Commission on Enhancing National Cybersecurity

Established by Executive Order 13718,
Commission on Enhancing National Cybersecurity

American University Washington College of Law Yuma Building
Claudio Grossman Hall
4300 Nebraska Avenue, NW, Washington, DC 20016

The Commission on Enhancing National Cybersecurity (Commission) was convened for its sixth public meeting at 9:16 a.m., Eastern Time on September 19, 2016 at the Washington College of Law, American University in Washington, D.C. The meeting in its entirety was open to the public. For a list of attendees, please refer to Annex A.

Welcome and Overview

Camille Nelson, Dean, American University Washington College of Law

Welcome to the Washington College of Law and in particular welcome to our new legal campus. We are honored to be able to host this Commission hearing. We hope that this will be the first of many. I am privileged and delighted to co-host this program with the Kogod School of Business Cyber Security Governance Center and to continue connections with other units of American University.

John Delaney, Dean, Kogod School of Business (KSB) at American University

It is a privilege to host the final field hearing of the Presidential Commission on Enhancing National Cybersecurity. We are honored to welcome Secretary Pritzker and the members of the Commission to our campus. It's my pleasure to welcome the Deputy Director of the Cybersecurity Governance Center, Professor Rebecca Lewis to the podium to offer a brief welcome and to talk a little bit about the center itself.

Rebekah Lewis, Deputy Director, Kogod Cybersecurity Governance Center (KCGC)

The cyber security Government Center was founded in 2015 with the core mission of promoting cyber security governance by providing guidance specifically to boards of directors, senior executives, and other leaders so that they can make informed decisions about cybersecurity and confidently move Commerce forward in the digital business environment, we view this mission as being very closely aligned with the mission of the Commission and the future of our Nation's economy.

Ms. Todt called the meeting officially to order at 9:16 a.m., Eastern Time.

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

I call this meeting to order. Good morning, and welcome everybody to this meeting of the Commission on Enhancing National Cybersecurity. We've had five tremendous meetings and we're very privileged to be here at American University. Thank you, American University College

of Law and Dean Delaney D. Nelson, and to Miss Lewis for hosting us.

It is my honor to introduce Penny Pritzker, the Secretary of the Department of Commerce, the 38th secretary. Secretary Pritzker has made cybersecurity the focus of her efforts and those of her agencies. Since she was sworn in over 3 years ago, she is uniquely positioned as a leader of an agency with a broad range of responsibilities; from the surface of the Sun to the bottom of the ocean, horizontal across agencies such as U.S. Patent and Trade, Census, international trade and NIST, to truly understand the diverse cyber security needs of this country and a growing digital economy.

In this position, and as a former CEO, Secretary Pritzker also has an important awareness and recognition of where government policies and processes can improve to facilitate efficient functioning, particularly as they pertain to cybersecurity. She has been a relentless and effective advocate for raising awareness of cybersecurity among senior executives in the c-suite and in the boardroom.

The Commission truly appreciates the work of NIST as the Secretariat for its work, and the constant support of Commerce in its operations over the past few months. Thank you Secretary Pritzker, for your leadership in this process, and for the impactful work you and your agency have done and continue to do in cyber security.

Meeting Opening

Penny Pritzker, Secretary of Commerce, US Department of Commerce

Secretary Pritzker conveyed the President's gratitude to everyone on the Commission, and staff behind the scenes. The work done by the Commission is the centerpiece of President Obama's Cybersecurity National Action Plan. Sitting on the Commission is a profound service to the country. There is a lot of work ahead. There are two issues:

Cybersecurity challenges faced by a cabinet secretary, and the partnership between government and industry that is needed to protect the digital economy. Every device is connected, networked, and online. Cybersecurity is integral to core missions of government and industry, the economy, and the country.

The Secretary of Commerce is accountable to the President and the American people. The Secretary is accountable for Commerce's twelve bureaus. Network security and resilience is necessary to protect those networks and data. Commerce cannot promote its interests domestically or abroad, protect intellectual property, deliver weather data to communities, or meet its other responsibilities without strong cybersecurity.

