Commission on Enhancing National Cybersecurity

Established by Executive Order 13718,
Commission on Enhancing National Cybersecurity

New York University School of Law – Vanderbilt Hall
40 Washington Square South, New York, NY

MEETING MINUTES

The Commission on Enhancing National Cybersecurity was convened for its second public meeting at 9:02 A.M. Eastern Time on May 16, 2016 at the New York University School of Law in New York, New York. The meeting in its entirety was open to the public. For a list of meeting participants, please see Annex A.

Welcome

Zachary K. Goldman, Executive Director, Center on Law & Security; Adjunct Professor of Law, New York University School of Law; Co-Founder, NYU Center for Cybersecurity
Trevor Morrison, Dean, Eric M. and Laurie B. Roth Professor of Law, New York University School of Law

Mr. Goldman welcomed the Commission to NYU School of Law citing there is no better group of people to help think through the types of challenges that we face. The Commission was established pursuant to an Executive Order signed in February 2016, with a goal to create actionable and sustainable recommendations to increase preparedness aimed to deter, disrupt and interfere with malicious activity, and help the country figure out how to respond and recover from cyber incidents. Cyber-attacks are a threat that are of the greatest strategic significance that manifests itself as a tax on small and large private companies, making it a challenge to devise a sustainable set of solutions. In February, the President also announced measures aimed at achieving more coherent and cohesive approach to cybersecurity.

Mr. Goldman introduced Mr. Trevor Morrison, Dean of the New York University School of Law to offer welcome remarks.

Mr. Morrison thanked Mr. Zachary Goldman and Mr. Samuel Rascoff for their work with the NYU Center on Law, the Center for Cybersecurity, and for assisting with hosting the Commission proceedings at NYU. He stressed the importance of the proceedings and the great responsibility of the Commission to think through issues that are facing us now in the cybersecurity space. Mr. Morrison stated that the Commission has deep expertise and welcomed them to NYU.

Opening of the Meeting

Kiersten Todt, Executive Director of the Commission on Enhancing National Cybersecurity, NIST

Commission Executive Director Ms. Kiersten Todt introduced Commission Chairman Donilon for opening remarks before the first panel on finance.

Opening Remarks

Thomas E. Donilon, Commission Chair, O'Melveny & Myers, Vice Chair, Former U.S. National Security Advisor to President Obama

Chairman Donilon thanked Professor Goldman and Dean Morrison for hosting the commission proceedings at NYU. Cybersecurity has become one of the most pressing challenges facing the country. Cybersecurity attacks have become one of the most pressing challenges for our country, government and American citizens. There is important work to be done.

The meeting today is the first of a series of workshops that will be held around the country. Each workshop will have a specific topical focus depending on the region where the meeting is located. While the panels today will focus on finance, insurance and research and development, the Chair encouraged the panelists not to confine their remarks to these specific areas given their breadth of general cybersecurity experience.

The goal of the commission is to develop a national agenda for the next 5 to 10 years as set forth by the Executive Order. In the nearer term, the goal is to set the agenda for the next President. The Commission's report is due on December 1, 2016, and will be presented to President Obama, and to the president-elect thereafter.

Today's panels will work through three areas:

- Cybersecurity experience and challenges to the financial industry
- Insurance in the U.S. and the power it has to drive standards and mitigate costs
- Research and development and the latest technical solutions for cybersecurity

The financial sector has been more visible and successful due to having more cybersecurity resources, but still faces a series of challenges.

The commission hopes to learn what points can be taken and broadened, and learn what challenges are still prevalent. History has shown that the insurance industry can be very powerful in driving standards and mitigating cost in the United States. The research and development panel will think through recommendations for the latest technical solutions and the country's R&D investment agenda for the next 5 to 10 years.

Panel 1: Finance

Phil Venables, Managing Director and CISO, Goldman Sachs
Greg Rattray, Managing Director, Head of Global Cyber Partnerships, JP Morgan Chase & Co.
Marc Gordon, Executive Vice President and CIO, American Express

Marc Gordon, Executive Vice President and CIO, American Express

Mr. Gordon began by stating that he planned to focus on three areas including the threat landscape, provide some thoughts on how the government can help enhance the security and protections across the financial spectrum, and discuss the differences in cybersecurity financial services.

In recent years, there has been a substantial increase in cybersecurity threats. There are tens of thousands of attempts to scan financial companies' network perimeters daily. Across the industry, Mr. Gordon estimates that there are well over 100,000 attempts every day. On average, American Express receives five to ten new, broad-scale and focused phishing campaigns every day. Using threat indicators as a proxy for the level of activity, Mr. Gordon indicated that they see 30,000 or more threat indicators every week and more than a million and a half o an annual basis.

He continued by providing some recommendations on how the public and private sector can work together o cybersecurity efforts. First, focus on information sharing. This is one of the best return on investment actions that the private and public sectors can initiate. American Express, along with others in the industry, supported legislation that passed at the end of last year. There is a strong belief that one company's attack can be the entire nation's defense. There is no excuse for the same attack technique or technology working twice in our country, but it does and often.

Mr. Gordon stressed that he would like to see aggressive acceleration of real-time information sharing across industry. Progress has been made. However, at the pace the country is moving, information sharing across industries is probably years away. Information should be shared in real-time, but would settle for getting the information the next day after an attack. The capabilities, legislative support and technology are in place for information sharing. It is not clear how forward- leaning the government would be in sharing government cyber threat information as compared to cyber threat information that is shared in and across private industry.

He encouraged the Commission to look at ways to accelerate the government's information resource sharing as it would be very helpful in protecting businesses and their customers.

The second recommendation is for the government's role at the front end of a cyber attack's life cycle to be clearly defined and forward-leaning. It is often unclear what role the government plays in preventing attacks.

The third area of focus is on the financial services industry, and that the industry has a deeply embedded risk management mindset and skillset which differentiates it from other industries. The following eight differentiators that separate the financial services industry from other sectors are worth noting: 1) Inherent risks and residual risks, 2) Investment levels, 3) Level of collaboration, 4) Interaction with the start- up community, 5) Application of big data, 6) Separation of personal and professional networks, 7) Engagement with cloud providers, and 8) Identification factors to protect customer's identities during payment processing.

Mr. Gordon thanked the Commission and concluded his remarks.

Greg Rattray, Managing Director, Head of Global Cyber Partnerships, JP Morgan Chase & Co. (JPMC)

Mr. Rattray began by stating that his remarks will focus on the need for stronger private and public sector collaboration and provided background of how JPMC views cybersecurity, the depth of its efforts, and the need to uplift how it works with the government. Cybersecurity is a fundamental concern of JPMC and its clients, with many cybersecurity efforts appearing in the top 10 objectives for the company. In 2016, JPMC plans to invest $600 million in cybersecurity and will have 2,000 people working in this area.

The company works closely with the Department of Treasury, Department of Homeland Security,

the FBI and others on variety of projects, including automated information sharing, and is highly supportive of the NIST Cybersecurity Framework as a basis for constructing cyber programs and oversight. They have also participated in a series of exercise events offered by the Department of the Treasury and the International Cyber Center (ICC) at George Mason University to practice capabilities in order to plan how to jointly respond to cyber events.

In general, the government has very strongly communicated that cybersecurity is a major challenge and has established broad programs to engage in partnership with the private sector. However, in terms of enhancing cyber defense, the programs do not necessarily meet the needs of firms like JPMC that have already invested in developing mature cyber capabilities.

JPMC, and firms like it, seek to build partnerships with the government that have a prioritized focus on providing dedicated support capabilities for large firms like JPMC that have more resources and have already established robust cybersecurity programs. JPMC understands the strategic importance of cybersecurity and will continue improving its cyber defense efforts. However, he stressed the following significant issues that he hopes the Commission will consider when making recommendations to the government on how to improve collaboration with the public sector:

1. Information Sharing – Producing predictive, actionable cyber threat intelligence driven in part from our requirements, and including access to dedicated government classified reporting and services. The public sector needs to work with the private sector industrial base cyber-crime center. There is no dedicated service for the financial services sector to get access to the right government reporting.
2. Intelligence and Disruptive Operations – National-level efforts need to provide intelligence and conduct disruptive operations against organized crime, in addition to efforts against potential nation-state adversaries. Criminal attacks against financial services companies and associated utilities can have wider-ranging national impacts and must be countered.
3. Crisis Response and Contingency Planning – Improving crisis response capabilities via increased investments in sector exercise programs, establishing joint crisis response protocols, and conducting joint contingency planning for destructive or large-scale attacks. We believe systemically important institutions must receive dedicated support in these efforts.
4. Improved Protection of Core Financial Utilities and Infrastructure – Improving cybersecurity and fraud prevention integration with core financial utilities (such as Fedwire).
5. Prioritize Improvement of the Cyber Environment – Drive efforts with Internet infrastructure and ecosystem providers (such as email providers, Internet Corporation for Assigned Names and Numbers (ICANN), and domain registrars) to reduce malicious activity and improve the environment for clients and customers.
6. Limiting Financial Sector Stress Due to Cyber Event – Ensuring government resources and leadership attention are devoted to understanding and addressing potential impacts to public and market confidence with clear liquidity guidelines, settlement and cash distribution procedures, updated regulatory guidance and a communications strategy in cases of systemic cyber-attacks on the financial sector.

7. Efficient Access to Government Resources for Assistance during Disaster Response – expected to result in more effective response and recovery.

In order for these priorities to be effectively implemented, the U.S. Government should make clear across all departments and agencies that prioritized and enhanced support to systemically important firms is authorized and required to protect our nation's critical infrastructure.

The Chair thanked Mr. Rattray for his remarks.

Phil Venables, Managing Director and CISO, Goldman Sachs

Mr. Venables stated that he would be sharing five recommendations that are complementary to the recommendations provided by the other panelists, but wanted to first mention the importance of emphasizing that cybersecurity is not the only technology or information risk that we have to deal with as a nation, or a sector. There are many risks in digital business and society; for example, systems and software reliability, predictability, resilience, and capacity. Large parts of our society are challenged with how we digitally transform and manage all of these risks. Cybersecurity is definitely important, and may be the most critical concern given the potential impact of failure, the increasing number and sophistication of threats, and the supporting and supported role in managing all these risks.

Mr. Venables provided the following five recommendations to create and sustain national cybersecurity risk mitigation:

First, integrate cyber security into the fabric of organizations:

- Risk management must be integrated. It is imperative to ensure that cyber-security risk management is embedded into the main risk management and strategic processes of organizations from the board, to risk committees, to the wider processes of strategy formulation, product development, investments and acquisitions; both within the organization and across its extended supply chain.
- Technology must also be integrated. Experience and observation shows that good technology management/hygiene promotes solid cyber-security, and that for a controlled technology environment to also be agile and cost-effective, it has to have risk mitigation designed in – meaning ambient controls.
- Resilience and recovery must also be integrated. However, no matter how well risks are managed, something may still go wrong: misidentified risk, a control breaks, new adversarial technique, an unforeseen circumstance or an insider threat. It is important to build the muscle memory of effective detection, containment/response, and recovery through continuous scenario planning, drills and exercises.

