it doesn't become a network operations problem later.

Mr. Chabinsky: Sometimes I feel like the Commission has been asked to set out the course for curing disease, not a disease but all disease. Then, we'll get people who will come in and say, "Well you better make it global", because it's of course a global problem. There is the opening shot across the bow of the top three things Mr. Louie would do.

The first is organize nations around a set of activities to clean up; in other words, the world has to start somewhere, right? Let's figure out a set of activities that maybe we could try out everything we've been discussing in the notion of cleaning it up. Mr. McLaughlin was very compelling when talking about the asymmetry that bad guys can act in an increasingly automated way and at huge scale. One guy wakes up in the morning who could control literally over one million infected machines, and to what aim?

Talking about Mr. Schlein's view of whatever we do, we'd better make it measurable and hopefully add in some deterrence and attribution at the same time while we go after the bad guys. This Commission has been asked to provide bold recommendations. When I hear all of that and pull it together, one thing that does come to mind is the fact that we have hostile actors that really are able to operate at scale in ways that really can happen in the regular physical world with these millions of computers. Recently, the U.S. government indicted seven Iranians for DDOS attacks against the finance sector. The government also indicted five PRC officers for economic espionage attacks.

Mr. Schlein mentioned ransomware as a terrible problem that folks are facing. Russia brought down the Ukrainian power grid with a DDOS attack, or actually with large scale infected networks. What all of those have in common on the cybercrime side, economic espionage, and potential use of the net for terrorism and warfare. It is this problem of large scale malware distribution which people commonly refer to as botnets, but it's really so much more than that. I'm wondering about this idea of organizing nations around a set of activities to clean up the net. Do you think it would be an ambitious, achievable, and worthwhile objective for us to come out of the gate and say the U.S. will have leadership with the private sector and the government, to entirely clean up botnets within two years?

Mr. McLaughlin: I think that would be an interesting and ambitious goal. One of the things that we tend to do, not surprisingly, is to get very, very, focused on the most advanced attacks because they are very painful. But the vast majority of attacks don't fit that category today, they are more common than that. All of them are caused by botnets and they don't cost a lot. Unfortunately, a lot of systems can’t stop them and people fall prey to those. On this idea of raising the cost, if we could go in and eliminate a certain strata of attacks, or make them make them way more expensive or less way less effective if nothing else; we move people into the more sophisticated realm. It's not necessarily a great outcome, but a lot of attacks would be eliminated. I think that's an interesting idea.

As a side note to trying to test out some concepts like that that, we've been associated with something called the Cyber Threat Alliance. We brought some of our competitors together and said to them, what if we actually were sharing indicators of compromise, not the common stuff, not virus totals, the stuff that we think is top shelf? We shared that in a machine automated format using STIX and TAXII, and then whatever we do with it, we do with it. We all have the same levels information, so we've been doing that actually for the better part of a year with a few other security companies and it's up and running.

The second thing we did, was we actually know quite a bit collectively about campaigns. Sometimes, like botnet campaigns, the collective wisdom, not surprisingly, was greater than any individual wisdom. It was very manual in nature but done just to test the idea out. The Cyber Threat Alliance said we're going to go try to figure out everything we know about the CryptoWall 3 campaign. We got together as companies and pulled our resources on it, and after a while came out and said we now know eight hundred seventy-ish collected pieces of information about indicators of compromise around that campaign.

It wasn’t easy, it took a while, but it worked and we went to the government. We went to a couple agencies in the government, gave them what we know about CryptoWall 3. Some of the agencies came back and shared what they knew, and gave us one hundred sixty-five things we didn't know. They said in the process they didn’t know three hundred things the group shared. It took months, but nonetheless it got done. When that was finished, we turned around and we published a report on CryptoWall 3, and made the world knowledgeable about these thousand things, indictors of compromise that were not known yesterday.

It took the bad guys all of twenty-four hours to move the CryptoWall 4. The point was, they had to. One of the goals that we have with this thing is along the lines brought up by Mr. Chabinsky, is to say, what if we could actually track and work on five thousand campaigns simultaneously. The security industry, along with many larger companies possessing a lot of threat intelligence, could actually do that.

If they were doing five thousand campaigns at a time, that's really going to put the hurt on the bad guys. It's not going to put them out of business, but it’s going to make them move, move, move every time that we show how an attack works. The defenses get stronger and stronger, and that will increase the cost to them and start to get the wheat and chaff out of there. I think it's an interesting idea that could have a lot of benefit.

Mr. Schlein: To put some numbers behind the buzz, there's about a half a billion, if not more, compromised systems throughout the world. I think the going rate is about ten thousand for an hour can be rented for a dollar fifty. This is what makes it amazingly scalable. I love the audaciousness of what you want to do. I do worry about your ability to do it. I think it becomes a little bit of a whack-a-mole. There is some benefit to knowing where the bad guys are actually. I do think an area to try and get a solution would be to stop the efficacy of bots. Remember, they're automated at the end of the day. If we could separate the automated traffic from the human traffic, we could stop bots from mattering. That may be a more doable goal than trying to eliminate that half a billion that'll just move somewhere else.

Mr. Louie: Here are a couple thoughts. First, at the very high level, nation-states are not going to give up their ability to collect their own intelligence, nor are they going to give up their ability to prosecute military advantage including all the tools that we've talked about. On the other hand, there are enough challenges globally across the board at this lower level.

The point is not to eliminate it, but to significantly raise the cost and slow up the bad guys. There's two things: one puts a marker down that forces a conversation at nation-state levels, either bilaterally or multilaterally, about who's in who's not in, which is a worthwhile exercise in and of itself; second, it engages the common carriers. Because it is about the stuff in the middle now, not just about the end points.

Third, it promotes the research necessary as we raise the bar and to keep raising the bar, not just raise it one time to make that hop to the next level, but systematically making it much more expensive. It becomes not a dollar fifty, it's a hundred fifty; then it's fifteen hundred, and then ten thousand. If we take out the economic benefit of being able to do this, and we start securing the nodes and the pipes along the way; we say it's to everybody advantage to do so. It's not just the U.S., we need Singapore, we need China, we need Russia and all these other countries that are out there who may not historically be in our favor.

We all share a common interest. We need our financial transactions to happen, because the money must keep flowing. We need to make sure critical infrastructure and nonmilitary kinds of situation in times of peace to be safe and secure and we need to have trust. Some nation states will check out, but that's OK. If it gets to be on what I call the rhetoric of negotiations and the rhetoric of treaties, it's very easy to say we're against it. It's very easy to write a law that says something is wrong to do. It's a completely different thing to say we are committed to this, like we were to getting rid of smallpox.

We're going to raise that cost so that we can eliminate whole sets of bad actors, so those that I call the script bunnies are gone. The kids who are just constantly mucking up the system which slows everything are gone. The penalty quite frankly is, if you don't comply, we're going to put all the walls around your packets to make your packets go slower than everybody else's because you have bad hygiene.

It's like airplanes going from untrusted airports. Airplanes that go from untrusted airports get significantly more hassle than airplanes travelling from a trusted place to a trusted place. I think we have to pick the right fight, about the right set of goals. Sending something that creates global engagements also will lead to economic rewards for companies joining the fight. Companies who have innovative solutions, researchers who leave universities to create startups, and big companies are already in the game trying to figure out where to put R&D resources will all play, because it creates a marketplace. It's a great idea, but we need to make sure we frame it right so we don't set ourselves up for failure.

Ms. Murren: Your comments were already very unique and thought provoking. One of the things that I wanted to follow up on that you both mentioned is the area of corporate incentives. When we think about eliminating things like the SEC's requirement to disclose a material event relating to a cyber breach, or a legal remedy for a cyber breach for a company, how would you change the incentives to encourage companies to be good citizens? The frame of reference that I'm using to think about it would be to look back at manufacturing companies and how they treated things like environmental safety or consumer safety. So, how do you prevent companies from externalizing their costs in a way that doesn't damage their ability to actually fix the problem?