The Secretary is wary of any vast centralization effort that dilutes the authority of a secretary as a manager to hold his/her team accountable. The Commission faces many questions: Should there be a unified government network similar to .mil, or unified email for government workers? Secretarial needs vary greatly across agencies. The Commission faces the question of centralizing certain functions, while maintaining the balance needed to complete missions.

Commerce has experienced a shortage of skilled personnel, but lacks the authority to do anything about it. We face uncompetitive salaries, and slow hiring processes. There is inter-agency

poaching and the private sector hires people away. We are only as strong as the team we assemble. I ask the Commission to consider a centralized system to recruit, train, and place cybersecurity personnel. There may need to be specialized pay scales to compete with the private sector in cybersecurity. We need to end the "musical chairs" in cybersecurity positions in the government. It may be time for contracts with pre-set time commitments. We need bold ideas in recruitment to help get the people we need. An ever evolving threat landscape demands resources. Cybersecurity must be an indispensable condition for every priority.

Federal appropriations hinder procurement of the things that are truly needed. Securing funds from Congress on specific programs is easier than making long term changes. Congress can fund long term programs. Cybersecurity is severely underfunded. Agreement on this basic principle is a major culture change in Washington. DHS continuous assessments and diagnostics is a valuable tool to enable agencies to secure networks and data. Access to emergency-ready personnel would be welcome. Shared services for IT would help access to leading edge solutions immediately, without waiting months for legal to evaluate licenses. A sandbox environment to evaluate the latest software would help speed the process. We must have the political will to protect key assets.

Adversaries grow more sophisticated by the day. The government must get its house in order. There is the broader challenge of protecting critical infrastructure. Most critical infrastructure is owned and operated by the private sector. There must be teamwork on multiple levels. It requires universal standards and best practices that are understood by government and the private sector. The NIST framework works for all. There are no meaningful ways for cooperation between government and the private sector. Threats will only grow more widespread.

There is a risk of erosion in public trust of innovation that will lead to the future. We have the threat of a, "death by a thousand paper cuts". We need innovation and a true joint defense posture. Defense is failing to keep pace with innovation. The Commission's recommendations will shape how the government and people will defend themselves in the 21st century. The Commission's report to the President will shape the Nation's priorities in cybersecurity on day one. Be bold in your recommendations, be creative in your solutions, and most of all, be unrestrained by convention.

International Discussion

Chris Painter, Coordinator for Cyber Issues, U.S. Department of State

We are in a place where there has been significant progress, but there is more to do. Through its diplomacy, the State Department works to strengthen our collective cybersecurity. Our efforts to coordinate, consult and negotiate with a range of countries and international organizations complement the practical day-to-day work of our interagency colleagues who maintain network security. Our cyber diplomats work to reduce risk and enhance stability in cyberspace.

Their efforts include, but are not limited, to a number of core areas:

- Working with our interagency partners to promote internationally a framework for building cyber stability,
- Building the capacity of foreign governments to provide cybersecurity and respond to

cyber threats,

- Using diplomatic channels to support cyber incident response, and,
- Partnering with other countries to combat transnational organized crime. I will briefly touch on each of those and a few recommendations as well.

The Department of State, working with its interagency partners, is guided by the President's 2011 International Strategy for Cyberspace, which sets out a strategic framework for international cyber-stability. This framework has three elements:

- The affirmation that existing international law applies to cyberspace, just like it does in the physical world. A whole new legal construct is not needed for cyberspace.
- The development of international consensus on, and promotion of, additional voluntary norms and responsible state behavior that apply during peace time.
- The development and implementation of practical confidence building measures, or CBMs, among countries.

The U.S. can more effectively respond to foreign cyber threats when our international partners themselves have strong response and cyber-crime fighting capabilities. Therefore, the Department of State is working with others to build the capacity of foreign governments, particularly in developing countries to secure their own networks from cyber-criminals.