Second, public and private partnerships must be sustained and improved:

- There has been immense progress in establishing and coordinating national cyber-security measures, from sharing threat intelligence to coordination of capabilities needed to respond to particular events and incidents.

- However, we should recognize that threat sharing alone is not enough. It is important to share actual incident data and the vulnerabilities or other factors that led to incidents in a suitably anonymized and protected way, so that everyone can benefit from that experience.
- Information sharing with the private sector requires handling classified material in some cases, requiring potential recipients to hold security clearances. Rather than solely increasing the number of cleared individuals within the private sector, the preferable course of action should be to declassify/desensitize information as much as possible so it can be utilized more readily.
- We also need improvements in international as well as cross-sector coordination. While cyber-security is a clear imperative for our national security, we should remember that many of our businesses are internationally connected and exposed to multiple threats in the physical and digital world that extend beyond our national borders.

Third, harmonize rules and guidance:

- There is a multiplicity of frameworks, standards and guidelines for cyber-security; many of which are effective and practical, but organizations can find it difficult to decide which to utilize.
- We recommend that we continue to emphasize the NIST Cyber Security Framework, and in particular, the development of associated profiles subject to appropriate certification schemes.
- We should further raise awareness of the need for organizations to more firmly adopt a strong set of baseline controls, such as the Center for Internet Security's Controls for Effective Cyber-Defense.

Fourth, improve capabilities amongst people, processes and technologies:

- There needs to be continued emphasis on embedding controls into all available technology products and services, instead of embedding controls late in the design or development cycle. This practice is often ineffective and is an inefficient use of resources. We need secure products, not just security products.
- Similarly, we should recognize that cyber-security risk mitigation is not solely the responsibility of designated cyber-security professionals but also resides, in the domain of leadership, risk managers and engineers at all levels of organizations. Mr. Venables supports a national program to embed cyber-security training into all academic and professional training and qualifications. We need more security-minded people, not just more security people.
- Mr. Venables fully endorses all efforts to deal with the shortage of trained cyber-security professionals to help manage these risks, but also notes that there is a wider issue: the productivity of the cyber-security professionals we already have, and more needs to be done by government and industry to improve tools, processes and the orchestration of defense across multiple platforms to get the most out of the people we have.

The final recommendation is to design for defensibility:

- Our goal should be to design our technology and information processing environments to be more inherently defendable: able to deflect, be adaptive in response to, and to continue operation and prove resilient in the face of attacks.
- Such defensibility includes not only currently available technology, but much active research and development that needs to be brought to market faster with government help or other incentives.
- Additionally, much work is needed to assist organizations in transitioning from complex legacy environments to simpler and more defendable environments that are more comprehensively enclaved and less susceptible to one successful attack causing wider compromise. Finally, it is worth remembering that despite the advantages of mass and constant interconnectedness, there may be some things so critical that they should remain isolated under different and higher assurance of control.

Mr. Venables thanked the Chair and concluded his remarks.

Panel 1 Discussion

Commissioners of the Commission on Enhancing National Cybersecurity

The Chair thanked the panelists for their statements and began the discussion by focusing on the internet of things.

Mr. Donilon: In reference to Mr. Venable's fourth recommendation on ensuring technology products and services embed security as a priority from the start, what mechanisms should be utilized to get this dynamic going in the private sector?

Mr. Venables: There should be communication of expected standards, including public safety standards. Organizations such as NIST have been working on providing recommendations in this space. Some of the devices that we use in society are embedding this technology and have significant safety dimensions to them. It would not be inappropriate for this to be seen as a set of safety standards for certain products.

Mr. Donilon: Essentially, we should set the standards and find a mechanism to communicate to consumers the products that have met these standards.

Mr. Gordon: There is n laboratory equivalent available in cyber to determine if a product has been tested and if they followed the standards.

Mr. Donilon: What are you seeing as far as market dynamics and the availability of talent? If we are short, what can we do about it?

Mr. Rattray: There is a recognized lack of talent overall. The National Initiative for Cybersecurity Education set forth by the President is a good resource designed to provide information regarding the cyber workforce. The initiative does not pay for people to get trained.

The challenges cannot be resolved quickly as the skillsets that are necessary for many jobs are experiential and not academic, and both are needed. The challenges have outpaced the amount of time needed to grow our cybersecurity professionals.

Mr. Venables: When talking about cybersecurity workforce development, there is a need to determine the type of professionals that are being referenced as there are many different skillsets, some of which can be trained and some are more specialized and can take up to 15 years to accumulate expertise.

Mr. Gordon: The field is very competitive and the cost for cyber security professionals has increased substantially. Other industries have now woken up to the threat and are actually hiring cyber security professionals from the financial services industry. The challenge is not being able to find entry talent but determining mechanisms to accelerate the speed of their effectiveness.

There is a great benefit of the internet with it being open. Is there an alternative to the openness of the internet by prioritizing elements of critical infrastructures and doing things in the way they would have been done pre-internet?

Mr. Venables: Things will always need to be connected, if not for commercial value but also to manage the level of other risks. There is value in more simple component-based systems which can provide more predictable behavior. However, that is not how we have evolved over the last 30 years. Organizations, including CMU and the Software Engineering Institute, are conducting research on how to transition from legacy, more complex systems to more simple designs which should have increased focus and concentration.

Mr. Banga: What is the rule that the Federal Government will develop standards versus the private sector?

Mr. Venables: There are several instances in which the public and private sectors have worked, and continue to work, together on developing certain standards. The NIST framework is a classic example. Developing standards should be a collaborative effort.

Mr. Gordon: Universally, the NIST framework is thought to be the best collaborative effort between the public and private sectors.

Mr. Banga: Small businesses seem to be the weakest link as they are more vulnerable as an entry way to attacks due to lack of resources. Do you address this issue with your smaller partners?

Mr. Rattray: The financial sector often considers how it interacts with others and spends a lot of energy to bring a broader and broader set of players together. There are mechanisms for smaller institutions to participate. The NIST framework applies broadly and all institutions, independent of scale, are aligning with the same basic principles and baseline controls.

There are weakest link aspects because every institution is not equal in terms of risk. Strengthening the entire set of institutions is good and focusing on the key aspects of the system that may need specific investments into operations and support is also beneficial.

Mr. Venables: The financial sector is keenly aware of designing not only large firm solutions but solutions that small firms can quickly adapt.

Mr. Gordon: I is difficult for small and medium size businesses to translate the NIST framework into their environment. They work with many startups to assist. The commission should recommend efforts that would make the NIST framework more actionable for small and medium size businesses.

Mr. Donilon: It is not only a small and medium size business issue, but also with weaker banks, such as the Bank of Bangladesh breach. What do you all think about this problem?

Mr. Rattray: As a public and private team, we need to make sure that the payment and clearing systems are as strong as the large institutions when a weakness has been identified. JPMC is working on efforts in this space.

Mr. Alexander: Al of the panelists mentioned a need for private and public partnerships that will assist with how to interact with the government in timely manner while also being classified as much as possible. It will be key to addressing serious issues that may arise that are similar to the Bank of Bangladesh breach. Are you suggesting need for real-time public-private partnership?

Mr. Gordon: Yes, there is a need for front-end communication. Currently, there is little interaction with the government on how to prevent attacks.

Mr. Venables: It is important to look at the different array of threats.

Mr. Rattray: The financial sector has been working on developing contingency plans for the top ten scenarios and would like for the government to be involved. Joint contingency plans will enable all aspects to be thought through in order to formulate quicker responses.

Mr. Palmisano: Has the policy issue with information sharing been resolved?

Mr. Gordon: The policy has been enacted. It has to be activated and tested.

Ms. Anton: What is the worst case scenario for the financial sector as far as impact? What are the ways that this scenario could have been prevented and what is needed between private and public partnerships to prevent this type of scenario?

Mr. Rattray: It is better to identify a top set of contingencies, practice responding to them, have the right procedures in place and build a contingency plan for each in lieu of identifying a single scenario. The role of the government in this area needs to be strengthened. He recommends that there be investment in contingency planning and response.

Mr. Venables: *(Referencing Mr. Rattray's comments)* There should not be a focus on a single worst case scenario. The work can be deeper and more of a resource challenge than a conceptual challenge.

Mr. Gordon: Some work has been done by DHS to identify some scenarios.

10:45 A.M. – 11:00 A.M. Break

Panel 2: Insurance

Lee Garvin, Director of Risk Management and Workers Compensation, JetBlue Airways
Peter Beshar, Executive Vice President and General Counsel, Marsh & McLennan Companies, Inc.
Randal Milch, Former General Counsel, Verizon; Distinguished Professor, NYU School of Law
Catherine Mulligan, Senior Vice President, Head of Professional Liability, Zurich, North America

Mr. Donilon welcomed the panelists and mentioned that insurance was not listed in the Executive Order. However, the Commission viewed the topic as an important component in mitigating risks and is eager to learn ways to support the industry in this effort.

Randal Milch, Former General Counsel, Verizon; Distinguished Professor, NYU School of Law

Mr. Milch thanked the Commission for inviting him to the proceedings. He commended the Commission for investigating the role of cyber insurance as part of its effort to enhance national cybersecurity and believes that it is squarely inbounds of the Executive Order and charter. A well-functioning insurance market does have a chance at lowering cyber risks nationally over time. Many of the issues outlined in his formal statement will be fixed over time as long as the cyber insurance market remains profitable one. I will be several years before it is determined whether or not the market is profitable; however, he noted that in his remarks he would propose several recommendations that could help accelerate its viability.

well-functioning market has three attributes. The first is related to information. The need for information sharing has been mentioned often and the passing of the Cybersecurity Information Sharing Act (CISA) was a great event. However, it needs to be stood up in a way that makes sense. For insurance to work, there needs to be a general level of understanding of cyber risks and how to insure against them. Also, an understanding of where risks fall within the risk spectrum enables underwriters to determine what to charge and provides information on how to lessen risks.

Insurance brokers, insurers and insureds do not have adequate time for meetings to deeply discuss cyber insurance issues. Mr. Milch does not have any recommendations on how the Commission can mediate this resource allocation issue and feels that this is something that the industry would have to resolve on its own. At this stage, insurers receive a better premium or more coverage if they have a better response capability, meaning the right letters get sent to the right people once a breach has occurred. Prevention does not count as much as response at this stage.

Insurer-required assessments of the prospective insured' insurance policy are rare. This would not be rare in a well-functioning market because there would be more information about the insured's capabilities and the ability to provide customized insurance.