Mr. Schlein: The tax code can probably be used to do it to some extent. I think when I had originally come up with the idea of the risk preparedness index, about fifteen years ago, I had the insurance industry ready to vary insurance premiums based upon what the index had as well. If we use it as a proxy for why would companies do this good hygiene, what would in it for them? I think when we talk about private industry at the end of the day, earnings per share will matter most in terms of getting companies to do it properly. I would think of ways to help incent it, maybe the tax code, and the incentives that are around insurance premiums.

Mr. McLaughlin: This is also an area where the free markets are going to start working harder than they have as well, just from the competitive aspect of what is secure and what is not secure. We're starting to see some advertising across industries where security is a key component of what the company is saying. How they actually back it up might be a separate thing related to scores, or government seals of approval, or things along those lines, or getting reduced premiums on insurance policies. I think all these things would help.

More and more, it seems like there's so much information about cybersecurity in the in the realm of public knowledge. There's a market opportunity for companies to differentiate themselves based on how secure they are. Companies are starting to take that up. I'm not sure how much government incentive is needed for companies to do that versus the market just working.

Mr. Louie: I think there needs to be some level of safe harbor if parties are not negligent. I go back to the airplane example, if there is a bad airplane that where there was a known problem with the wings falling off, and an incident occurs where the wings fall off, the owner is negligent, and should be punished for it. If someone takes off in an airplane, and a missile shoots it down, it may or may not be negligence. It's someone shooting a missile at the plane.

The problem with cyber is a combination of multiple factors. I think there needs to be some level of standards and Mr. Schlein's ideas are worthy to be considered. What is a reasonable expectation of cybersecurity and trusts a consumer or company or an entity should have if they're using your service and product? As long as we follow that level of trust, companies doing the annual security audits, just like doing the required financial audits; then there should be a safe harbor because we should not incentivize the attackers to do cyberblackmail.

Cyber-blackmail says, "We're going to take your company out. We know you're going to have to report. You're not going to report to the New York state attorney, you have to report it to the FCC and we will make it a headline in The Wall Street Journal. So, we're coming after you unless you pay us off." That's kind of the model we have right now, because all the incentive goes to the attacker. If a company is negligent, didn't do that hygiene, didn't safeguard that data, it is still negligent and shouldn't get a free pass. However, if there's an attack and the company followed the rules, just like following an airplane accident, the disaster team would show up in this mythical new world that we live in, figure out how the attack happened, and it would keep it confidential. That safety warning was put out immediately as the best practice for everybody else. A cyber alert message goes out at machine speeds and our machines will all get updated to shut that wall off.

It's close to being right, but there's a lot of problems in the middle. It’s always tricky but that's framing that we need to think about it. Cyber is one of the few places where the victim is guilty and the attacker is the winner and gets all the reward. We’ve got to change that equation pretty quickly.

Mr. Lin: You all emphasized the importance of international cooperation and coming to some consensus on some set of rules, and so on. I want to describe three different worlds and I want you to rank order them in order of your sense of desirability.

There are lots of other nations in the world. So, world number one: Everybody agrees with the United States, and says what the US wants for the internet and cyberspace is a really good thing and we all sign up to it.

World number two: The balkanized world that Mr. Louie mentioned, where there are like-minded blocks getting together. There may be some allies and some other nations with other views and they get together and form something like the Shanghai Cooperation Organization. They get together and make own different rules.

World number three: A world in which all nations engage in a negotiation. Since it's a negotiation, everybody has to give up something. In particular, the U.S. has to give up something that compromises on some of its core values.

Please rank or order these in your order of desirability. I believe that everyone's going to say number one is more desirable or at least better. I would certainly say number one is better, but to me, the interesting question is whether the number two, the balkanized world, or number three, the one where we all agree, but the U.S. has to compromise on certain values. Which one of those is the most desirable and whatever your answer is say why.

Mr. McLaughlin: The Geneva treaties exist to describe how prisoners should be treated. Nobody compromises on any of those principles whatsoever. Everybody agrees what’s humane and civil, and that's how things are done. Not everyone follows the rules, but nobody's compromising their core fundamental principles that I'm aware of to agree to those things, including the United States. I'm not sure that the frame works.

Mr. Lin: You assert that there is a common core of values among all the nations that you would want to bring in the important nations in the world; on which there could be some fundamental agreement. Is that what you just said?

Mr. McLaughlin: It's possible, but it depends on how you narrow down what those sets of values are going to be. I'm suggesting that there are examples where almost all nations have agreed to things without compromising any of their fundamental principles because of what's at stake. The Geneva treaties is an example of international warfare. Everyone figured it out, and people usually follow them.

Mr. Lin: Fair enough. So you would believe, for example, that the nations of the world are more or less in agreement on the value of all free expression, free speech, access to information?

Mr. McLaughlin: There may be agreement on the importance of information, the importance of data, and the importance of GDP productivity, and things that go along with that. The common organizing principles in cyber are fairly short before everything starts to fall apart. There are cases where if there isn't a list of a hundred things that have been done historically when there start to get more than a few, we will be in world number three, and that would be my second choice.

Mr. Louie: I think there's some good thinking along those lines. That is, anybody's that's ever had to negotiate a trade agreement understands the difficulties of doing anything at a global scale. Whether it be land mines or global warming, there are lots of examples of global initiatives that have taken herculean efforts to get some group of nations to agree. There has to be a lot of back door discussions, quiet rooms, off the record. This is not something that any of our countries, at least on a bilateral level, may be on some small set of multilateral discussions that we can agree on.

The first topic is an easy one. Financial transactions should be protected. Most responsible countries would agree with that because nobody wants their bank transactions to go slower than anyone else's. That's a good one, that's pretty easy to agree on. We should do a level of activities to see reduced consumer internet fraud. Why? Because the U.S. is not the biggest victim of internet consumer fraud. China is, not the US.

If we can't even agree with Canada, Great Britain, or the traditional five "I's" who can we agree with? It starts with little steps but it starts with Mr. Lin's idea, which is the point of world number one. If you start with a U.S.-centric view, namely what benefits my country as the basis of a negotiation, it's flawed. We have to start with whatever is the common denominator that groups of countries can agree to. Even if they can't agree to exactly our words, maybe China or Russia creates some other version has a slightly different set of words but has the same results. As the world moves to a greater, connected world and machines control machines, it is in nobody's interest for any responsible nation-state to allow third parties or rogue actors to intervene to cause great harm. It is to nobody's interest. We are not talking about democracy. We are not talking about freedom of speech. We are talking about life and safety, and we can start there.

Mr. Lin: A New York Times headline can be deadly in China.

Mr. Louie: The art of negotiation and diplomacy has been going on for two hundred fifty years. We've got an agreement on rules of the high seas. We can come up with similar sets or frameworks on the internet, because it is to everybody's financial and safety advantage to agree on a set of common, agreeable values. Not every country is going to step up, I'd be happy if sixty percent of the countries do. Quite frankly, I'd be happy to have a third of the countries in the world would say this is what responsible internet usage looks like. It's at the foundation level, but it starts with us thinking about what is a fair and level playing field for everybody to play in and is not advantageous to the U.S. on these particular issues. I'm not talking about giving up military advantage, and I'm not talking about law enforcement.

Mr. Schlein: I probably am skewed towards where Mr. Louie is at, which is just around taking small steps first, and trying and get some common set of rules and understanding with a smaller group before trying to boil the ocean with everybody else.

On your world number three proposal, the answer is, it depends on what we're being asked to give up, and where we're being asked to compromise. Until the details of it are known, I'm not so sure we'd get to Nirvana with that one. I would definitely just focus on our allies to get started, and then and then go from there.

Mr. Louie: But even our own adversaries are sometimes adversaries, and sometimes friends. Look at the Trans Pacific Partnership (TPP), what China was willing to give up. We never in a million years thought they would even sign a piece of paper saying they would make the trades that they came to trade now. Whether they enact it or reenact it is a completely different issue. The TPP has its own set of challenges. However, there was a basis for our dialogue and there was at least some common ground and understanding that it was to neither country's interests allow this kind of behavior to exist.