In responding, the United States uses a whole-of-government approach to respond to and deter malicious activity in cyberspace, which brings to bear the full range of instruments of power and foreign policy tools: diplomatic, law enforcement, economic, military, and intelligence through diplomatic channels as appropriate and backed by applicable law. The State Department plays a key role in our inter-agency deliberations on major cyber events and how respond and engage through diplomatic channels when needed, such as raising concerns about cyber enabled theft of intellectual property or responding to the denial of service attack that plagued our financial institutions where we raised the level by doing diplomatic demarches to over twenty countries around the world.

The United States is a global leader in combatting cyber-crime. The State Department, with its partners, actively promotes membership in the Budapest Cybercrime Convention, which we think is a core instrument that will allow countries to have the substantive and procedural tools, along with the G-7 24/7 network that now has over 70 members around the world. It allows better information sharing and preservation in incidents. As we look ahead, at these rapidly expanding global cyber threats, we know they are going to continue to be a challenge. We are not in the place where we've seen that interest has waxed and waned in this subject. It is clear now this is a clear issue in our national security, economic policy, human rights, and ultimately foreign policy. This Commission's work is really coming at an important time to keep that momentum going. I offer six recommendations for the Commission's consideration:

First, efforts to further strengthen the strategic framework of international cyber stability should continue through promotion of voluntary norms and responsible state behavior in cyberspace that apply during peacetime, expansion of global affirmation that international law and state

behavior apply in cyberspace; and the development and implementation of additional confidence-building measures that reduce risk and the chance of escalation. There has been a lot of good work done, but we must continue and build on it by getting more countries to sign on.

Second, the United States pursues a vision of openness and collaboration and multi-stakeholder governance for cyber space which is in stark contrast to alternative state concepts of cyberspace governance pursued by some countries such as China and Russia, who try to control content and attempt to draw sovereign boundaries around cyber space. Therefore, the U.S. should continue to advocate bi-lateral and multi-lateral forums including the United Nations for stakeholder governance so that the internet includes all parties.

Third, The United States should continue to build the capacity of foreign governments, particularly in developing countries, to secure their own networks and to promote donor cooperation and joint capacity building initiatives. This will enhance our own ability to deal with cyber threats if they had that capability and those policies in place as well.

Fourth, given the transnational nature of the internet and the communications infrastructure, international cooperation is obviously essential to effectively address cyber incidents. Therefore, the U.S. should continue efforts to enhance its understandings of other countries cyber-incident response capabilities and coordination. I had to formalize communication channels that include network defense, cert-to-cert, law enforcement, diplomatic, military, and others. We were able to respond to incidents which are always global more quickly.

Fifth, to further combat transnational crime, we should continue to aggressively promote membership in, or at least adopting the tenets of, the Budapest Convention and continue to enlarge operational frameworks like the G-7 24/7 network.

Finally, here at home, the State Department should continue to mainstream this issue into our foreign diplomatic engagements and build necessary internal capacity to formulate, coordinate, and implement cyber policies throughout our government. I would say when Mr. Donilon and I were at the White House, this was a new field.

Since my office was created 5 years ago, we now have 25 counterparts in foreign ministries around the world. There is a lot of understanding and all-government dialogues about the issues, and that's important. I have submitted a written statement, and some documents including a report related to Congress to talk about our implementation of the international strategy, where we're going on norms, and where we see the threats that I commend to you as well.

International Discussion

Commissioners of the Commission on Enhancing National Cybersecurity

Mr. Chabinsky: I tend to think we focus our efforts, policy efforts, financial resources, manpower on defense and putting effort at the lowest level. Every entity is defending itself because we haven't brought this up to a level to try to get the cybersecurity problem as far away as possible from end users. One of the ways to do that is going after threat actors, whether it's nation-state norms or elements of national power, or trans-national criminal efforts. What I've seen is two-fold. One, the public's view is one of haplessness. There is a view we can't beat the bad guys, so we have to be impenetrable. There is a sense it doesn't even seem meaningful that we might be able to reverse the

strategy and make it threat-centric.