The second aspect of a well-functioning cyber insurance market is the ability to have after-action forensic reports. This capability is susceptible to some external assistance. A "carrot" would have to be provided to induce companies to share reports with appropriate organizations that can rapidly disseminate the information on how a successful attack occurred. This information is being closely held by companies and needs to be released in some way. Mr. Milch suggested a less bureaucratic approach if the Commission was seeking to emulate the Patient Safety Quality Improvement Act of 2005, which has had slow implementation.

Citing standards is the third aspect of a well-functioning cyber insurance market. It is important to note that standards can work and provided the Payment Card Industry (PCI) standards as an example. In the past, insurers would give insureds time to meet PCI standards. However, now insurers are more likely to deny companies that are not PCI compliant. Standards can be powerful tools in upping the insurance company's game. Currently, there is a situation with standards being set in the wrong way. In addition, there will be a rise in sector-specific regulators, which is not good because it raises due process and confidence problems.

The Federal Communications Commission (FCC) and the Consumer Finance Protection Bureau (CFDB) are not natural centers of excellence for cyber security regulation. The industry is on the

cusp of a lot of private lawsuits being instrumental in setting standards which will also not result in developing good standards quickly. There are lengthy ways of eventually getting standards which will be a painful process.

Standards should be developed in sections, and we need to determine who is going to set the standards and enforce them. One way for the government to get standards completed quickly is by requiring the use of standards for its own purchases for anything that is internet connected. There is a need for cyber insurance to become ubiquitous and a need to raise basic cyber hygiene citing that the industry is at the "wash your hands" stage.

Peter Beshar, Executive Vice President and General Counsel, Marsh & McLennan Companies, Inc.

Mr. Beshar began his remarks by citing that recent cyber-attacks in both the public and private sectors have shown neither government nor industry has the ability to solve this issue on their own. There is need for mindset that we are all in this together. In the prior panel, virtually every speaker spoke about the need for a private/public partnership. The question is, how can this be achieved? Books such as *Freakonomics* and *Nudge* have shown that providing incentives can drive the types of behaviors the Commission is looking to achieve. If the incentives are right, then the behaviors will follow. The focus today is on two tools that have the potential of creating those types of incentives. The first is cyber insurance and second is the Support Anti-terrorism by Fostering Effective Technologies Act (SAFETY).

Cyber insurance matters because history has shown that the insurance industry has been at the forefront of confronting new perils as they approach. Due to its visibility across multiple industries, it has the ability to identify and use appropriate incentives to drive people towards best practices. He referred to his written statement which highlights Benjamin Franklin's achievements of not only introducing the first all-volunteer fire brigade, the Franklin stove and the lightning rod, but also with creating the first insurance company. Technological innovations coupled with best practices can be driven through underwriting practices. Deaths and fatalities in the work place are more modern examples. Within the last two decades, workplace deaths have decreased by 35%. They have decreased significantly not because it could be mandated but because incentives were provided to urge companies to adopt best practices.

What role can cyber insurance play to address the new perils of cyber? If all that cyber does is simply pass risk onto policy holders like Verizon or onto insurers like Zurich, it is helpful as a financial matter, but not really significant as policy matter. Unfortunately, the underwriting process creates a set of incentives on companies like Verizon as well as small and medium size businesses. The challenge is how to drive behavioral change in enterprises that believe cyber is not a real risk for them. He cited as examples the air condition vendor and take-out delivery service that have recently endured attacks.

Simple things, such as using the NIST Framework and ISO standards, can put companies in a position to better decrease their risk profile and present themselves as better insured. Once the policy has been placed, the incentive then shifts to companies like Zurich because they now have hundreds or thousands of policies in which they want to do what they can to try and mitigate or totally avoid the risk that the policyholder actually places. Because of this, many insurers are offering an array of services to assist policyholders that have been positive, including anomalous

behavioral monitoring and rapid response services. This is essentially the promise and power that cyber insurance potentially offers.

The second tool that has the potential of creating incentives is the Safety Act. The threat has changed profoundly. Much of the focus in the past 2 years has been on data breaches involving credit cards at large retailers and social security numbers at the health care companies. In the wake of the attack on the Ukrainian power grid and other various recent incidences, people are really beginning to understand the specter of what it means to have attacks on critical infrastructure and the control systems that underpin them. Now that we are moving from traditional terrorism into world cyber terrorism, there is a need to try and take some of the lessons learned over the last 15 years.

Congress and policy makers will need to determine how to fundamentally embed cyber terrorism into the Terrorism Risk Insurance Act and the Safety Act that were both passed in the immediate aftermath of 9/11. There is also a need to urge companies to innovate new, sophisticated anti-terrorism products and services that have the potential to mitigate risks of terrorism. He mentioned that DHS has now granted Safety Act designations and certifications to over 800 companies and encouraged the Commission to take the mechanism of the Safety Act to entice companies to innovate and then have it validated.

Mr. Beshar thanked the Commission for its time and concluded his remarks.

Lee Garvin, Director of Risk Management and Workers Compensation, JetBlue Airways

Mr. Garvin's remarks focused on the buyer's perspective in terms of cyber insurance. His role is risk management and determining strategies to successfully protect companies and their assets. Mr. Garvin noted that he is not an IT expert, but it is imperative for him to get involved in order to ask the necessary questions. Cyber insurance is a new product and many companies believe that they do not need it. Eight years ago, he had difficult time selling the idea of cyber insurance to his company although 85% of sales were coming from the internet. It is still needed today, as the risks have increased substantially. Insurers expect his company to keep spending money in order to be better and safer than the competition. If only standards are implemented, the cost incurred for his company to become compliant as well as its savings on the backend would be a concern. Best practices are different as it would only be an underwriting issue. JetBlue decided not to pursue the Safety Act because of the cost involved to implement it internally.

In addition, because the company does not have a cargo department, it was not in their best interest to implement the act. Mr. Garvin mentioned that i the act ever extends into an area that holds value for the company, he would definitely propose it to his board of directors because he will be able to validate the return on investment. Knowing whether an attack is against his company specifically, or against America, in which his company was adversely affected is an issue. An attack against America should include some protection built in when buying insurance.

Statutory penalties are also an issue and Mr. Gavin expressed concern about what is considered a settlement and a fine. There are 50 different state governments with different policies and rules, which causes difficulty in this area and it needs to be wrapped together. Reporting these penalties is a concern. Often the company is not aware that there is a breach until late in the process. In

addition, the company has to be quiet while under investigation, but is also at risk of backlash for not publicizing the breach. There is a need to remedy this disconnect because if there is a leak of personal information, the company becomes liable. Coverages for cyber insurance are broad. The company purchases it anyway, but this is not sustainable. He is interested to see where this goes in the long term.

Catherine Mulligan, Senior Vice President, Zurich North America

Ms. Mulligan thanked the Commission for the opportunity to provide insight on professional liability insurance. The $2 billion liability insurance industry is now at a critical point of loss and potential loss in the courts with property damage, bodily injury, business interruption, and supply chain concerns pushing the industry to move forward into new risk management techniques and coverages. It is also pushing underwriters to evolve their understanding of complete exposure.

It might be useful to differentiate between what capacity is currently available and what will possibly be available in the future. The current marketplace focuses on network security and privacy liability and has ample capacity in the neighborhood of $500 million. Network security involves cyber breach issues, while privacy events can occur simply by misplacing paper. The Federal Insurance Office Annual Report indicated that billion dollar capacity is needed; however, it did not state what was meant by cyber insurance. There is really no such thing as cyber insurance and the term is colloquialism for network security and privacy liability. The full scope of cyber as peril is a network event that is bringing to bear some cause of loss. Currently, the industry is trying to determine how to insure for these losses.

Information on this effort should be forthcoming in the latter part of 2016 and in 2017. The question has been: should the industry add additional coverages onto this already unwieldy product, or, should they push cyber-as-a-peril into an existing product such as property, home or general liability insurance. How do they get the underwriting expertise to proceed in these areas?

There is ample capacity in the network security and privacy liability space. Seventy five percent of the premiums are written by five or six primary markets and are not evenly distributed amongst industry segments. Most of the buyers consist of highly regulated industries and those with the most personally identifiable information and personal health records, as well as larger companies with billion-dollar-plus brands. Diversification is still needed for this type of portfolio. Small and mid-size enterprises are slower to purchase the insurance because they assume they are not a target, although the data shows otherwise.

Another component that will drive enterprises to purchase the insurance is through development of the industry's actuarial knowledge. In North America, all commercial enterprises have been purchasing general liability insurance regardless of size or industry segment for decades. The industry has been able to slice general liability data to refine and price other types of coverage. However, the data is not available to extrapolate for use of refining and pricing insurance for cyber.

Loss reporting is an additional challenge. Notifications to insurance carriers often do not occur. In some instances, law enforcement has advised insureds to not disclose that there was a loss to their insurance, which makes it difficult to adjust the loss properly. Additionally, outside counsel

will often cite that information is client-privileged and therefore, will not provide the necessary reporting to make claims whole. The data collection does occur over time as the losses and lawsuits go through the system in order to determine the appropriate direction.

Aggregation is another area of concern for the industry. Aggregation by line of business makes enterprises susceptible to shareholder suits if a cloud service goes down or another major external breach where customers are at risk occurs. The insurance industry is regulated industry and they are being asked for prudence in this area and regulators are asking insurers to be thoughtful in how fast they are growing. There is a balance between delivering customer needs and growing in a thoughtful and prudent way.

The industry is looking to refine underwriting by sector. Cyber hygiene is a challenge with achieving this goal, which the industry is trying to overcome. Ms. Mulligan echoed what the previous panelists stated about information sharing and noted that the insurers are not aligned on the best practices. Some underwriters may see the need for the Payment Card Industry (PCI) and others may not.

The other issue that will need to accompany new coverages in the expanding world of cyber as a peril is business partners providing assistance with risk management issues that are increasing. The industry has been teaching resiliency instead of protection. Therefore, one of the challenges has been determining how to fit the need for help into the insurance process. This need is critical as insurers are sharing that they are challenged with how to communicate key exposures and controls.

PANEL 2 Discussion

Commissioners of the Commission on Enhancing National Cybersecurity

Mr. Chabinsky: Am I hearing correctly that companies are getting actual direction from law enforcement not to provide information to their insurance carriers without timelines?
Ms. Mulligan: The loss notification will come in bare bones. The feedback that I have been receiving from insurance brokers is that the companies are saying that law enforcement is stating there is a certain amount of data that cannot be shared with the insurance company.
Mr. Chabinsky: My recommendation is that the industry begin to request that insureds obtain documentation from law enforcement citing this information.
Mr. Chabinsky Is there a requirement to report a cybercrime to law enforcement?
Mr. Lee: It is not a requirement outside of what is required by the state attorney general.
Ms. Mulligan: Not every incident requires law enforcement. I would be helpful to have standardization for all states instead of having 47 different laws in place.
Mr. Chabinsky: What is the government doing well?
Mr. Beshar: Notification of breaches from the FBI and Secret Service to companies is something that the government has done well. However, over the last 2 to years, the government seems to fault companies for not having the right systems in place to combat risks instead of the actual perpetrators.
Mr. Chabinsky: Is it not allowed by law for insurance companies to cover government-imposed penalties or is it market-driven?
Ms. Mulligan: would have to get back to you on that.