It was hard and unfortunately it got buried in a set of negotiations which may not come to pass for other reasons. That's why I think we need to separate these issues, and make cybersecurity its own negotiation, and go back to the drawing table, have those quiet backroom discussions, then start to frame. We're starting with our allies and people we have shared interests with which sometimes means our adversaries and cut our deals.

Mr. Schlein: It is why I stress heavily the need to get attribution right and to focus on attribution. Sometimes, I think as a country we prefer not to do attribution because it's something we don't have to deal with and also get the punishments right. Attributions must be consistent and enforced. Both those things must be done together, whether it's done in a small group or a big group, it must be agreed upon and then enforce that way.

Mr. Alexander: I have two sets of issues, and I also have some comments. I won't make those comments now in the interest of time. First, on the insurance, I think about Mr. Schlein's comment on the insurance industry and where it is, and what Mr. Louie kind of echoed. I think you all agree with the fact that when a company is sued for not defending its network against a nation-state that even the government wouldn't be able to prevent, we're in the wrong place and in a liable situation.

One of the things that we have to do is put something down in writing some place and say it needs to be looked at. Is that what I'm hearing all you say? I just want to get that up because I do think when you look at Anthem and others with all the lawsuits that are coming at them, and look at what's happened to government, we've got to fix that.

The more important question from my perspective, stems from the earlier question this morning when we look at what Facebook has with 1.65 billion users, we pointed out that eighty percent of them are not from the U.S. How does the United States work with industry, how does our government work with industry, how does our government work with other governments, and how does industry work with industry? I agree in part that we don't have this right. But I think we need to get more resolution on some of these comments and I just want to put some things on the table to make sure I understand.

There are multiple layers that our government has to deal with. What Mr. Louie is pointing out, as I understand it, is who is it that negotiates with other countries about how we act in cyberspace. It's not the military, it's not law enforcement, and it's not potentially somebody in another law enforcement-like agency. It should be somebody else. That's the real key I think you're bringing up, is that fair?

Mr. Louie: That's correct.

Mr. Alexander: I do think though that our government has to engage other governments on behalf of industry in our nation on how the rules of the road in cyber are going to be written with respect to collaboration. It means that a company like Google or Facebook or Yahoo or whoever, isn't held to one standard here, another standard in this country, and a third standard over here. We ought to get one third, one half, or somehow come up with an equalizer that sets the stage right. My opinion, from working across the government, is while that entity would be a non-military, non-law enforcement, everybody's got to help. I do think though, that to couple with what you're saying with what Mr. Schlein brought up, I think he said a cybercommand should get more respect and so should its previous commander.

Actually what Mr. Schlein is saying is that on the military side, it's not organized right. I think you could look at that, but I also think, and what I would like your opinion about is, what we really need to do, is have a way of setting up a war game or some kind of exercise where participants figured out what's the right way for all these agencies to interact to accomplish these different sets of goals. I do think some of it is right and some of it is skewed. It's an important thing because what you both want to accomplish are things that we pointed out earlier that have to be done. We have to get our government to work with other governments to set the stage. We've got to provide cover for industry and it's got to be fair, and we've got to protect the network and we're not doing those.

Mr. Louie: We have multiple tools in the tool bag and it's clear that there's not one tool that can solve all the problems. Otherwise, we wouldn't need to commission, we could just go grab the tool and we'd be done. Even on the military front, we have great liaison capabilities with other nation-states. We think about nuclear code-handling, I'm chairman of the Federation of American Scientists, which was used to be called the Federation of Atomic Scientists, which was created in 1946. The whole goal was, as scientists, how to make sure the world is responsibly safeguarding all the nuclear stockpiles and use of nuclear materials.

Even in countries where we might end up in a very bad adversarial relationship, there is common ground to make sure that our militaries are talking to each other, particularly in cyberspace. An attack, just like the way we have in NORAD, potentially could be disguised as an attack by somebody else could be wrongly perceived as a first strike. The first strike means your network is going down before a real attack happens, and somebody gives you enough false information across all sensors to create the illusion of an attack. Is there time to take your hand off that red button in a world where we're going to have hypersonics? Is there time to choose to not press it?

That is the reality we're heading towards. Militaries, even adversarial ones at times like the U.S., Russia, China; and the nuclear states have something really serious to discuss regarding cyberspace. For better or worse, cyber is one of the classic first moves that people will use to launch an attack. We can engage on multiple levels: State Department, Commerce, Defense, law enforcement, and Interpol. When we consider the bombing attacks that took place in London, or Paris after the shootings; for the first seventy-two hours, all the countries in the EU cooperated with each other. There is a basis for cooperation in times of great distress. We have to figure out how to do it when it's not in a time of great distress, so we can prevent bad things from happening before they happen, so we're not in a mad scramble after.

I was on a mission to the EU right after 9/11, and we had this issue arise about privacy. The European view of privacy are very different than that of Americans. I won't say theirs is better than ours or ours is better than theirs, it’s just different. We were trying to get personnel file records to deal with the potential terrorist threats of terrorists flying into the U.S. There was a lot of sympathy, but there was this different debate going on at the same time about whether they can share, is it appropriate to share, is it legal to share, what's the consequence of sharing. What some of us told the EU was if 9/11 happens in the U.S. again, it would be just like Pearl Harbor, and that's a bad thing.

In the U.S., we'll do a study and create a commission, find blame, fire a few people, we say they’re disgraced, and we move on. We've done it time and time again as a nation to where every time there's a crisis, we do a study, we blame somebody, remove the person or people, and then we go on. We told the EU during our mission there, if a nation-state doesn't share with other nation-states and a thing goes bad; there isn't any firing, but they put the whole EU in jeopardy. The EU needs to figure out a basis for sharing information, in spite of personal preferences regarding privacy.

This dialogue is a very tough dialogue to have, it has lots of gritty complexity. However, we've got the best diplomats in the world, leaders who are willing to engage with others. We just have to raise it up to that level and not make it about technology. Unfortunately, the problem we have today with many nation-states, is they think this discussion is about the U.S. seeking an advantage for its technology companies, security equipment, and internet providers over others. We need to get beyond that and deal with these really heavy issues at each level of government where it’s appropriate on an international basis.

Ms. Anton: We've heard a lot of different ideas. We've heard about if you fly a plane, you have to follow the rules of the FAA. We've heard about the SEC, Commerce, and State coordinating with our allies. We've had a proposal for a new secretary of cyber. DHS was established in response to 9/11 and when we read the 9/11 report, we see all of the things that went wrong. Our country is really great at establishing something very big, that's very bureaucratic in response to a really tragic event. I have a twofold question, number one, what is going to be the cyber 9/11 event that causes us to really do some of the things that the three of you proposing, and number two, do we need to have another bureaucratic agency to deal with these things? Or, is it simply a matter of, as General

Alexander was saying, really coordinating in such a way that we are really doing serious war-gaming, and coordination, that we have all the protocols and we're good at doing what we need to be doing.

Mr. Schlein: I'll answer something you didn't say but you sort of implied using DHS as an example of how maybe gathering all these different agencies together didn't quite do exactly what we thought it was going to do. I thought about this as I formulated my proposal. DHS just took twenty-one different, disparate groups and put them into one agency. I'm not proposing that at all. The likeness of this is I want FBI cyber, and DHS cyber, and I want U.S. cyber command. I think you're actually aggregating to eliminate the bureaucracy, rather than keep the bureaucracy that I think we will continue to have when you have law enforcement trying to break into something that they can't or don't have the technology to do, but it is to their benefit their national security or law enforcement to do that.