It also seems it might be a self-fulfilling problem. When we see the billions of dollars, within the Federal Government alone, spent on information security efforts, compared to what we are spending in the Justice Department and State Department in our international efforts to actually hold people accountable and create systems and policies that go after the threat actor to stop this problem from hitting us in the first place. It's so disparate. What are your views on the disparity of threat mitigation based on your perspective and years of service?

Mr. Painter: Targets need to be hardened to make sure it deters all threat actors. From a real world perspective, it will not deter all of them. There's more to it than simply locking the doors. There are different kinds of threats. There are nation-state threats, national criminal group threats, and lone actors. It requires a mind view of working with law enforcement and diplomatic colleagues to disrupt those threats. Justice has been working on disrupting criminal groups. It has been doing undercover and other kinds of operations. It takes both kinds of action and there must be consequences. Consequences must include law enforcement, sanctions, diplomacy, pressure, and possibly military tools. State tries to encourage that collective response. It is an important and possibly under represented part of the puzzle.

Mr. Chabinsky: What would it take to change the tide to get success against the threat? If we changed our focus to deterring threat actors, how should we go about it?

Mr. Painter: We can't do it alone. It has shifted to some extent. It takes threat denial and resilience, and going after threat actors. We have to be able to change some of the mindset that we don't have the power to change the behavior. When there are consequences to actions, it makes a difference. There are ways to deter nation-states, using the tools we have. There have been successes. It is a focus that has to happen. I believe people do understand the threat exists.

Ms. Murren: As you have been observing, and you've been part of the changes that have been made in the last couple of decades in enhancing cybersecurity. You mentioned there's been a lot of progress, and there has been a lot of action. As we move forward, and recognize the need to prioritize our time and treasure to address all the different aspects of cybersecurity, what are the things that you believe we've done where we've allocated people or money, that it may be better served to end, and where we could put them instead?

Mr. Painter: I'm not certain where money may be taken from. It may be until recently that not enough resources have been devoted to this issue. The number one thing is leadership and making sure from the very top that there is a very clear priority on this issue. It includes the White House, and the cabinet level of all agencies. It should be a priority with their own systems and engaging with the private sector.

It is certainly true my area did not exist five years ago. We have made progress. It is a small group of people compared to some of the people doing defensive activities. There needs to be an understanding that some efforts will pay dividends beyond the short term. Greater stability in the long term will help everyone. It needs to be clear that no matter where our resources are, we must have priorities.

Even if we increase spending as the President asks in the CNAP, we will still be stretched. We will

have to figure out where our priorities are. One of the most important things is having a comprehensive approach, as opposed to a silo-ed approach. The international strategy tries to do that. It talks about human rights, it talks about economic issues, military issues, and cybersecurity issues. If we continue to look at these things in stovepipes as we have in the past, we will continue to make ourselves weaker. It doesn't take a large expenditure of money to bring things together. It includes bringing all these communities together in a shared interest. The demand now is huge. We must keep our eyes on what we want to achieve.

Mr. Gallagher: I have two questions, both in the character of a status report. With regard to state governance, what's the current state of affairs with regard to state based vs multi-stakeholder approaches? The second question touches on this law enforcement cooperation, to what extent is the discussion around encryption affecting that cooperation?

Mr. Painter: When we talk about internet governance, the reason these are all inter-related is when some countries talk about information security, they don't mean cybersecurity. They mean securing and preventing spread of information and securing virtual boundaries around their territories. It has implications for human rights, security and governance. When they promote the idea of states running the internet, that's why they're doing it. It's not for any other reason. We have made great strides. We have pushed back on countries advocating a more state system.

It's not a battle that's over. It's going to continue. We recently signed an agreement with India covering international security, cybersecurity and governance issues. India changed its point of view on this. They went to a multi stake holder system. It is significant because of their leadership in the G-77. The battle is by no means done, and we must continue it. Now, internet governance means everything to do with the internet, it used to mean the technical running of the internet. Now, it includes everything. So, we have to be attuned to that as well.