Mr. Beshar: I varies. In some places, it is against public policy to d that. If you look at the outstanding judgements to date versus the amount of fines that people have to pay for privacy infractions, you may understand why insurance companies may be reluctant to pay the latter.
Mr. Chabinsky: For our perspective, I am trying to figure out if it is market-driven or if the insurance companies cannot do it because they are not allowed.
Ms. Mulligan: In some instances, the insurance companies are not allowed to pay government-imposed penalties but there is also a practical challenge on how to price it.
Mr. Milch: The Patient Safety and Quality Improvement Act (PSQIA) does provide a recommendation. The interaction of law enforcement is very transient and not the most difficult problem that the Commission has to worry about. Standards and best practices gathering is more important.
Mr. Palmisano: The nuclear industry has suggested that the government and insurers should work together. Is this something we should advocate?
Ms. Mulligan: In regards to information sharing, DHS has put together a working group to help to mitigate loss and improve standards. They have made recommendations by gathering ideas from the insured marketplace and CISOs and now the question is who would manage the process. They all agreed that it should be someone in the private sector in this role, but there is still the issues of anonymization, getting the reporting in a safe way and having liability protection. We are seeing value with insurers using captives which can potentially pool out, expand out.
Mr. Alexander: The impression is that the private sector has more of the risk than the public sector. Is there a place where the government should step in?
Ms. Murren: How do you think of the framework within the healthcare industry?
Mr. Milch: Ransomware is a substantial issue targeting the healthcare industry.
Mr. Garvin: I is important to note there needs to be a distinction on the type of loss. The personal is only about $10 million, which is not significant enough. The major loss is in the infrastructure. Don't think it is great threat. Shutdowns and cyber-attacks are more critical. There is nothing to indicate the loss of private information causes the greatest risk. There is a question of whether it should be easier for people to replace their own identity, and how can someone re-establish themselves as themselves through a more convenient process. Public messaging in schools can be effective. There is a need for more to be done about messaging on corporate and government cyber actions. There can be better technology. The fingerprint button is a great advance. However, we are not sure how to use browsers more safely.
Ms. Mulligan: There has been a dramatic increase in electronic health records. The privacy potential risk is high. NIST, DHS and multiple stakeholders are working on the problem. The Health Insurance Portability and Accountability Act (HIPPA) regulations are evolving.
Ms. Anton: What drove the underwriting of privacy as an insurance area?
Ms. Mulligan: As the world became more networked, it has evolved to bring in the privacy breach and cost to respond to claims. Insureds were asking for first-party cost to be covered that they were incurring to mitigate a response.
Mr. Beshar: I is assumed that we have these mandatory notification laws, but this is not the case. There is a need for improving the notification process.
Mr. Gallagher: How much penetration is needed to make a difference in the market?
Ms. Mulligan Incentives are needed in order for smaller entities to purchase cyber insurance.

There are questions of whether it can be included in existing policies.
Mr. Garvin: Some of his vendors have cyber extension on CGL policy. The return on investment is a concern.
Mr. Gallagher: How concerned should we be if the insurance market does not move?
Ms. Mulligan: Having the differentiation would be good and is currently a challenge. There is a need for more benchmarking.
Mr. Milch: There is a need to differentiate amongst vendors. In addition, there is absence to judge if a particular software is good on security. Maybe this is an area in which the commission can help.
Mr. Banga: There is need not to dismiss small businesses as they are often the entry point. How do you manage incentives at premium prices when there are 4 state regulators?
Mr. Milch: The industry would like for the Commission to help us solve this issue.
Mr. Lee: How would you go about finding the right threshold for technology?
Mr. Milch: Encourage technological innovation. Determine new cutting-edge ways for threat detection and prevention. You have insurance up to a certain point. Also, urging the power companies to be more forthcoming with sharing information, companies to refine information and provide incentives are ideal.
Mr. Garvin: He is a component for knowing that his company is protected by the government at a certain point. If they are spending money, he would like to see a cap.
Mr. Milch: There needs to be a standard for getting incentives. There are several questions to be asked for any company that eliminates risks. When you eliminate risk, there is a moral hazard that comes along with that.

Mr. Donilon stated that there needs to be a path to getting standards set which is a core point with insurance helping to drive. He thanked the panel for participating and concluded the session.

12:30 P.M. – 1:30 P.M. Lunch

Panel 3: Research and Development

Greg Baxter, Global Head of Digital, Citi
Jerry Cuomo, IBM Fellow, VP Blockchain Technologies
Irving Wladawsky-Berger, Visiting Lecturer of Engineering Systems, MIT; Strategic Advisor, HBO; Executive in Residence, New York University; Adjunct Professor, Imperial College, London
Alex Pentland, Professor, MIT

Afternoon Session Opening Remarks

Mr. Sam Raskoff opened the afternoon proceedings with brief remarks on NYU's cybersecurity activities. NYU Law School has entered partnership with the NYU Tandon School of Engineering. Everyone at NYU appreciates the need to train the next group of leaders. NYU is attempting to address the need for new talent. There are five students on scholarship sponsored by the National Science Foundation (NSF) who are able to take law and technology classes, graduate with law degrees and commit to working in cybersecurity for a number of years following graduation.

The Chair welcomed the research and development panelists to the meeting.

Irving Wladawsky-Berger, Visiting Lecturer of Engineering Systems, MIT; Strategic Advisor, HBO; Executive in Residence, New York University; Adjunct Professor, Imperial College, London

Mr. Wladawsky-Berger noted that he started getting involved in digital currency about 10 years ago. One of the first lessons learned was that money makes the world g around. Money is one of the most critical inventions. Money facilitates transactions and commerce. Today, money is mostly intangible. Digital funds dominate today's financial transactions. The digital financial ecosystem has become very complex and sophisticated.

The financial sector has created global payment infrastructures, personal identity management, regulatory regimes, etc. The digital ecosystem has served us well so far, but it is complicated, inefficient and inflexible. It may not be up to 21st century demands of scalability, security and privacy. There are billions of people around the world who pay for things with their smart phones as well as the many billions more using internet-of-things transactions of all kinds that need to be evaluated because of health and safety impacts.

Changing the digital ecosystem requires government, international and other stakeholders to embrace innovation. All stakeholders must be encouraged to embrace change in the ecosystem for it to evolve. The internet has changed everything. Once the internet was embraced during the 1990s, it became much simpler to send emails and other activities. Everyone was using the same standards back then, including open source implementations of key protocols. Institutions collaborated on developing a common internet architecture and internet-based applications like email and the world-wide web.

International organizations were created to oversee its evolution, including standards. Open collaborative innovation was encouraged. Innovations can take on a life of their own once they hit the marketplace. This is what happened to the original conception and implementation of Blockchain. Today, blockchain has transcended its original purpose. It has adapted to have the capability to accept trustless transactions. Parties do not need to know or trust each other for transactions to complete. Blockchain has brought the concept of the accounting ledger to the internet age. Institutions have automated the processes used to manage ledgers, but the underlying structure has not changed.

The bank of England stated in a recent article that the ledger system has not changed since the 16th century. Today, each institution still owns and manages synchronizing its records with other institutions. It is often a cumbersome process that can take days. The internet proved to be a major catalyst for change in global supply chain ecosystems. It is too soon to tell if Blockchain will become a major catalyst for change in supply chain applications. Much more work needs to be done with the Blockchain. The evolution will be a tough and lengthy undertaking, but very important and exciting.

Greg Baxter, Global Head of Digital, Citi

The global financial infrastructure is built on trust. A breach of that trust would have severe implications. In an increasingly digital and global world, the ways in which clients are served and protected is changing significantly, but the need for trust remains absolute. The digital revolution has transformed financial services. With it comes significant opportunities and tools to facilitate success and prosperity. The migration to digital money brings new, sophisticated and growing cyber risks. The migration to digital financial services is already well underway.

Investment in financial technology has grown exponentially. It reached $19 billion in 2015. Over 70

percent of investment has been spent on the "last mile" of the consumer experience. The United States leads in this type of investment, followed by China, the United Kingdom and Sweden. Most of the spending to date has been in the areas of payments and lending. The U.S. and Europe are still at an early stage of disruption. We project the rate of disruptions in North America in the banking sector will grow from 1 percent today, to a 10 percent rate by 2020. Innovation at lower levels of the underlying structure is now occurring.

We are at a disruptive shifting point. There is a shift in financial products from vertical products to horizontal services integrated in the new digital ecosystems. The new realities are much broader ecosystems with many more points of access and cyber threats. Protecting people and assets requires new ways of identifying and authenticating customers and devices, new approaches to managing and using payment credentials, and new and more sophisticated monitoring capabilities. Advances in bio-metric technologies and behavior analytics, and adaptive technologies allow us to combine both of these without being so intrusive, which allows us to improve authentication substantially.

Tokenization of payment credentials no longer requires storing or transmitting static payment details, but instead creating dynamic single-use payment tokens bound by time, location and value will dramatically reduce the volume of stolen credentials. It will also eliminate the need to store payment details. Static tokenization is already being deployed and marks an important first step to enhance security and privacy.

Proliferation of new payment nodes creates new points of vulnerability as well as millions of information points. Each node in the network must become intelligent and have awareness of upstream and downstream threat activity. Big data and analytics provide the potential to collect threat data and to respond in real time. Security includes every node on a network and every participant in the digital ecosystem. In a more open and inclusive ecosystem, collaboration and accountability will be critical in solving threats. There can be no free riders.

There is a more systemic threat that needs to be faced. An attack on the global payment system represents a far greater threat to global economies and society: Sophisticated actors do not want to steal assets but attack companies or destroy downline systems. Defending against these sophisticated actors requires significantly different objectives, incentives and capability. It requires extremely sophisticated defense capabilities, and many businesses will be ill-equipped to respond.

There are 3 ways where the government may be able to support the private sector: 1) Intelligence sharing – increasing speed and quality of two-way information flows, 2) R&D dramatically increase speed and scale for public and private sectors, requiring increased investments in R&D, and 3) Workforce Development – a shortage of trained personnel may be the most critical issue facing larger corporations. We need to increase and maintain the available work force which may require and need educational capacity and incentives.