In the private sector world, we find the best person to solve the problem and we go solve it. Understanding full well we have laws and authorities that overlay problem solving efforts, and need to be respected. That's why I would argue it needs to be done centrally to coordinate it. Removing the bureaucracy and streamlining processes should be why we want to do it, from my perspective. As for what would amount to Armageddon, we all might come up with our different versions of that, but I've always believed that it will be a coordinated and systematic attack on the grid. It would be really interesting to see what happens to our society when we lose electricity for a few days. I was fascinated by hurricane Sandy, when the fighting that started to erupt about people trying to get fuel. If I had to pick one thing, I think ultimately fighting over fuel would cause more chaos than anything else.

Mr. McLaughlin: I'd say that there's a lot of 9/11 scenarios we can come up with. I think if there's going to be such a scenario, we would likely see it from a terrorist organization rather than a nation-state, just for self-interest purposes. It doesn't mean it wouldn't be any of those sorts of scenarios. The ones that are being tested all the time are really about the Information and Communications Technology (ICT) and Supervisory Control and Data Acquisition (SCADA) environments, and what can be done with IT technology relative to dams and electric power grids and those sorts of things. It's not hard to concoct scenarios.

I can agree with Mr. Schlein that it's better to try to simplify the bureaucracy rather than to create new ones here. However, in thinking about and listening to what we were talking about, one of the challenges of all this becomes defining missions. The mission of cyber command is different from the NSA, and different the FBI. Companies are aware of the difference when they call somebody and ask for assistance. Sometimes, the response itself depends on whether the request is made to a law enforcement agency, or a national security agency. The national security response to such a call may be to watch that for a little while longer before we do anything. Getting the missions harmonized may be kind of difficult.

It still seems working together would be somewhat helpful along those lines. There's just one other thing to sort of wrap things up. A common theme has come across is defining what's a common interest. When we're talking about our agencies working with other nation states, I think we're all saying the same thing, which is, that some level there's a common interest. Probably a financial interest, probably an interest in safety, and that's the place to start building trust and interoperability for things that we need for not only in our society across other nations as well.

Mr. Alexander: One of the things that Mr. McLaughlin asked, I just want to hit on this key point to make sure I got it right. The issue of sharing right now, there are barriers to certain agencies sharing with commercial industry. In my experience for the most part, I had to go through others to push their data out. For a whole host of reasons, it took more time. It tends to give people the perception that those with the data are not sharing. I don't know how to address it. It's a fact that's on the table, and it may be something that we look at going forward. Because there is a lot of sharing that goes on; even if it gets pushed around to multiple parties before it finally goes out. That, by definition, is not real time and is something we have to look at.

Mr. Louie: I would agree with you, General. There is a lot of sharing, even among federal agencies. However, there are a lot of barriers and they are constructed that way for good reason. If you think about it, when we're sharing information with the FBI and FBI prosecutes, it is a matter of due process for the defender to know where the information came from. They have that right, and we don't want to take away that right. We share with intelligence agencies who don't have the ability to prosecute about activity that's happening overseas. It’s handled in a completely different way.

Some contracts are just really difficult to determine is that solvable. It requires a different level of thinking that just doesn't make the rules go away. This country stands for something, we can't get rid of the basic foundations of what our country's been built on, because the cyber threat exists. That's what makes it difficult and that's why easy solutions aren't so easy.

Another thought on the big attack. I think cyber, if it's done right by those involved, is a little bit like malaria. We should definitely raise the bar and make it difficult to act. In any event, crooks are not going to kill the golden goose that delivers the money. They don’t want to take down the internet. They want to exploit it. The most reliable computer is the one that never crashes. It's the one that's totally trusted, and it gets milked and milked, and shaved a little bit. Anybody who screws up the existing system will get whacked. If I was an organized criminal, and if Mr. Schein was an organized criminal and he got greedy, that raises the stakes from a level three to level four. When that happens, I'm going to whack Ted. Why? Because what he's doing will kill the golden goose.

It’s also true at nation-state levels. There doesn't have to be this massive event, other than an all-out war, that causes an extreme reaction. Look at what happened with Russia and Georgia, and why what happened, happened at Georgia. They keep the good stuff until it really matters. That's what nation-states do. There might actually be a digital Pearl Harbor if we’re really dumb. We have the capacity to be that dumb.

I suspect what's going on is a slow bleeding, and a slow cost that creeps in like a cancer. It begins to create a level of distrust or Balkanization that we will all regret later. That’s a much bigger problem than one event, because the one event happens and it's gone. But the cost of distrust on the internet, and the cost inhibiting the ability to put better goods and services, better capabilities on the internet and the danger of putting that stuff on an unprotected network, that's the true cost. Putting all of our information and our personal privacy at risk every single day is something that we need to figure out and solve.

Mr. Donilon: I would say one thing on our assignment, which is an express assignment from the President, has been to think about roles and responsibilities in the federal government. To better answer the question of who is responsible for what aspects of dealing with cybersecurity, to what degree increased centralization would be better, how we ensure access both in the government and in the private sector to the best information, the best ability to respond, to be resilient; we're going to be working very hard on the structural issues. With that I just want to thank you, just a terrific panel, and I really appreciate you doing this, given the energy and thought that you've put in your presentation is much appreciated.

Center for Long-Term Cybersecurity (CLTC) Briefing

Steve Weber, Faculty, School of Information, UC-Berkeley

The notion of a transition memo, to me, naturally focuses people's minds on the 100-day window during which a new administration can make some really dramatic moves and profound decisions. What I would like to do is just highlight for you some of the thoughts I think that came out from today and have come out from some of our work and remark about the 1000-day window which I think this memo should address as well.

When we started this center we called it "long term cybersecurity", we had this sort of single motivating notion that we needed to go beyond the immediate concerns of today's and even tomorrow's attack, out to a longer and broader horizon of the issues and challenges that you are going to face are going to look very different than the ones we obsess about today. As has been said over the course of today, that argument doesn't in anyway represent the claim or notion that we don't have to worry the short term. The point simply is that it's a both/and proposition, not an either/ or. So, what we've tried to do is to get some insight, in a disciplined way, into what we believe the cybersecurity landscape will look like, and what cybersecurity professionals will need to deal with going out to that longer term trajectory.

We decided to focus roughly on the period between now and 2020. The year 2020 is not a long time from now and it's not what one would usually think of as a long term sort of projection. We thought it was the "sweet spot" where the implications of many of the technologies and the political dynamics that have come up throughout the day, that we already see today that are just becoming visible which start to play out in ways that actually could surprise us. A concrete example, I think was just raised in the last discussion of this panel. When this long term, corrosive lack of trust flips to a point where ambient insecurity has created a view among large numbers of users that we start from the position that we interact with the net from a position of distrust, rather than from a position of trust. That's a very, very different world for commerce, for relationships with government, for relationships between people and individuals.

So, how have we done this? Well, one of the things we have done over the last year has been to try to construct a set of scenarios, actually 5, that look at significant, plausible, challenging opportunities and threats in that 5-year timeframe. I'm not going to go through that work, it is readable on our website. Like all scenarios, they are not predictions. What we have tried to do is create some models that take key driving forces and exaggerate them a little bit and add the simplicity back.

What I would like to say is that the purpose of constructing scenarios, and the need for trying to prepare for what the future might be, is not to try to predict what that landscape is going to look like; but serves instead for the Commission to force people to ask the question: How would I know, empirically, if the world is moving in one direction rather than another? What indicators should I be looking for now to make those kind of big investments?

Many of the issues, or many of the policy proposals that came from today are things that would be hard to reverse with prior significant investments, including changes of institutions, which would be very, very hard to unravel, as we know. The business models of government policies that would need to come with those kinds of changes are not things that anyone is going to go along with lightly.

Second, and potentially more important, what the sort of output of that kind of work is, what is true across the landscapes of scenarios that we can possibly imagine? What is true regardless of how these factors play out? And, we came to a number of interesting conclusions about that in our exercise and I would ask you to do the same. I'm going to just mention one because I think it is very, very simple, but it also sits behind many of the challenges that came up today. There is an ongoing and ever increasing demand for features, performance, extensions of digital capabilities and that is going to continue to expand to fill the space of what is technically possible, and then go just beyond it.