I don't have a solution on encryption today. It is a difficult issue for everyone, not just for the U.S. Governments around the world are grappling with it. We need strong encryption for privacy and security, and protection of citizens. We need to look at the problem and break it down. Does it affect business? It is one of the issues we are grappling with. It is a policy issue also.

Mr. Sullivan: I have two questions. Shortly after the Sony attacks, I was talking to a national security official, who said, "The thing you in the private sector don't get in these international incidents is that, to eastern governments, companies are viewed as extensions of state power. Western companies do not appreciate their role in the middle of all that." I'd appreciate your view from the point of view of the State Department. What's your view on this issue?

Mr. Painter: It depends. For planned economies, where countries have controlled, owned, or joint ventured in all their companies, there is a different view of public-private partnership, here vs. elsewhere. They have had to change and have some growth in their private sectors in order to be competitive. One of the interesting things about the Sony attack: why is the U.S. raising this incident to such a high level? It was an attack on our sovereignty, involving threats of violence, and an actual attempt to change free speech in this country.

Other countries see a self-interest in U.S. proposed measures. State control persists, and a lack of understanding of companies as independent actors. While speaking with certain countries about

the multi-stakeholder system, they interpreted governments and private entities to really be the United States. It was clarified that those private entities were actually within their country, and should have a voice in the system. It subsequently became the case. It makes the point we really do believe in the system. It's not a unified voice, government and industry do have different voices. Will that change the countries that have more planned economies? Not right away.

Mr. Sullivan: You are in a situation where private industry in western countries are not considered critical infrastructure. They don't have government agencies building their defenses, but yet are left as potential collateral damage or direct targets by states in other parts of the world that consider it fair game. What can the U.S. Government do?

Mr. Painter: There are two parts to that. The first question is, targeted for what? If it is for a disruptive attack, it is a real concern. The U.S.'s interest doesn't just extend to protecting critical infrastructure. It maybe prioritized because it can cause major death destruction, and damage.

Secretary Pritzker has been working with non-critical infrastructure. There must be consequences for these actors as well. Sony is a good example where we quickly and decisively acted in terms of attribution and what was done. There is also espionage, the theft of intellectual property to benefit the private sector of another country. It is not limited to critical infrastructure. It targets businesses in the United States and around the world. It comes up in every bi-lateral discussion with our partners.

We have made progress in getting China to recognize there is a distinction between intelligence gathering and stealing intellectual property. We have a commitment from them they would not continue. The jury is still out and we have not taken any tools off the table. Most countries agree this should be the norm. Likeminded countries can work together over time to collectively enforce that norm. We need to make sure we're not just looking at critical infrastructure, but looking at targets generally, and what the exposure is. We need to work with those companies. I meet with the private sector often, because there are some things I don't know in the government. I'm not always aware of the challenges, and what the opportunities might be. We need to continue to do that.

Mr. Sullivan: I also wanted to ask about mutual legal assistance treaty (MLAT) reform and efficiency of data sharing for law enforcement. Has it made progress?

Mr. Painter: We have been dealing with a lot of countries, that when all the data is stored here, they can't get data on their citizens. It has led to secondary effects like data localization, or viewing it as an impediment in the relationship. We have made progress. We have increased funding to DoJ to streamline the process. However, it is not the fastest process. There is now a 24-7 network.

We have also started talking with the UK Government to see if there is some sort of agreement we can reach that would stream line the process for certain kinds of data. It will require legislation, which has been sent to the Hill. If it goes through, we'd be open to talking to other governments. However, those governments must have protections in place. Overall we are better off, but there is a long way to go. We continue to look for creative solutions.

Mr. Banga: My first question connects to what you and Mr. Sullivan were just talking about. Most companies are facing a multitude of regulatory frameworks and different countries revolving around cybersecurity and data automation and localization. It's not just a question of what it does

for company expenses and material cost of operating. It's also going to destroy some of the advantages of scale in cybersecurity and capabilities in the internet of things if we end up doing everything country by country.