The potential role of the government to provide a proactive defense to critical companies that come under cyber-attack needs to be evaluated. We need to look to real time intelligence, in response across public, private and government agencies, accompanied by legal framework required to implement such progress. Our solutions and partnerships need to stretch beyond the USA. In a world of exponential technological change, investment must grow at the same rate. New threats

will emerge that will have a significant impact on quantum and current cryptographic algorithms. A public/private partnership must emerge to develop new national and institutional capabilities.

Jerry Cuomo, IBM Fellow, VP Blockchain Technologies

Eighty years ago, IBM assisted the U.S. government with creating the Social Security system. At the time, it was considered the most complex system ever developed. As financial systems are increasingly digital and networked, the public and private sectors again need to combine forces to make the financial systems of the future more efficient, effective and secure than those of the past. Social security numbers became the key to personal identity for an entire generation of systems. Today, institutions must collaborate to create digital methods for establishing identity to secure a new generation of transactional systems.

Blockchain technology is becoming an essential tool as businesses and society navigate the shift. It holds the potential to transform commerce and the interactions between governments and individuals. It provides trust and security, but for it to reach its full potential, it must be further developed and rely o open source to make it deployable o a grand scale. There is a critical role for government to enhance national security and competitiveness. The government must invest in scientific research to accelerate progress.

NIST can help set standards for interoperability, privacy and security. Government agencies can become early adopters of blockchain applications. The government can certify the identities of participants in a blockchain-based system. Blockchain came to prominence as a core technology underlying bitcoin. Industries and government agencies are now exploring the use of blockchain where transaction participants are known.

This is known as “permissioned blockchain.” A distributed ledger shared on a peer-to-peer network contains an ever-expanding list of data records. Each participant has an exact copy of the ledger data. Additions to the chain are propagated in real time across the network with all parties consenting on the validity of the entries. Everyone in the chain has an up-to-date ledger with the most recent transactions. Once transactions appear in the ledger, they cannot be changed. Cryptology and digital signatures are used to verify identity authenticity and enforce access to the ledger.

It is fast and resolves transactions immediately, eliminates cost and is resistant to tampering, collusion, and cyber threats. IBM is the founding member of the Linux Foundation's Open Source Hyper Ledger project, helping to build foundational elements of a business-ready blockchain with privacy, confidentiality and auditability. IBM is pioneering the use of blockchain to re-engineer some of IBM's business processes.

There are four areas to enhance:

1. Proof of Identity – The Social Security Number (SSN) is not a secure or certifiable enough identity tool for a blockchain-based ecosystem. A new identity management system must be created. As an example, India is issuing 12-digit identity numbers to its entire population. An individual's number is linked to biometric and demographic information, and can be used to set u a bank account or access government services.
2. Data provenance – Ensures the safety of exposing personal and confidential data to financial

applications. New systems must track every change to financial data so that it is auditable and completely trustworthy. Data provenance must provide fingerprint and time stamp to show that information is up to date. It must be accurate, up to date and un-tampered with.

3. Secure transaction processing – While the parties in the transaction using blockchain are known to the system, the individuals only have access to the details of the transaction. The entities validate transactions to verify the contracts are being fulfilled without revealing confidential information to them. This involves onomorphic encryption. It makes it possible to verify information without having to de-encrypt it. This technique is still several years from being practical, but it is coming.
4. Sharing intelligence – The good guys are under pressure to change the game due to a rising tide of threats and cyber terrorism. Blockchain has that game-changing potential. It is more secure than other networks, it can be used to share threat information. Many financial services firms are reluctant to share threat information, but blockchain makes it possible to share securely. Threats can be shared in real-time so that accounting measures can be taken. IBM looks forward to working with government and industry to get this done.

Alex Pentland, Professor, MIT

Mr. Pentland had a conversation with Secretary Pritzker and the European Union Vice President of Digital Marketing about privacy and security. The Department of Commerce is in the process of coordinating negotiations on data transfer with the European Union. In the areas of finance and the internet of things, they agreed they needed to make some crucial decisions on data transfer. We need to specify what standards we should hit with these new technologies. Technology moves too fast to really keep up. Unless it is done at the beginning, there are few opportunities later to improve security.

Secretary Pritzker suggested Mr. Pentland's group work with NIST. Mr. Pentland's trust consortium represents approximately 85 percent of the authentication mechanisms that think about where we are going as far as technical standards and how they interact with legal standards.

Things to discuss today:

First, secure multi-party authentication – If data is ever de-encrypted, it will be attacked and stolen. Data must always be encrypted and never decrypted. We are heading toward a world of complete encryption. It is estimated that 70 percent of the threats come from insider attacks.

Second, there needs to be a way to do things even in the presence of bad actors. Blockchain helps to do this. People can attempt to fool blockchain or make mistakes and it will work correctly. This helps to solve the problem instead of putting more band aids o the problem.

With secure multi-party authentication and blockchain, two things happen: 1) it becomes more practical than before, and 2) it is the law that all the restrictions on data sharing can be overlooked. We could not do this before because of conflicts of risks, ownership, etc. It becomes transformative in terms of risk. In transforming the world this way, we are driven toward the world of completely encrypted data and distributed ledgers. It makes attacks extremely difficult. It also means that the NSA and FBI cannot get data because it is encrypted. There are ways to engineer so that these entities can get data without compromising security. We need to discuss how law enforcement can

view selective data in an encrypted world. We will not have true security until this question is resolved.

3:00 P.M. – 3:45 P.M. Commission Discussion

Commissioners of the Commission on Enhancing National Cybersecurity

Mr. Lee thanked the panelists and asked a technical question and a broader question: In the concept of permissioned blockchain, would there be law enforcement challenges in its use?

With permissioned blockchain, the rules can be set up at the network level, with member services and the governors of that network deciding what the permissions mean in terms of access and roles. An auditor role may have greater permissions than transaction-related roles. It is set-able at the network level.

What is the sense of inevitability and how democratized will this technology be? Is this something the U.S. government might adopt? Mr. Lee also noted the technology could exist outside of government control. Many people feel the government should not do this. It should be in the hands of banks and representatives of the citizenry, with all stakeholders represented. The example we set will be copied. All stakeholders must have a role in the certification aspect of the technology used. There is a large fraction of the technological community that would insist upon it.

Mr. Wladawsky-Berger The internet started with Defense Advanced Research Projects Agency (DARPA) support. Then the NSF developed NSF Net, which became a major manifestation of the internet. Government has a huge role to play, but not a controlling role. It has an enabling or participating role, and this has worked well in the past. There is concern that it takes a lot of research and development; it is extremely complicated. When it comes to long-term research, the government has the capability. The Commission will be making recommendations for technologies for the next to 1 years. When it comes to long-term research, there is no one else. If the government does not do it, will it still happen? Perhaps eventually.

The problem is not lack of technologies, but there are no system architectures that can accomplish what we are attempting to do. We need to have living labs to make sure systems do what they are supposed to. The internet was widely used as a test bed in the late '80s and, once proven, went into general use. The hope is that government and industry would come together to envision and test the systems of the future.

Mr. Baxter: There is not a great deal of traction in the consumer space or need to replicate what we have in place at the moment. Digitization of a fiat currency may or may not use blockchain. As an alternative to digital currency, it is not inevitable, as governments will continue to seek to control monetary flow. In the corporate space, there are multi-party settlements and multi-step money movements. Treasury, trade, supply chain financing and settlement of exchange traded goods are areas where digital currency has a greater potential to play a role.

The only way these systems work is when all players come together in a network. Investments at Citi are less associated with technology and more associated with players, and participants with two things – credibility to bring together a consortium within the industry, who can then bring the liquidity and that they understand the problem we are trying to solve. We see it as less of a technology question, but as selective in its adoption over approximately the next 3 years. Beyond

that, there are significant opportunities. Distributed ledgers need to be put in place and data must be migrated to those ledgers. Legacy systems would need to be cut off and reporting tested to be sure it has maintained its integrity. Many areas are being tested to evaluate potential impacts.

Mr. Pentland One thing that may be different going forward, is that we are entering a world where the internet of things and wearable computing is likely to become one of the dominant sources of interaction on financial networks. Finance and micropayments, in particular, represent more than dollar bills. We need to see how it will actually work. There are many visions about how things may work, but we do not really know what the reality will be.

Mr. Palmisano There always has been someone looking at the end-to-end architecture. Who is the one able to get global adoption to this standard of architecture? What is the appropriate mechanism to establish that entity?

Mr. Cuomo Proving out the uses of blockchain will be important to work on continuously. A proven way to do this is through open source. It is a mechanism to quickly try ideas so that academia, government and technology companies can evaluate new things. We are working with the Linux Foundation to discuss open government to try to create balanced views, and working with the Hyper Ledger project.

Mr. Pentland: Open source enables communities to discuss developments. Academia, companies, and non-government offices representing citizen views need to be at the table. Open source, government and citizens working together can make real changes. Discussions should be open to all these entities. Organizations such as NIST can act as the standard setter, with other entities funding the efforts.

The World Economic Forum has been active in Europe to bring parties together. The commercial members of the forum worked together to establish best practices for privacy, and had some positive results. Standards need to be interoperable and not stifle innovation.

One way to bring things together is through application. The government has some excellent applications. There are a series of smaller steps that can be made along the way. Picking single problem to solve together can create the impetus to go for larger challenges. There is not a single convener that will make things happen.

Ms. Murren: Mr. Pentland, you have mentioned that the body who convenes to work on these problems should contain citizen advocates, do you have recommendations you would make if you were on the commission to enhance cybersecurity and information security for individual citizens or households?

Mr. Pentland: There are a bunch of standard ones to look at, starting with the Mozilla Foundation, the Linux Foundation, and the Electronic Frontier Foundation. There have been a series of foundations that have been active in setting technical standards and convening people to have those discussions. They are not the only ones, but they are the ones that show up at DAVOS [conference], so you have the head of the Federal Trade Commission, the head of Bank of America, and the head of the Electronic Frontier Foundation, and they all sit in room to discuss what would be a win-win.

That is the convening portion, but it is not a "let's try it and test it out"; because in that discussion

there is speculation about what will happen if it was actually tried. So, there is a secondary step of building something, testing it out and seeing what people actually think about it. These are very complicated systems with a lot of unintended consequences, so you actually have to build it and see who comes.

Ms. Anton: Mr. Cuomo, you mentioned the identification card in India and one of the challenges I think of, when discussing this case in particular, is enhancing national cybersecurity and how we preserve privacy and human dignity. How do you manage the collection of biometrics when the information is going to be scattered for every basic use? How do you handle government usage and oversight of this personal information?

Mr. Cuomo: I think there is a piece that is missing from some existing systems where they tend to be more a database of things. The nice part of blockchain technology, while it has a shared ledger aspect of storing personal information, there is this notion of smart contracts, which is logic that goes along with the data. A citizen would control their own data through smart contracts. In a healthcare situation, a citizen entering a hospital for 24-hours would provide keys to their healthcare information for 24-hours and those keys would expire after that time.