That is the world that we have gotten used to and that single observation to me, at least, in light of the kind of vagaries of human behavior that go along with it mean that the digital realm will continue to be vulnerable, no matter what. That is a fact of life we are going to have to live with. There is no "silver bullet" out there. And, more importantly there isn't going to be one. I don't think that surprises anyone, in principle. But when you combine that argument with the observation about how deeply integrated these technologies are into human life, then I think we land in an important insight which could shape that 1000-day view. It's this, cybersecurity is now approaching the point where it is probably the most profound psychosocial economic impact issue of the next decade. That's going to be a very big deal.

We all know the internet has had a massive impact on nearly every facet of human life, whether we are talking about psychologies, socio-ability, and the economy. But, frankly, cybersecurity issues have not, for most of the people outside of this room, had that kind of impact on their lives. The ugly truth is, for individuals, it's largely been a nuisance or embarrassment. Sometimes a little bit of a financial toll, a source of fear and worry, but not a fundamental risk that changes how they live.

For firms, attacks of vulnerability are a worry, but not one that rises to that existential level for most firms. The kinds of things that keeps CEOs up at night. Unexpected shifts in consumer behavior, economic crises. I would say the same is true for most, not all governments.

Now, if that's about to change, and I think many of the things I've heard today lead me to believe that it is about to change, that has lots of consequences. It requires us to think very, very differently about how we are going to structure the conversation going forward. To say nothing about what you guys are going to propose about that 100-day window.

I have to say I'm generally skeptical of analogies from the nuclear era. The Nuclear Deterrence Doctrine and the cyber realm strike me as very, very different. But, I think there is one analogy that is quite powerful and works exactly right. It has to do with the way an earlier generation probably experienced the period of the 1950's with regard to the nuclear threat. Thinking about what mutually assured destruction felt like, not in 1980, but in the 1950. The current global crises, and experience of day to day life with constant reminders of the nuclear presence in the world.

It changed how people thought about their lives, the sanctity of life, their families, the relationship with science and technology, faith in governments and their place on the planet. Consider in writing the Commission report how it will feel when cybersecurity enters into that arena of impact when corporations and governments come to know us better than we know ourselves. Memories and emotions become shareable, storable, and possibly changeable. These are the types of things that touch on the core of being human.

Ultimately, they rise to the level of the feeling we call security. Those kinds of things look like the sorts of unpredictable consequences that emerge at the intersection of humanness, and digital machines. That's what needs to addressed, more so even than the contemporary debates that are just getting started on issues like jobs being taken by robots, or artificial intelligence escaping the control of human goals and objectives. It would be disappointing if the Commission did not take on some of those issues.

From our perspective, the issues of cybersecurity start to take on a feeling like we have thought of climate change. It is an existential risk question that demands global commitment of political, economic and technical resources as well as changed behaviors on the part of billions of people. It is a ridiculously tall order. It also means we must consider more of the really ambitious, even audacious proposals that could really change the game. It may not be a position this Commission wants to take, but I hope the Commission will debate it. There is a place in this conversation, to quote Herman Kahn, "to think the unthinkable".

I heard a couple of ideas today that maybe unthinkable but need to be addressed. I'm going to comment on two of them: One, the notion of thinking about models of public health. We persuade people. We incentivize people, and sometimes we find ourselves in the position of coercing people to do things differently. Using seatbelts, vaccines, we were close to that on smoking. It is a very, very counter-cultural kind of view for the way we've come to think about internet society, or internet culture. Someone must address it.

Second, back in the late 1990s, David Eisenberg coined the phrase, "the stupid network" to refer to the end-to-end principle of internet organization. IT is so deeply embedded in the way we think about the internet, it seems unquestionable. There has been a lot of talk today about the notion that the stupid network means it is "polluted", almost like a cesspool. It may be time to put a question mark on that. We need to ask ourselves, As Mr. Louie asserted, do we need the level of certainty that guns and vests provide. Questions need to be raised about some of those long term cultural issues, and it should be done in a way that captures people's attention.

One further remark about the short term, and I'll stop. What has really stood out for me in the last year, as I have spent most of my time trying to understand this issue, is the need from the university perspective, the government perspective, and the industry perspective to work on one simple principle – shortening the transmission belt from the results of basic research to policy and action and markets. There are risks to shortening it too much, such as getting caught in a beta software trap, or an interim technology trap.

We may not want to invest a generation's resources in the cybersecurity equivalent of hybrid cars, if we know a fully electric car is just around the corner. Right now we are heavily weighted on the other side, meaning technologies are taking too long to find their way out of the lab and into the product. There are useful analogies here, such as FDA. The FDA used to be overly risk averse in keeping promising new drugs from being released to the market. It took a lot of criticism for that. It has changed in the last decade, and in some cases now has taken a "risk prudent" position with a more experimental, and less precautionary mindset. It's a little different with people dying of untreatable diseases. Some of what I have heard today has lead me to believe people will come to feel similarly about some of these issues in the next couple of years.

It doesn't all have to be about new technologies, or scientific breakthroughs, some of it can be about simple applications, business models and common sense. Here is a concrete example: Anyone who has bought or sold a house in California will understand this. There are pages and pages of disclosures, that no one reads, that inform the buyer about repairs to the plumbing made thirty years ago. In the next few years, how many IoT devices will people have in their homes? Shouldn't those also be disclosed when the house is sold? Wouldn't that disclosure create a lot of different incentives for IoT customers and manufacturers to build their devices with a different mindset and business model relating to security? It means taking on the National Association of Realtors, which may not be the most favored way for technology people to spend their time.

However, the more we can shorten the transmission belt from basic research, to the devices, protocols, technologies, and network concerns that we know are coming, all the way down to the mundane devices, like the IoT devices people have in their homes, the better we will do. As it shortens, we will be creating the kind of incentives researchers need to actually do things that serve the public interest in an immediate and focused way.

Public Comments

Russell Thomas, George Mason University, Zions Bank

Please refer to Annex B for Mr. Thomas's written statement.

Mr. Thomas has one recommendation for an initiative for novel R&D processes to promote institutional innovation. In the short five-minute period, I'm going to explain everything that's packed in that sentence. What is meant by "institution"? I will use an analogy of an orchestra or a band. The hardware, the software, the technology of the band is represented by the instruments. What the instruments play is the policy. How they play, the skills they develop, the range of performance, who they play to, represent the institutions. Using that crude analogy, I contend, ladies and gentlemen, that globally we are really great at instruments. We are somewhat great, but certainly prolific at musical scores. In practice we are pretty poor and we stumble a lot and we're pretty poor at being an orchestra over time.

The comments of the previous panel, and the comments of the previous speaker and in previous sessions of this Commission there have been example after example of changes recommended to this Commission that can be viewed either primarily or secondarily as institutional change or institutional innovation. I am hard pressed to pick one area that is purely technical or purely policy. Much of what the Commission is doing is either policy or institutional change. We can view the work of the Commission here as an act or process of institutional innovation.

Let's take another analogy. When you first started coding, you joined a big team. There was a problem of coding without a discipline. Software engineering was that discipline. It is the plan and the method that gives order to coding. When speaking about institutional innovation as a process, I'm advocating a process that gives order, productivity and fruitfulness to the process that we have not had so far. I would like to provide four brief examples to make this concrete:

1. When offering incentives, offer intrinsic incentives, that become self-managing. Instead of extrinsic incentives such as tax cuts, etc.
2. There has been research showing trustee certificates offer more incentives to bad guys to make the certificates visible than good guys. It is a contrary indicator to security. The trustee organization is well intentioned and well considered, but it shows the difficulty in coming up with good institutional designs.
3. There is no practice for vetting or testing any practice for cybersecurity, and therefore, no credible basis for saying any practice is any better than any other. What does it say about this process, the institutions being built around it, the mandates, how executives stand behind it?
4. Consensus and conventional wisdom are the enemies of innovation. We should not be starting with consensus; we should be starting by putting consensus at the end of the process.