Mr. Painter: These are real challenges. As countries deal with these issues, if there is a fragmented regulatory framework around the world, it creates issues for companies. We have been promoting the NIST framework. It is voluntary and has been used around the world. It has had a lot of uptake, particularly by countries in Europe. Europe has just enacted the Network Information Security Directive. It is a good base for defining policies for countries. The trick will be in how it's implemented. It can be implemented in a regulatory fashion, or it's implemented in a way that allows interoperability which companies need that really promotes cybersecurity. Fragmentation does not promote cyber security. The private sector and government push back on data localization. Data localization requirements can cause problems. We need voices in the private sector too.

Mr. Banga: You are correct. There are a number of private companies willing to push in the direction of the NIST framework. There are two ways to do this, one is to allow for trickle down. Or a group of like-minded countries could work together and find their own way through how to implement it. Historically, things happen when countries work together and create an example for others to follow. In cyber we are still at a stage where it's laissez-faire. We are doing our own work, and hoping other countries will follow our example. I'm wondering if the Commission can put forward a more constructive and forceful point of view. We should question that logic.

Second, in my view in the current system, there is no way to declare a state actor a pariah. We do it one-on-one. Others have done work, and in the case of China, the recent visit by the President. There is no benchmark for acceptable behavior in the cyber world. It exists in the physical world. There are bodies that judge behavior and can make determinations. What's the solution in the cyber world? Is it all laissez-faire or trickle down? Should there be more a forceful, or constructive and driven way to think about it?

Mr. Painter: On the first question, I look forward to any recommendations you have. I think we have to be careful if we try to have "one ring that rules them all", that tries to bring things together. We won't end up with the inter-operability we need. That's why the NIST framework is so powerful. It is something we've advocated around the world. My NIST colleagues travel with me to these countries to do presentations and discussions, to try to make it happen. They need to understand the benefit of inter-operability. As soon as we try to have some formal global system, then a lot of other things creep in.

In sanctioning bad actors, we are in the process of determining what bad conduct is in cyberspace. It involves the voluntary norms we've talked about, such as not attacking critical infrastructure of another country during peace time, the expectation of cooperation if there is malicious code originating within the borders of a certain country. These are important voluntary norms, but many countries around the world have not grappled with these issues or signed up. We have received some affirmation from the G-20 and other venues.

To combat bad activities, we build a larger and larger group of countries who support the norms. Then, if there is a bad actor, the larger group can act collectively to sanction that bad actor. There

are many means by which this can be accomplished. It has worked in other arenas, it can work here too.

However, we don't have the luxury to wait the forty years it took to develop nuclear policy. It is true it will take some time. It is notable that within a few years of first proposing these norms, we are getting them accepted by many countries around the world. It is very quick by any diplomatic measure. We need to redouble those efforts.

Mr. Banga: So you are saying it makes sense to have a group of like-minded countries having constructive discussions, meaning they get together to discuss a common problem. We have these great technologies that can revolutionize access to information and democratize it beyond all limits. Look at what can happen if we don't take control. We should get together and have a conversation about what are the benchmarks of good behavior, and what's outside the norm. If that's what you're saying, that's a good move.

Mr. Painter: It is what we are trying to do. We just had a Nordic –Baltic- U.S. meeting, and we talked about these issues. They are like minded countries. We talked to our 5-I allies, and they are like minded countries. Our big push now is to get more countries to deal with these issues and adopt these norms. Then we can move to the next stage. I would not call this a formal or like-minded club because we want to have as many participants as we can. We need to continue to expand, and that is really where our efforts lie.

Ms. Anton: Following on what Mr. Sullivan was discussing, there is a lot of posturing in the EU right now with respect to US privacy practices, with respect to safe harbor, and privacy shield. The EU is threatening to halt U.S. company practices within Europe. It can cause major hits to U.S. companies.

What should the government be doing to help US companies that are sued from abroad, due partly to perceptions about mass US surveillance and cooperation with these countries?