Ms. Anton: That is a lot to ask when we are talking a lot about cyber hygiene and people not knowing how to protect their information, and frankly lot of people d not know how long they are going to be in the hospital, so there is lot to think through for real scenarios.

Mr. Cuomo: With any contract there are legal agreements, such as standard rental agreements, so there could be some standard agreement in place for these types of scenarios.

Mr. Pentland: There is a fundamental point that Annie is making. Our group helped chair the National Strategy for Trusted Identity in Cyberspace and there is a broad consensus on the point being made and there is a way to begin to approach it.

It starts with a secure private identity, in which you can generate, at your will, a persona. The persona is not your biometric, but rooted in your biometric, by your choice, when you want it, so that you can be the "public" Sandy, "work" Sandy, or "hospital" Sandy and no one knows that it is the same person. These personas can be thrown away at any time, without deleting the root.

We have the technology to do these things, but we have not gotten to that point. Like Annie, he is nervous about having a uniform cyber identity. I met a person who told me that his grandfather, when the Nazi's invaded the Netherlands, he worked at the National Statistical Offices, and burned the building down to save lives. This is something that I d not think will happen here, but our model will be used in other countries, where this could happen.

Ms. Anton: More recently in Rwanda, the genocide was fueled by using national identity cards as well, to which Mr. Pentland agrees, so it is a serious concern we must consider.

Mr. Wladawsky-Berger: One thing that I find interesting in looking at these issues is that safeguarding money, digital identities and personal data are much intertwined and you cannot do one without the other. That is why you see consensus that this must be done as a system. Because it is so complicated, it cannot be designed but must evolve over time and see where it takes us. We need research and experimentation in the evolution.

Ms. Anton: I agree, but I feel if we let it evolve over time, then we will not have built in the security that we need to ensure privacy.

Mr. Pentland: This is part of the need to actually do live experiments where you can see what happens. Let me reinforce Irving's point about data, in that money and data are not so different anymore and you need to have something that is very holistic to deal with personal data, just as you would with the strings of ones and zeros we call money.

Mr. Alexander: Sandy (Mr. Pentland), just to pick up on part of your discussion can you give us how you would, if you could enact all you talked about, how this would work between Apple and the FBI, calling it the next generation (or iteration), where we now have some ability to authorize the government on the security side and industry to protect, but to do it in a disciplined manner where both sides could win?

Mr. Pentland: I have an opinion as to what the end game would look like, but not sure how you get to the end game. I think that the end game, all data is encrypted all the time, the ledger that keeps track of that is also encrypted, but is synonymous so that there is a unique hash for each actor, rather like what NSA collected. Some examples of what this allows for is money laundering and discovery of terror cells, without knowing who the people are, with this sort of permissioned system.

With a court order, you can challenge it and reveal the true identity. So you need something that you can get to the root identity with court order. We need balance where there is metadata that is open and visible but the actual private data requires a much more visible formal mechanism, but by default everything is encrypted. The reason is to prevent bad guys from "blowing up" everything around us.

Mr. Alexander: I am an advocate for this. So, it seems to me that we should do what you are saying in this country and test it, then work with our closest allies in an attempt to make this international. The issue is you are going to run into some countries that will not adopt it because of their view on what they should have access to. I do not think we should take that on at first, but we should see if this works, and how it works, and can we make it work, then take on some of the other fights in a sequential and not parallel manner.

Mr. Chabinsky: One area that intrigued me is where the government can do a better job of being the "test bed" and having all of these applications of use. A couple of things come to mind if you have views on, one being the permission blockchain idea. I think that we might be in a situation where some of the areas with the highest security requirements have the lowest privacy demands. It might be a really interesting "test bed" for some of these notions, where more permissions are acceptable, and we can see what is the best security can do without being embroiled in the privacy debate. If you have ideas in that range, in what the government can facilitate in "test bed" for high security/low privacy, maximizing R&D and full bore ahead of attribution with full security, that would be helpful. Secondarily, what are some of the areas that the government can start on as a "test bed," even if it is a portion of the program?

Mr. Wladawsky-Berger: For example, internet of things (IoT) devices, of which there are already billions and there were/will be many sensors tracking traffic. It is hard for a sensor to say, "Irving, a

little privacy please." Security is very important but a lot of these devices do not have the privacy a human would have, but yet the underlying infrastructures would be very similar. There is quite a bit one could test with the infrastructure, so that the type of privacy a human being may want is not as big an issue and then let it evolve from there. So, you are making an excellent point.

Mr. Baxter: It is looking at where our flows are already occurring and where you are already sharing the data. Blockchain makes it more tamper-proof, more transparent, so that you can go and look at it, and it makes it to where it can be encrypted in flight or at a steady state. We run into a lot of complexity when we think about how to expand this technology into areas that d not exist today. In a commercial sense, we focus on where things are done today that have multi-party steps in them with multiple versions of data at rest in multiple locations. It does not transform the whole of financial services, but there are use cases where we all would look and say that is an area where we can get some savings and prove the technology out, without any detriment to the stakeholders.

Mr. Pentland: We have discussions with Treasury about doing these sort of things in financials between banks to instrument dark pools for risk reduction. That is the hardest privacy case as the banks cannot reveal anything about what they are doing so this notion of secure data sharing is critical. Similarly we have discussions around private and small business tax returns and being able to do careful permissions sharing. There are areas of immediate high value, not in terms of just cost reduction but risk reduction for the entire system.

Note Mr. Alexander and Mr. Pentland had to leave the meeting and leave the commissioner and panelist tables respectively.

Mr. Cuomo: To reiterate, we do not have to bite off the whole problem. There are aspects of maybe tax returns, the dispute side of it, where this technology can be used. We call it a shadow chain where it shadows the main business process, but not the main business process or business network, which is a way to introduce this without replacing the whole current system.

Ms. Todt: On behalf of a commissioner that could not attend in person, what are the most promising areas for investment related to better consumer authentication online? The questions stem from more of a retail perspective in looking at the digital economy, which is the focus of this commission. The Washington Post ran an article last week about how there are fewer individuals doing consumer retail online because of the concern they have with trust and privacy.

Mr. Sullivan: What are we doing to look at this consumer authentication online, beyond the financial sector?

Mr. Baxter: There are a couple of key areas from our perspective. One of those is around biometrics and the use of biometrics and behavioral analytics, which are starting to be used by a lot of people today. They are not federated in a way consistently or in a standard way so that when you do authenticate yourself, on say mobile device, it does not create pass that allows you access to applications or to pre-fill information.

There are various industry groups that are looking at how to create a federated identity that involves biometrics and other areas, where people are comfortable with the biometrics today. I think this is an important area as it is less evasive than areas where you receive a text message or out-of-band communication. Behavioral analytics is interesting as well as it looks at the way that

people behave and you can apply both biometrics and behavior to things as devices have a unique definition and they have particular behaviors.

I do not have a great answer for how you resolve the privacy side, but unless we start to get participation and collective accountability, it is going to be difficult to see these billions of devices being nothing more than vulnerability points. I do believe that with awareness and education, consumers would opt in to solutions that would allow them to be better protected as long as they knew how it was being used.

I also touched on tokenization briefly, which is not storing static payment credentials in all of the sites you go to and now all of the things you use to make payments. You should not have a permanent payment credential anywhere; it should be a relationship with yourself and the financial provider. So, moving towards static tokens where you have a replicate key of your payment details, so that way if it gets attacked, you replace that key and not all of them. Over time, one moves towards dynamic keys, where point and time, value, and location give you a token for payment for that particular transaction. This will protect the individual from putting their payment tokens out there or that particular token being valuable to anyone.

Mr. Wladawsky-Berger: That means nobody gets to see your credit card. When you put in your credit card information, it goes to the cloud, retrieves a token and sends it back to make the payment for your purchase. Currently, there are credit cards with the chip, but there are stores where that type of payment is unavailable and you still have to swipe your card, even though payment with a chip is much safer.

Mr. Baxter: We have seen very little true uptake in payment devices and the question is still, why is that? We see two main reasons for this, value proposition is not much better than plastic, and secondly, it is the safety and security. I think the idea of saying you will never have to store payment credentials in devices is an argument that anyone can understand and we are very excited about tokenization.

Mr. Banga: I live this everyday so will try and stay away from giving my perspective. Both of you talked about data versus devices and a lot of the conversations we are having tend to go back and forth. Since you use both, I find it helpful to break up the discussion into those two aspects. would like to get your perspective on both as I view data and the encryption of data as being a different imperative than devices and their encryption. My reasoning is, in some countries in society, there is due process for accessing encrypted data, but there is n due process in place for accessing encrypted devices and that is some of the friction we are currently seeing.

Mr. Cuomo: One of the things we have been thinking about is for identity, it is really hard in certain situations to draw a relationship between your biometric identities. Your digital identity is intimately tied to that device and essentially the two are bound together, so i one is compromised, so is the other. Looking at device identity is as important as looking at personal identity; being able to work with device manufacturers and new identity ideas, such as tokenization, to make sure we have as thorough a way of linking these two as possible.

Mr. Banga: I think the important thing is to make this completely pass-through to the consumer. It should be seamless to the point that the consumer does not have a lengthy thought process to

provide access to their keys for 24 hours, which can be difficult. Everything we are trying to accomplish must hide the complexity from the consumer in order for this to be successful. What are your thoughts on that with respects to data and devices?

Mr. Wladawsky-Berger: This gets back to the need for market experimentation because it is hard to tell ahead of time what people are willing to "tolerate" and "put up with" and what levels of additional work people are willing to put in. In the mid-'90s when e-commerce was beginning to rise over the internet, IBM worked with VISA and MasterCard to create secure, encrypted transactions, which were a lot safer than what everybody started using, but failed due to the fact that a certificate authority was needed ahead of time.

It failed because users thought the other option was good enough and if a transaction is fraudulently made, then the bank or credit card company pays, not the individual account user. Dual authentication currently exists, which has to be used in some instances, and works very well, but I wonder how many people actually use dual authentication for purchases. I do not think there is going to be just one thing, we just have to keep raising the bar and maybe eventually people will have to make a decision o how protected they want their identity to be. Maybe incentives need to be made to use these different methods, such as the financial institution not being held responsible, in order for these actions to take place.

Mr. Baxter: To reinforce that point, everything that is getting adopted is seamless and simple to use. For instance in an Uber transaction, no one gets into the car with bank and they love the fact that no bank is sitting next to them when they do that transaction. The concept of splitting data and devices makes sense, expect for the fact that devices and people are becoming synonymous as the identity of a person and the identity of a device are becoming linked. Along with that, the behavior of person and the behavior of device are becoming linked.