I'd like to highlight a talk given hear at UC-Berkeley four or five months ago by Duncan Watts of Microsoft Research. He is famous for his research on social networks. He called for a problem-oriented computational social science. By this he meant, let’s pick "Goldilocks" problems. He gave the example of self-driving cars. The solution involved "knowing it when you see it", but the getting there was important and interesting. It may even involve dramatic new theories, new methods and new ways of organizing things. I would encourage the Commission to look at all the suggestions given to you and try to identify "Goldilocks" problems that might become focal points for novel, different, and unique R&D processes. The process of innovation can be a focus of research and development itself. We can learn from other fields. In my written report, I offer five or six examples. There is no need to wait on this. The Commission does not need to wait to conclude its work to begin doing this, as there are people already doing it. It would be great to point to examples of seedling projects that are already underway in the Commission's final report.

James Elste, University of Nevada, Reno

I wanted to provide examples of laws that are already on the books in Nevada that satisfy some of the topics we've been talking about regarding incentivizing businesses. These laws are written in a way that is future-proofed. The first law was written in 2009 known as Nevada's encryption law[1]. It

[1] CHAPTER 603A - SECURITY OF PERSONAL INFORMATION The relevant sections are: NRS 603A.040 “Personal Information” defined and NRS 603A.215

provides safe harbor incentives for companies that encrypt PII. The safe harbor for companies comes into effect if a company has a breach, and it can show it was not negligent in its protection prior to the breach. If PII was encrypted during transport, the company will not be subject to civil litigation for that breach.

That law provides a very distinct incentive for companies to utilize encryption. The problem with encryption is, it has a shelf life. It changes. The way the law was future-proofed involved not embedding the encryption language. Instead, we embedded references to standards bodies. If companies comply with the standards, they are compliant with the law.

The second change we made to the disclosure was to change the definition of personal information. The definition of personal information was established years ago with SV-1386 years ago in California. Name, SSN, and more was covered. There was a freshman assemblyman in Nevada that was very interested in including driver authorization cards in the definition. Driver authorization cards are issued to non-residents. What was added to the law in Nevada does not exist in any other law to Mr. Elste's knowledge. An authentication mechanism was added to the user identification definition. Instead of the vendor owning the user id and password. The user owns the information and has the right to disclosure if the information is compromised.

We had a State Department delegation at the university of about five or six European countries to talk about the Data Protection Act and all the things that were going on in Europe. They were specifically interested in the laws being written in Nevada, and what the state has been able to put on the books. Lawmakers in Nevada make themselves accessible to citizens who want to propose laws. It was important for the legislators to understand why these issues were important. Assemblyman Flores had a very specific interest in protecting his constituents with legally protecting the driver authorization card. He needed guidance on how to incorporate language that would enhance the definition.

The University is developing a cybersecurity program as part of its workforce development effort. They use a public health analogy to make cybersecurity easy to understand for non-technical people. If we talk about anti-virus as an example, it can be likened to an anti-bacterial hand soap. What we are hoping to build to solve the workforce problem is a teaching hospital for cyber. Teaching hospitals are used to train medical students by allowing them to practice techniques on real patients under the supervision of experienced professionals.

In a cyber teaching hospital model, the academic institutions would teach basic skills. The mission is the practical application of those skills. The goal is to build effective “cyber physicians." To build a cyber teaching hospital is a simple thing. It is simple relative to a medical facility. We can do virtual cyber-interventions without having physical facilities. The patients for the cyber hospital are plentiful. We'll work with the state and support the state government and industry in Nevada. It means that in the state there is collaboration and it will make an impact. It is a brilliant way to bring people into the profession and get large numbers of highly skilled cyber practitioners.

Meeting Adjourned

The Meeting adjourned at 4:28 p.m., Pacific Time.

The next meeting will be held in Houston, TX on July 14, 2016 discussing critical infrastructure, and state and local efforts.

I hereby certify that, to the best of my knowledge, the foregoing minutes are accurate and complete.

Tom Donilon
Chairman
Commission on Enhancing National Cybersecurity

These minutes will be formally considered by the Commission at its August 23, 2016 meeting, and any corrections or notations will be incorporated in the minutes of that meeting.

.

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
Alexander	Keith	Founder/CEO of IronNet, Former Director of the National Security Administration, and retired four-star general who headed U.S. Cybercommand	Commissioner
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
Cooper	Betsy	Executive Director, Center for Long-Term Cybersecurity, UC-Berkeley	Presenter

Last Name	First Name	Affiliation	Role
Gilman	Nils	Associate Chancellor, UC-Berkeley	Presenter
Belknap	Geoff	CISO, Slack	Presenter
Heim	Patrick	Chief Trust Officer, Dropbox	Presenter
Prafullchandra	Hemma	EVP and Chief Technology Officer, Products, HyTrust	Presenter
Stamos	Alex	CISO, Facebook	Presenter
Andriola	Thomas	Vice President & CIO, University of California System	Presenter
Dwork	Cynthia	Distinguished Scientist, Microsoft Research	Presenter
Grosse	Eric	Vice President, Security Engineering, Google	Presenter
Sugarman	Eli	Cyber Initiative Program Officer, The William and Flora Hewlett Foundation	Presenter
Louie	Gilman	Partner, Alsop Louie Partners, former CEO, In-Q-Te	Presenter
McLaughlin	Mark	Chair, National Security Telecommunications Advisory Committee (NSTAC); Chairman, President and CEO, Palo Alto Networks	Presenter
Schlein	Ted	Managing Partner, Kleiner Perkins Caufield & Byers (KPCB)	Presenter
Weber	Steve	Faculty, School of Information, UC-Berkeley	Presenter
Elste	James	University of Nevada, Reno	Presenter/Public Participation
Francoeur	Jacques	SJSU – LCoB Center for Organizational Resilience	Presenter/Public Participation
Thomas	Russell	George Mason University & Zions Bank	Presenter/Public Participation
Chalpin	JP	Exeter Government Services	Meeting Staff
Drake	Robin	Exeter Government Services	Meeting Staff
Barrett	Mark	Exeter Government Services	Meeting Staff

Last Name	First Name	Affiliation	Role
Izadjoo	Mase	Exeter Government Services	Meeting Staff
Laszczak	Tatiana	Exeter Government Services	Meeting Staff
Walker	Burden	Commission	Attendee
Scarfone	Karen	Self	Attendee
Landfield	Kent	Intel Corporation	Attendee
Ward	Steven	Eli Lilly and Company	Attendee
Laguisl	M.	UCB	Attendee
Silva	Rob	UCB	Attendee
Conanan	Chris	UCB HAPS	Attendee
Niejelow	Alex	MasterCard	Attendee
Choi	Jor-Shan	UCBNRC	Attendee
Goldhammer	Jerge	UC Berkeley	Attendee
Mays	Carla	Mays Civic Innovation	Attendee
Zhi	Chen	Not indicated	Attendee
Capelli	David	Tech Miami, Inc.	Attendee
PoAn	Brien	NIST/KeyW	Attendee
Henry	Allison	UC Berkeley	Attendee
Reddie	Andrew	UC Berkeley	Attendee
Dardi	Vilerami	Microsoft	Attendee
Coito	Joel	USCG	Attendee
Ackerman	Byron	Dropbox	Attendee
Griffin	Daniel	Wells Fargo	Attendee
Carlo	Brian	UC Berkeley	Attendee
Borohovski	Michael	Tinfoil Security, Inc	Attendee
Spaulding	Catherine	Bay Area UASI	Attendee
Dziedzic	Craig	Bay Area UASI	Attendee
Bryant	Justin	Microsoft/Duke University	Attendee
Zhuo	Haorae	Berkeley Law School	Attendee