Mr. Painter: It has been a problem for the last few years. We think it's important not only for American business, but also for European businesses. They understand having a system that is inter-operable but not the same. Privacy frameworks will never be completely in agreement, but they should be inter-operable for the benefit of both parties. I am optimistic it will happen.

We have spent a lot of time talking to EU colleagues in the last few years. One of the problems I see is that people tend to conflate all these issues together. What are the proper rules for surveillance and for intelligence gathering? They group those issues into cybersecurity, but these are not cybersecurity questions. They are important issues, but not the same issue. It has hindered progress in cybersecurity somewhat.

Discussions about surveillance practices need to happen. We have had them in this country. It is what President Obama wants. There are rules and oversight. It is a discussion that should happen around the world. Increasingly countries, including in Europe, are beginning to understand there is a distinction. We need to have that conversation. If there are not shared goals and shared objectives between the U.S. and Europe, there are countries that will try to drive a wedge between us. We can't let that happen. There has been some real progress. The conversation has changed in the last few years, but we need to keep at it.

Mr. Donilon: Your paper makes a strong point on adopting international law and norms in the

cyber world. There should be a core set of peacetime norms that countries should abide by in terms of economic, political and other relationships. What is the way to accelerate this process? Is it not to have like-minded countries come together and expand the circle around these norms? What should the mechanism be to achieve the goal of broad adoption of international law, and adoption of neutral standards of behavior, a NIST type framework and standard of care conduct in cybersecurity? Some people have proposed we should move to a cyber-NATO, an alliance of like-minded countries. In your mind, what is the mechanism for broadening the circle, and getting accelerated adoption?

Mr. Painter: We need to engage at all levels in our international engagements, including the Presidential level. At every summit held by the President over the last year, a significant portion of the summit statement has talked about cyber issues, and everyone has talked about affirmation of those norms. The framework agreement we signed with India last week has core norms at front and center, so India agrees with the U.S. on those. It is working hard bi-laterally, and multi-laterally to accomplish that. What it is not doing is trying to get a "cyber-treaty". I don't know what form that would take or who would negotiate it. Given different interests in cyberspace, it is unlikely to be of benefit to the United States.

There are countries that would want to use a treaty as a means to control information. It is a norm they are trying to push. I think we have to go beyond the like-minded. We need to work with those who are likeminded. It is important to have countries, including China and Russia, who agree to these norms, and this group of governmental experts in the UN, to see the benefit of it and get wider adoption. It is continuing and accelerating, not only at my level, but at the Presidential level, the cabinet level, and others.

We need to get back to capacity building. We have a lot of countries focusing on this, but there are a lot of countries still on the fence. They understand the siren song of stability, which Russia and China talk about. They also understand the benefits of economic growth and innovation. Those are the ones to concentrate on if we are to build this consensus. Capacity building, then, is a key element in the process. It's not just policy engagement. We just need to continue and accelerate that. We have done things in the last year, including work at the UN. We don't want to water these things down. We want to make sure we have things that are genuinely useful to everyone going forward.

There are lots of threads of effort. There has been work on what international law means in cyberspace. That's important. Confidence building measures are the easiest part in some ways because they are practical measures and are value neutral. Having hotlines, exchanging points of contact and other examples are important. We've done this in the OSCE. There are now 16 confidence building measures that we've done. We've looked at ARF as another forum to do that. We've talked to OAS about that. Rather than trying to have one place to convene it all, we need to look at regional organizations and bi-laterally with our partners.

Mr. Donilon: Combine your comments on capacity and regional organizations. The United States Government has not made formal statements on what I am about to talk about, but there is a lot of cyber pressure coming from Russia. We may be involved in seeing a set of broad based information efforts. How would you assess the current state of capacity building at NATO and European

countries to confront this threat?

Mr. Painter: There has been a real change over the years. Remember during our time at NSC, when NATO made cyberspace part of its strategic concept. Now, we've just had the NATO summit where cyber was reaffirmed, and reaffirmed as a domain for NATO activities. The first issue with NATO was to make sure they actually protected their own networks. That was the foundational step they had to take. Real strides have been made there. Working with other governments in terms of their own cybersecurity and national cybersecurity policies has been going well. The cyber-ambassador for technology issues for NATO has been very active in trying to build this.