This makes behavior and biometrics so interesting in that they link things that are easy for people to have, to touch, to speak, to be looked at in the eye or face, to be able to detect where a transaction is being made and where your device is located, and are they in the same city when you are making a transaction. If we can create awareness, participation and rules around usage, I think we can make the experience relatively seamless using natural behavior and natural interactions with devices while improving security.

Mr. Cuomo: To add to that, one of the keys to making it simple is to delegate the complexity to someone you trust. Trust plays a really big role in this. You trust the manufacturer of the phone, you trust the network provider, and you may not know you have put all of your trust in them, but you have implicitly done so. I think this is where standards come into play because some of the things we are talking about are not simple; however, we are starting to understand some of the complexities and do something about them.

We recently put out a set of emerging standards as to what it would take to run blockchain in the cloud. It is really looking at whether to trust the cloud authority. Here are some of the things you should be asking them: At some point the rubber is going to hit the road and you are going to have to delegate that trust to someone else. This is one area that we can provide standards for. What are the elements that I should trust you by?

Everything we do, we do with a sense of certainty. I work with a bank because there is a sense of certainty there. I may not understand the details of what is going on, but I trust it, because my dad and generations before have, so I do. Trust is an important thing and to gain trust around digital identity as it pertains to devices is going to take time. Ultimately, it is going to take folks like you and I to provide that level of trust through a set of standards, which not every citizen is going to have to understand.

Dr. Lee: Listening to this discussion is really interesting in the sense of trying to be relevant to consumers and so seamlessness seems to be one obvious effort. Another is that maybe people can be inspired by what touches them directly, so I wanted to get back to what I detected as a somewhat cheapish discussion involving the replacement of social security numbers. The kind of model that was mentioned several times was the internet and the role of ICANN, the International Automotive Task Force (IATF), National Science Foundation Network (NSFNET), and DARPA. But another model going back to that era would be a moonshot. I guess I wanted to pin you down as panelists, truly on your thought as to whether the social security example was brought about as a throw-away example or if there is more commitment, and your thoughts behind that.

Mr. Wladawsky-Berger: More of a commitment to evolve from the social security number to a digital identity? I honestly do not think we have a choice. I think it is shocking that my Medicare card has my social security number listed there and that is one of the easiest ways to steal identity. We have all of these other technologies from EMV chips to digital certificates and certificate authorities. The technology is there, it is just question of evolving and it is no longer complicated. It is much nicer when am logging on to check something at MIT, it checks my certificate authority in my laptop or device and, i it is happy, it goes ahead and does what it needs to do. Obviously, if someone steals my device we have some other problems. The good thing about social security is that it has been around forever, but people can use it for so many nefarious ways that we need to evolve to something much stronger digitally and the technologies are there, it is just a matter of mapping out how to do that evolution. This does not take technology research, but market-facing research as to what people are willing to "evolve to" to protect their identities.

Mr. Baxter: As a non-American, I came here without a social security number, so I know the challenges of not having an identity. And as someone that leans into digital, would say yes, you should go in that direction. I just do not know if it is possible to do this practically. That being said, I touched on biometrics and behaviors and there are other ways we can achieve some of it. Another important thing to note is, this is happening anyway, separate from government identities through federated biometrics.

For example, when you authenticate yourself through your phone, you can now see transactions from certain banks, ourselves included. We currently use the Apple or Samsung biometric as a means to access data, as well as other institutions. We are slowly building up that sense of identity and trust. Would I prefer it to be more structured than a Facebook, Google, etc.? Absolutely, but I think we could lean into it by getting more government support around some of these identity agencies. I think biting off the whole SSN question is extremely ambitious.

Mr. Cuomo: While this is a moonshot, I think there are things we can do between now and then. If you g to website, you might see at the top number like, 192.XX.XX.XX, which is really no

different than a social security number. At some point you need a number, but it is what is under the number that counts. The cool part about going to a website, like Amazon.com is that when you g there, the bar turns green, which means that they are trusted, but what does that mean? It means that they have a name that is registered in ICANN and it relates to that number and Verisign has sent certificates out and validated that those certificates are correct.

So, if person's social security number was backed by mechanisms like that with cryptography and validation, you could wear your social security number on your hat and not be afraid, just like you have your name on your business card. I think there is nothing inherently wrong with the number itself, it is what we do with the number that is really important. I think we can start incrementally building those systems behind the number.

Ms. Anton: I have another question based on some of the information we have been asked to look at as commission: can you point to good examples of academia, government and industry collaborating and investing together in research that has led to significant technological advances? What advice do you have for us as to what we should be proposing so that we can continue to invest as nation in research?

Mr. Wladawsky-Berger: I would say the internet itself is exhibit A. The way it happened was incredibly close collaboration between government, academia and the private sector. They each played different roles along its early life. That has been a superb collaboration and the reason for the model in my head for what we have been discussing about cybersecurity. When say cybersecurity, I mean cybersecurity that enables life to go on and become even better despite there being bad people out there. I honestly really believe in that model.

Linux, by the way, was similar model in that universities played a huge role, super-computing centers used Linux. When I was in the President's IT Advisory committee in the mid to late '90s, there was a question, will open source make the software much less secure? We had hearings and people from the NSA said it is the opposite. The more people you have looking at the code the better. Yes, there are bad people that may try to do things there, but there are many more good people who will catch it, in comparison to proprietary software where it is a smaller number of people within a company who have to catch it. So, I think we have superb examples of collaboration and I think this should follow that kind of a model.

Ms. Anton: S as follow on to that, where are we falling short today with federal investment and research and basic science and technological research?

Mr. Cuomo: I think if we look around to see what other countries are doing, the CTO of the UK has written some pretty nice papers on the application of blockchain in the government. I hope that implies that they are looking to utilize and build some of those applications. One of the things that the UK government has done is given more encouragement to some of the businesses in the UK to be bolder in this space, just because as they are casting an opinion on this, it makes citizens more confident to go out and use it. So, one thing I see is, just put the opinion out there, and we would love to help you establish that opinion, because it will encourage the rest to come together and contribute.

Mr. Baxter: Interestingly, we have opened a cybersecurity center in Israel and we see so much of

interesting non-periphery but core innovation coming out of that space and I cannot explain exactly why. I know that all the way from the PM down they talk about this and that is a clear statement of commitment. I think it would be an interesting case study to see what is driving that and why do companies like Citi and others open a center there versus here.

In the UK, think the ID program where they have done a federated ID with the private sector is a way to get the sort of identity without having universal ID, in which they do not have either. When it comes to data flows, there are very few companies that can do what large corporations can do in the space. From an out perspective, it is probably an attack on the systems every 17 seconds. The more data we have, the more global insight we have of flows, the better, and what we are seeing is a consolidation of data back towards national boundaries.

The last one on my list I wanted to mention was quantum computing and I really do not know how close we are to this. I would think we are about 5 to 15 years, probably closer to the latter end of that spectrum. So much of the encryption we are built on is based on technologies that could be threatened by quantum computing and before we hit that point we need about 2 to 3 years of a solution in order to embed it, get to learn it, stabilize and scale it before the technology gets here. So that would be another area I would say government/academic research needs to lead us as well ahead of what industry is going to be capable of doing.

Mr. Donilon: That is an excellent finishing. The Israel case is one that we will look at as it is an interesting case, which is a case of national priority and talent development through their schools and their military service system. We do not have time for it here but we may come back to you on this sentence on quantum computing and the effects on current cryptography algorithms, which is another good, important R&D point. Thank you all very much.

As I was listening to you, there was a very strong point on the importance of research and how to make systems, particularly security systems, work for people in a natural way because if you do not, then they will not use it. Thinking about the discussion, we had at least three different baskets of things. We had the Internet of Things basket which was, let us get this right from the beginning with some set of standards. Then the medium term set of authentication advances like biometric, tokenization and behavioral analytics. Then, the third basket felt to me like the secure data sharing systems such as blockchain, and other systems that we were talking about here today, which are longer term systems which require more research and testing. It was a great discussion and we really appreciate all of the thoughtfulness you put into the presentations. Thank you very much.

3:45 P.M. – 4:00 P.M. Public Comment

[No name given]: My background is for 3 years I was IP and Tech Law and JP Morgan, BCC Committee Chief for Cybersecurity Compliance. Before that I was an advisor at the State Department, World Bank, and programming since I was 9. There are two main elements I found through the discussion that we have touched upon, but would hope could get incorporated in the dialogue in the future a bit more comprehensively. The first is the global perspective and the other is the about the involvement of SMEs or SMBs, whatever you want to call it, small to medium enterprises; to the extent that small- to medium-size enterprises have solutions which also present vulnerabilities when they are purchased by larger financial institutions.

There is a dynamic there that if you see both perspectives, it is kind of evident as there are not only legacy systems but legacy institutions, legacy dialogue, legacy interests, and there needs to be a little bit more discussion. I will provide a quick example: we were just talking about authentication and how things like Apple Pay authentication is pretty good. I am not sure if this was touched upon but Apple Pay is technically illegal because it does not d proper multi-factor authentication. Yes, you can have the phone tokenized when you sign up; yes, you can use a password, but the moment you start using your biometrics, the phone allows for up to six different fingerprints to be stored.

There have been cases where boyfriend and girlfriend have broken u and one person has taken the iPad, that they still have access to and wipe the bank account. Now this is something that small- to medium-sized businesses are not aware of and I think only three out of the top ten banks have incorporated into their Apple Pay terms and conditions, but because they have the capacity to understand it. So this speaks to the point you were talking about trust and having to have trust in institutions, that trust is not equal.

In this case for Apple Pay, the three sentences in the terms and conditions that allow Apple Pay to be legalized is, if someone hacks your bank account and you use biometrics, it is neither the bank's fault nor is it Apply Pay's fault. That puts the onus directly on the consumer and I think that is one of the best examples of how you cannot necessarily make it a seamless process for consumers because established interest will also try and make sure that trust goes in their favor without much transparency.

Ms. Alice Labrie: Former U.S. Department of State, Foreign Service. am here today as a concerned citizen, tax payer, resident of Target City, Bank America and MasterCard customer. I want to thank Mr. Goldman from NYU for making this event possible for the general public to attend. This is my question, which may be a bit off subject, but is important to me. What is being considered and by whom, retaliation against state nation hackers, especially regarding our infrastructure and reactors? I know the General has left and this question was going to be for him, so perhaps you cannot comment, but I hope that is up for consideration by the commission.

Mr. Randal Gamby: U.S. Bank. am the manager of the informational architecture. So, in the correlation between the first and the last panels today, I think there is a correlation that I want to make sure is captured with that. When we were talking about our love for the Cybersecurity Framework (CSF), some people say they are not that happy with it, the reason we like the CSF is that it gives us the opportunity to compare apples to apples when we look at an external organization and this gets in the area of trust, not necessarily risk.