Last Name	First Name	Affiliation	Role
Startip	Josh	Commercial Service	Attendee
Mari	Karts	Build Applications	Attendee
Landauer	Carl	Self	Attendee
Ritter	Michelle	Not indicated	Attendee
Not given	Kaliya	Identity Woman	Attendee
Portnay	Erica	Google	Attendee
Zhane	David	Apple	Attendee
Gheytanchi	Ethan	SMC	Attendee
Sheth	Natasha Saggar	Mossamah LLP	Attendee
King	Richard	Taylor Wessing	Attendee
Blahner	Susan	self	Attendee
Moelnagle	Chris	UCB	Attendee
Berman	Dr. Lawrence	LR Berman Co. - alumna	Attendee
Warshawsky	Brian	UCnP	Attendee
Kimmel	David	Cyber Risk Partners	Attendee
Stapleton-Gray	Ross	Packet Clearing House	Attendee
Lee	Flora	Not indicated	Attendee
Wang	David	UCB i-School	Attendee
Gray	R.	UCB	Attendee
Yaeri	Kim	McKinsy & Company	Attendee
Reynolds	Corey	Bay Area UASI	Attendee
St. Pierre	Jim	NIST	Attendee
Dodson	Donna F.	NIST	Attendee
Rowland	Peter	Packet Clearing House	Attendee
Baback	Kevin	Pager Duty	Attendee
Mather	Tim	Cadence Design Systems	Attendee
Lee	Victoria	British Consulate General – San Francisco	Attendee
Moornalt	Lowell	Self	Attendee

Last Name	First Name	Affiliation	Role
Bacchetti	Marina	UC Berkeley/Alumna	Attendee
Ng	Christian	UC Berkeley	Attendee
Villafana	Beni	UC Berkeley	Attendee
Giarrelt	Haley	LBNL	Attendee
Post	David N.	UCB Alum; attorney	Attendee
Brooks	Sean	NIST	Attendee
In	Ramil	Coryton & Burly	Attendee
Lowe	Marisa	Yale University	Attendee
Lacambra	S.	EFF	Attendee
Ball	Ben	Crossmatch Technologies	Attendee
Richard	Natasha	RLI	Attendee
Lu	James C.	WL Harper Group	Attendee
Pollau	Nate	Sycamore	Attendee
Azgail	Vined	UC	Attendee
Jupenda	Liladhar	UCB Library	Attendee
Rolzbough	Lary	UC Berkeley	Attendee
Tomb	Cliff	BAN	Attendee
Yiontes	Yaryan	UC Berkeley Law	Attendee
Berke	Allison	Stanford	Attendee
Gillis	Ryan	Palo Alto Networks	Attendee
Bornus	Michael	Berkeley and Xseed Capital	Attendee
Doune	Paul	UCB Grad	Attendee
Kalaman	Carol	Touro University CatRTA	Attendee
Zhou	Wa	FireEye, Inc.	Attendee
Wood	Jan	Thusia	Attendee
Skinner	David	LBNL	Attendee
Folkson	Michael	RB	Attendee
Rivelti	Alexandria	UCOP	Attendee

Last Name	First Name	Affiliation	Role
Zapata	Marlene	Hewlett Foundation	Attendee
Oh	Jeanie	UCB	Attendee
Pham	Sheila	Troutman Sanders	Attendee
Christopher	Jason	Research IT	Attendee
Kamra	Olivia	UC Berkeley	Attendee
Garcia	Marietta	Perupetro SA	Attendee
Reibe	Jonathan	CLTC	Attendee
Kelly	John R.	Confluence Labs	Attendee
Mio	Mark	Troutman Sanders LLP	Attendee
Andrus	McKare	UC Berkeley	Attendee
Gordo	Blanca	ICSI	Attendee
Nonnecke	Brandie	CITRIS	Attendee
Stepanyan	Arthur	SVIC	Attendee
Kejaz	George	UC	Attendee
Stine	Simon	HP	Attendee
Bhabtra	S.	Not indicated	Attendee
Tierman	Sean	Intel	Attendee
Carpenter	Katherine	Independent	Attendee
Westorer	Scoitt	LEWIS	Attendee
Steiner	Mary	Alumnus, United Nations Assoc. - USA	Attendee
Lightfoot	John	FBI	Attendee
Moore	George M	MILS - CySec	Attendee
Bradley	Janice	Community	Attendee
Murrann	Ben	LUCRUM Net	Attendee
McGuire	Peter	self	Attendee
Snupton	Nancy	Medtronic	Attendee
Thai	Duy	Duy Thai Law Firm	Attendee
Dauley	Charles	Kaiser Permanente	Attendee

Last Name	First Name	Affiliation	Role
Zuidema	Liz	MSFT	Attendee
Krebs	Chris	MSFT	Attendee
Gerding	Chris	Self	Attendee
Irving	James	Hornblower Cruises	Attendee
Edelson	Eve	Berkeley Lab	Attendee
Hibhn	Julie	GAO	Attendee
Gonzales	Yolanda	Kaiser Permanente	Attendee
Schanberger	Irene	Independent (self)	Attendee
Blachman Biatch	Sophia	Healthy Communities Institute	Attendee
Blankenship	Sabine	German Consulate General SF	Attendee
Rochford	Kent	NIST	Attendee
King	Rachel	The Wall Street Journal	Media
Menn	Joe	Reuters	Media
Sposito	Sean	San Francisco Chronicle	Media
Arnocdy	Ben	Christian Science Monitor	Media
Cave	Tony	Not legible	Media
Shinal	John	USA Today	Media
Cougan	Kate	Not legible	Media
McMillan	Robert	The Wall Street Journal	Media
Yadron	Danny	Guardian	Media
Higgins	Joshua	Inside Cybersecurity	Media

Annex B- Public Participation Statements

Public Statement to the Commission on Enhancing National Cybersecurity

June 21, 2016

Russell C. Thomas[2]
George Mason University and Zions Bancorporation

Summary

Cyber security desperately needs institutional innovation, especially involving incentives and metrics. Nearly every report since 2003 has included recommendations to do more R&D on incentives and metrics, but progress has been slow and inadequate.

Why?

Because have the wrong model for research and development (R&D) on institutions.

My primary recommendation is that the Commission's report should promote new R&D models for institutional innovation. We can learn from examples in other fields, including sustainability, public health, financial services, and energy.

What are Institutions and Institutional Innovation?

Institutions are norms, rules, and social structures that enable society to function. Examples include marriage, consumer credit reporting and scoring, and emissions credit markets.

Cyber security[3] has institutions today, but many are inadequate, dysfunctional, or missing. Examples:

1) overlapping "checklists + audits";
2) professional certifications;
3) post-breach protection for consumers (e.g. credit monitoring);
4) lists of "best practices" that have never been tested or validated as "best" and therefore
5) are no better than folklore.

There is plenty of talk about "standards", "information sharing", "public-private partnerships", and "trusted third parties", but these remain mostly talking points and not realities.

Institutional innovation is a set of processes that either change existing institutions in fundamental

[2] I am a Senior Data Scientist at Zions Bancorporation and PhD Candidate in Computational and Data Science at George Mason University. This statement is my own and does not represent the views or interests of my employer.

[3] Cyber security includes information security, digital privacy, digital identity, digital information property, digital civil rights, and digital homeland/national defense.

ways or create new institutions. Sometimes this happens with concerted effort by "institutional entrepreneurs", and other times it happens through indirect and emergent mechanisms, including chance and "happy accidents".

Institutional innovation takes a long time – typically ten to fifty years.

Institutional innovation works different from technological innovation, which we do well. In contrast, we have poor understanding of institutional innovation, especially on how to accelerate it or achieve specific goals.

Finally, institutions and institutional innovation should not be confused with "policy". Changes to government policy may be an element of institutional innovation, but they do not encompass the main elements – people, processes, technology, organizations, and culture.

The Need: New Models of Innovation

Through my studies, I have come to believe that institutional innovation is much more complicated[4] than technological innovation. It is almost never a linear process from theory to practice with clearly defined stages.

There is no single best model for institutional innovation. There needs to be creativity in "who leads", "who follows", and "when". The normal roles of government, academics, industry, and civil society organizations may be reversed or otherwise radically redrawn.