So, as we look at the control structures we have, compare them to the control structures of someone else and that gives us the ability to decide whether we are going to have at least the same level of security and protection of information that we already have. I think that when we talk about consumer trust, it is kind of the same way in that, while there may be biometrics to ensure that this is a good credential, there is not that registration process which is what we were asking for in the CSF. Meaning, d we have that UL type of thing so that we can ensure that the trust that was setup is something that can be validated against a strong authority?

In the case of the CSF, it is still self-attest, so that means there is no organization that says, "Yes, you have met this level of control." It is a self-assessment within the financial industry. The same way

with the registration of a user credential, you assume that the person is who they say they are, and there are cases where it has been demonstrated where that is not the case. So, I think tying in the registration to the trust is extremely important and to have the bodies to do that would be good.

NIST has four levels of trust they can use, but that particular trust model is based on the U.S. Government, so it is based upon that fact that you have a government credential that can be validated to g from level 2 to level 3. What we would like to see is that expanded out to trust for individual organizations and the National Strategy for Trusted Identities in Cyberspace (NSTIC) organization is looking at organizations like financial institutions who know you because they have been doing banking with you for 20 years. Possibly the medical field since your doctor knows you intimately probably better than the government does. And finally the government as a possible entity for that.

So, when we look at setting up the trust levels going across that, maybe take in the evaluation of what is a true trusted organization that we can use as part of the registration process, as an issuance process, and finally as a validation process as we look across trust in organizations.

Mr. Jim Dingman: With Pacifica Radio and have been in journalism covering national security affairs for over 30 years. I have two questions. I go back to the first coverage I ha as a young man about the Church Committee and its aftermath. Thanks, NYU, for these very interesting presentations. I want to raise to the panel that one thing I think the public would be concerned about, and useful in your deliberations is to consider the Orwellian aspects of this, because many people would be concerned with who is going to guard the guardians with this information. And that is an interesting problem that is part of the vexing issue that goes around the complexity of trying to deal with this.

Secondly, I think that the public needs to know more concretely, we have this example of people hacking and trying to disturb the water supply of New York State and New York City. Now, many of us who have been watching what has been happening since 9/11, there are all these questions that are raised about let us gather all of the data and let us figure out afterwards what is going to happen. Not every American citizen is happy with that and I hope that in your deliberation you counter or think about people coming in who have greater expertise and raise these issues and talk about the thoughtfulness of trying to come up with good policy.

Mr. Steven Marino: Five grown children, 12 grandchildren, 47 years at Bell Systems, 30 years in the military, retired Lieutenant Colonel. As you make things more efficient, you increase the vulnerability, and increase the possibility of catastrophic hacking event. Thank you.

Closing Comments:

The next public meeting is to be held in June. Thanks everyone. Thanks to NYU for hosting us and thanks to the great panelist and thanks to the great questions from the commissioners.

Meeting Adjourned

The meeting adjourned at 3:39 P.M. Eastern Time.

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

Kiersten Todt
Executive Director
Commission on Enhancing National Cybersecurity
NIST

Tom Donilon
Chairman
Commission on Enhancing National Cybersecurity

These minutes will be formally considered by the Commission at its June 21, 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
Baxter	Greg	Global Head of Digital, Citi	Presenter
Beshar	Peter	Executive Vice President and General Counsel,	Presenter

Last Name	First Name	Affiliation	Role
		Marsh & McLennan Companies, Inc.	
Cuomo	Jerry	IBM Fellow, VP Blockchain Technologies	Presenter
Garvin	Lee	Director of Risk Management and Workers Compensation, JetBlue Airways	Presenter
Goldman	Zachary K.	Executive Director, Center on Law & Security; Adjunct Professor of Law, New York University School of Law; Co-Founder, NYU Center for Cybersecurity	Presenter
Gordon	Marc	Executive Vice President and CIO, American Express	Presenter
Milch	Randal	Former General Counsel, Verizon; Distinguished Professor, NYU School of Law	Presenter
Morrison	Trevor	Dean, Eric M. and Laurie B. Roth Professor of Law, New York University School of Law	Presenter
Mulligan	Catherine	Senior Vice President, Head of Professional Liability, Zurich, North America	Presenter
Pentland	Alex	Professor, MIT	Presenter
Rattray	Greg	Managing Director, Head of Global Cyber Partnerships, JP Morgan Chase & Co	Presenter
Venables	Phil	Managing Director and CISO, Goldman Sachs	Presenter
Wladawsky-Berger	Irving	Visiting Lecturer of Engineering Systems, MIT; Strategic Advisor, HBO; Executive in Residence, New York University; Adjunct Professor, Imperial College, London	Presenter
Dingman	Jim	Not indicated	Presenter/Public

Last Name	First Name	Affiliation	Role
			Participation
Gamby	Randal	U.S. Bank	Presenter/Public Participation
Labrie	Alice	Not indicated	Presenter/Public Participation
Marino	Steven	Not indicated	Presenter/Public Participation
No Name Given	Not indicated	Not indicated	Presenter/Public Participation
Chalpin	JP	Exeter Government Services	Meeting Staff
Drake	Robin	Exeter Government Services	Meeting Staff
Salisbury	Warren	Exeter Government Services	Meeting Staff
Aguos	Charles	not indicated	Attendee
Alexander	Deborah	IronNet Cybersecurity	Attendee
Allsberg	Sam V.	FBI	Attendee
Anderson	Christopher	Cybercat Risk Management, LLC	Attendee
B…	Jim	Pacifica	Attendee
Bauchner	Robert	NYU Law School	Attendee
Boyens	Jon	NIST	Attendee
Brunet	Jennifer	IronNet Cybersecurity	Attendee
Cammaroto	Gerilyn	American Express	Attendee
Carnahan	Lisa	NIST	Attendee
Castelli	Christopher	PWC	Attendee
Chaudri	Vishal	Credit Suisse	Attendee
Chen	G.	self	Attendee
Clinton	Lenny	Internet Security Alliance	Attendee
Dinnigan	William	DTCC	Attendee
Dodson	Donna	NIST	Attendee
Dubinski	Vitaliy	Citi	Attendee
Dwyer	Meghan	Pryor Cashman	Attendee

Last Name	First Name	Affiliation	Role
E…	Michael	National Association Federal Credit Unions	Attendee
Egel	Naomi	Council on Foreign Relations	Attendee
Egger	Matthew	U.S. Chamber	Attendee
Eze	Uggi A.	Not legible	Attendee
Fenser	Brooke	King Street	Attendee
Frisch	Henry	self	Attendee
G..	Marc	American Express	Attendee
G…	E.	Fashion One, LLC	Attendee
Gallagher	Shawn	AIG	Attendee
Galvin	Tiffany	Goldman Sachs	Attendee
Gartenmann	Curtis	Citi	Attendee
Gerantt	Jaruthan	Not legible	Attendee
Gillespie	Noah	Schultz Roth Rabel, LLP	Attendee
Gray	Danielle	O'Melveny	Attendee
Hamilton	Christopher	FBI	Attendee
Hehner	Chris	SI C	Attendee
Hilgen	David	Zurich North America	Attendee
Hirsch	Frederick	Hirsch IP Solutions	Attendee
House	Eric V.	Van House Associates	Attendee
Jones	Robert V.	Presafe Technologies	Attendee
Kappoor	Shweta	NYU	Attendee
Kelly	Erin	Federal Reserve Bank of New York	Attendee
Kerdon	Isaac	NYU Law	Attendee
Kerrow	Linda	NYU alum	Attendee
Knelte	Ros	Not legible	Attendee
Krebs	Christopher	Microsoft	Attendee
Krimpotich	Laurie	New York Life Insurance	Attendee

Last Name	First Name	Affiliation	Role
la Brie	Alice F.	Former U.S. Dept. State for Serv	Attendee
Leger	Micki	Not legible	Attendee
Leinhardt	Bradley	Leinhardt Law	Attendee
Liebermann	Erez	Prudential	Attendee
Liu	Diyang	Mayer Brown, LLP	Attendee
Luis	Chuck	IEFE/Professor E.T.	Attendee
Magri	Josh	FSR/BITS	Attendee
Matsh	Michael	New School	Attendee
Maymi	Fernando	NYU Tandon	Attendee
McCabe	Matthwer	Not legible	Attendee
McClelland	Wes	AIA	Attendee
Morroc	Mattew	not indicated	Attendee
Noone	Brian	Nova Venture Partners	Attendee
Not legible	Not indicated	Not legible	Attendee
Not legible		Avery Labs	Attendee
Not legible	Stephen	New School	Attendee
Not legible	William	NYU Tandon	Attendee
O'Riley	Mark	IBM	Attendee
Padilla	Aaron	API	Attendee
Pawlick	Jeffery	NYU Tandon	Attendee
Pomerantz	Stewart	Jefferies	Attendee
Potter	Bruce	NIST	Attendee
Quincy	Julia	Perrot Library	Attendee
R…	A.	Not legible	Attendee
Romanelli	Frederica	Not legible	Attendee
Ronen	Kristie	USI Insurance	Attendee
Ronen	Marc	USI Insurance	Attendee

Last Name	First Name	Affiliation	Role
Rosi	Sheea	UN	Attendee
Rothman	Kevin	American Express	Attendee
Rymar	Zachary	Senator Menendez	Attendee
Schap	Minuele	Chresa Shahinian & Giastonian	Attendee
Scholl	Matt	NIST	Attendee
Shabtay	Sammy Henig	self	Attendee
Singh	Amendeep	NYU	Attendee
Sneh	Ithi	Cu-ISHA	Attendee
Song	Liping	Bank of China	Attendee
Southwell	Alexander	Gibson Dunn	Attendee
Stendahl	Benjamin	Google	Attendee
Stine	Kevin	NIST	Attendee
Tan….	Ha…	Suedentsche Rerbuy	Attendee
Tannenbaum	Andrew	IBM	Attendee
Terris	Chris	NYU Law	Attendee
Tyre	Sarah	Burson Marsteller	Attendee
Underwood	Mark	Krypton Brothers	Attendee
Vassansi	Anil	Sullivan & Cromwell, LLC	Attendee
Walker	Carolyn	not indicated	Attendee
Walsh	Robert	FBI	Attendee
Wang,	Shanxing	Not legible	Attendee
Weber	Rick	Inside Cybersecurity	Attendee
Welder	Kelly	Dept of Commerce	Attendee
Wood	Keppel	IronNet	Attendee
Xiane	Not indicated	City Tech	Attendee
Yuen	Rambo	not indicated	Attendee
Zhai	Jing	NYU SPS	Attendee

Last Name	First Name	Affiliation	Role
Heugner	Michael	Reactions	Media
Jonas	Erik	Not legible	Media
Otto	Greg	Scoop News Group	Media
Paglieri	Jose	CNN	Media

Annex B - Public Participation Statements

No public participant statements were received.