Techniques are different, too. Fruitful institutional innovation in cyber security might involve some of these:

- "Skunk Works"
- Rapid prototyping and pilot tests
- Proof of Concept demonstrations
- Bricolage[5] and exaptation[6]
- Simulations or table-top exercises
- Multi-stakeholder engagement processes
- Competitions and contests
- Crowd-sourced innovation (e.g. "hackathons" and open source software development)

What all of these have in common is that they produce something that can be tested and can support learning. They are more than talking and consensus.

There are several academic fields that can contribute defining and analyzing new innovation models, including Institutional Sociology, Sociology of Innovation, and the Science of Science Policy.

[4] For case studies and theory, see: Padgett, J. F., & Powell, W. W. (2012). *The Emergence of Organizations and Markets*. Princeton, NJ: Princeton University Press.

[5] "something constructed or created from a diverse range of available things."

[6] "a trait that has been co-opted for a use other than the one for which natural selection has built it."

Role Models

To identify and test alternative innovation models, can learn from innovation successes and failures in other fields, including:

- Common resource management (sustainability)
- Epidemiology data collection and analysis (public health)
- Crash and disaster investigation and reporting (safety)
- Micro-lending and peer-to-peer lending (financial services)
- Emissions credit markets and carbon offsets (energy)
- Disaster recovery and response[7] (homeland security)

In fact, there would be great benefit if there was a joint R&D initiative for institutional innovation that could apply to these other fields as well as cyber security. Furthermore, there would be benefit making this an international effort, not just limited to the United States.

[7] See: Auerswald, P. E., Branscomb, L. M., Porte, T. M. L., & Michel-Kerjan, E. O. (2006). *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*. Cambridge University Press.

Society for Maintenance & Reliability Professionals

Statement Provided by John Ferraro

June 20, 2016

Commission Executive Director
U.S. Department of Commerce
National Institute of Standards & Technology
The Commission on Enhancing National Cybersecurity 100 Bureau Drive,
Stop 2000,
Gaithersburg, MD 20899-8900

Subject: Open Meeting of the Commission on Enhancing National Cybersecurity – CA SMRP Comments on Enhancing National Cybersecurity

The Society for Maintenance and Reliability Professionals (SMRP) appreciates the opportunity to comment to the Commission on strengthening cybersecurity in the digital economy. The maintenance and reliability of cybersecurity systems and critical infrastructure is essential to the security of our nation.

SMRP recommends that the Commission should focus on the promotion, development, and implementation of a strategy for evaluating the impact of the known as the Internet of Things (IoT) devices and systems as it pertains to cybersecurity and infrastructure for small to large-sized business.

I. SMRP Introduction and Background

SMRP is an over 5,000 member professional society formed in 1992 to develop and promote excellence in the maintenance, reliability, and physical asset management profession. SMRP members consist of engineers, operations managers, repair and reliability technicians, worksite and project planners, and other service providers. We are experts in specification, design, purchasing, installation, inspection, testing, maintaining, decommissioning, and asset disposal. SMRP members can help evaluate the impact of cybersecurity and cyberphysical impacts of critical physical assets.

Maintenance and reliability jobs are skilled positions that provide competitive advantages to the companies that have them. Companies with highly trained, certified engineers reap a variety of benefits, including lower operations and manufacturing costs, reduced onsite injury risks, reduced environmental risks, and increased net profits. Nearly every industry sector requires the services of maintenance, reliability, and physical asset management personnel, including energy, oil and gas, pharmaceuticals, automotive, government and military, petrochemical, education, and commercial. Our ranks are made up of senior reliability managers from such companies as Cargill, BP, General Electric, General Motors, as well as utilities, government facilities, and the organizations that support them.

SMRP members are uniquely positioned to identify the impact of cybersecurity implementation on the reliability of the infrastructure, generation, and commercial / industrial end users. SMRP has developed enhanced tools that provide best practice metrics, benchmarking and reference materials for maintenance and reliability improvement. SMRP's participation in global collaboration related tophysical asset management, which is a framework for managing complex systems, includes recognized certifications from reliability programs to asset management, such as the ANSI-certified Certified Maintenance and Reliability Professional (CMRP) as well as the Certified Maintenance and Reliability Technician (CMRT) and internationally organized Certified Asset Management Assessor (CAMA).

II. Cyberphysical and Cyberinformation Advancements through IoT Devices

With advances in cyberphysical and cyberinformation systems (known as the Internet of Things (IoT)), unparalleled opportunities for improved monitoring, operations, and reliability of systems have been made readily available to all aspects of personal, public, private, and commercial entities. However, through rapid advancement and deployment, significant cybersecurity issues and infrastructure vulnerabilities have arisen as organizations do not necessarily understand the impact of a full threat.

A majority of IoT systems are implemented as monitoring systems and related maintenance systems within organizations and via third party maintenance organizations. These have the possibility of producing weaknesses in information security (cyberinformation), which may include critical operational and financial information, and access to controls, which may include the ability to effect systems and infrastructure (cyberphysical). Specialized search engines, such as Shodan.io, can easily identify internet connected systems, including maintenance systems, which provide support for internet security professionals who are verifying the accessibility of their systems, as well as cybercriminals who are searching for vulnerable systems. A great many applications for all operating systems, such as those for supervisory control and data acquisition (SCADA) systems, are freely available that can access systems for remote monitoring and operation.

On November 15, 2013, a complex cyberattack was conducted on Target stores through credentials obtained from a third party HVAC service company. Once cybercriminals obtained access to a beachhead in the HVAC service company's contractor billing, contract submission and project management system, they were then able to use information provided via the portal to access Target's credit card terminals. From November 27 to December 18, 2013, cybercriminals gained access to over 110 million consumer credit cards via Target's email system.

At the present time, there is little to no understanding of the impact of cybersecurity issues resulting from third party vendors or on small to medium-sized manufacturing facilities.

III. SMRP Cybersecurity Positions and Recommendations

It is SMRP's position that while an emphasis on larger organizations is important for a last line of defense, preventing cyberattacks on small to medium-sized organizations, and those that provide services to large-sized organizations and critical infrastructure should be the main focus. It is SMRP's belief that an understanding of threats through IoT devices, contractors and subcontractors, regardless of size, and the development of cyberdefense processes will further reduce the risk to the economy and infrastructure of the United States and its allies. SMRP recommends a federal study on cybersecurityissues related to small to large-sized businesses and related infrastructure and third party support vendors including reliability and maintenance contractors and IoT suppliers; and the development of a process, or processes, to vet third party vendor cybersecurity and vulnerabilities.

SMRP also recommends research into the potential threat through the first line of defense and the inter-connectivity between companies, vendors, contractors and subcontractors with an overall goal to establish a cyberdefense strategy. This includes the evaluation of cyberinformation, cyberphysical systems and best practice methods to prevent infiltration and damage to the front-line organizations. In essence, this will have an additional impact on improving security for small to medium-sized businesses while reducing the number of attacks on larger organizations. Because current business models for larger organizations include contracting services through smaller companies, this presents an inherent problem as smaller firms are more prone to cyberattacks and can inadvertently exploit sensitive information from larger organizations. As a result, SMRP also recommends including the development of a vetting process and identification of tested and secure IoT devices and related systems and software for potential vulnerabilities.

Summary

The maintenance and reliability of cybersecurity systems and critical infrastructure is essential to the security of our nation. We need to better understand the threats posed through IoT devices, contractors and subcontractors in order to truly reduce the risk to the economy and infrastructure. SMRP believes in a sound cyber-defense strategy and that research into the potential threat through the first line of defense and the inter-connectivity between companies, vendors, contractors, and subcontractors is the first-step towards this goal.

Thank you for your consideration and please do not hesitate to contact me if you have any questions.

Sincerely,

John Ferraro

John Ferraro
SMRP Government Relations Director
529 14th Street NW, Suite 750
Washington, DC 20045
Phone: 202-207-1121
Email: jferraro@smrp.org