It has been making real progress because people understand the nature of the threat. They may not know what to do about it, generally for policy makers. Things have changed in the last few years. Now there is a substantive and thoughtful conversation, in the U.S. and internationally. NATO has really grasped this as being something that's critical to the future. The threats we see now are not just physical threats. It involves a few different aspects. Part of it is harnessing the capabilities of NATO members, so that NATO does not have to do everything itself as NATO, but also call upon the capabilities of its members. The doctrine is in better shape now. It is something we are committed to continuing to build. It was baby steps in the beginning, but I think we are beginning to hit our stride more now. There is still more to do. Given the threat posed by certain countries, it has accelerated the understanding.

Mr. Donilon: Given all interactions you've had around the world in the last five years, are there countries, or sets of practices that you've seen that you'd like to see us look at more closely and adopt here? We have very effective cybersecurity regimes for example in Israel and elsewhere around the world. Are there other practices you've seen, are there regulatory regimes, voluntary regimes, governmental structures, or governance approaches that you think the Commission should look at?

Mr. Painter: It is a good question. I may have to get back to you on that. I'd have to do a survey of what I've seen. In many ways, the U.S. has been a leader in this area, where the rest of the world has noted its importance. One of the things I think is critically important and that we have in the United States, but could be strengthened further, is for the U.S. to have a whole-government strategy. There was a strategy back in 2003, but people were not ready for it at the time. We've sharpened it at the beginning of this administration as well.

The Australian Government just came out with a comprehensive strategy. They have mechanisms for working with the private sector that are good. There have been changes in some governments that have traditionally been very stove piped. They are now coming together to work in the government. That is important. There is not a regulatory regime I am particularly fond of.

From our perspective, we want to have all these governments develop these capabilities. We can then plug into them. That's what's critically important. The UK has been doing some good things. They just created a cyber center, and have been working on those issues. I can think about all these issues further and get back to the Commission.

Panel 1: How did we get to here? The Policies that Shape Today's Federal IT Landscape

Dan Chenok, Executive Director, Center for the Business of Government, IBM

Karen Evans, National Director, US Cyber Challenge; Former CIO, US Government
Eric Fischer, Senior Specialist in Science and Technology, Congressional Research Service (CRS)
Gregory C. Wilshusen, Director, Information Security Issues, U.S. Government Accountability Office (GAO)

Dan Chenok, Executive Director, Center for The Business of Government, IBM

This morning, I'll summarize some key points brought out in more detail in my written statement. The policy framework of government federal IT with respect to cyber security has many pieces. Some major laws are the Paperwork Reduction Act, which in 1980 authorized OMB to oversee a broad range of IT activities including privacy and security. The Computer Security Act, which in 1987 gave the OMB director authority over civilian agency security. FISMA updated the Computer Security Act in 2002, and again in 2014, to drive agencies more toward operational security. The Government Act, which in 2002 vested OMB's office of e-government and information technology, with leadership of IT and e-gov issues including security, and last year's Federal Information Technology Reform Act, or FITARA which gives CIOs new authorities and tools to manage IT.

In addition to these general statutes, DHS's cyber leadership was authorized first in the Homeland Security Act in 2002. These and other cybersecurity statutes are implemented through an array of policies that impact IT security including: OMB circulars, that integrate Federal information and IT policy and govern cybersecurity and enterprise risk management; FISMA guidance, which requires agencies to report on security activities, drives agency priorities and inspector general reviews; and NIST guidance which addresses security, privacy, and identity management in multiple ways that agencies utilize to make risk based security decisions. Additional policy frameworks address privacy and identity management. These laws and policies are led by a diverse group of organizations; among them the White House cyber-coordinator, OMB led by the Federal CIO, and the new Federal Chief Information Security Officer in the e-gov office, DHS led by NPPD, and NIST just to name a few. The framework that I just described has involved in a world of rapidly emerging threats.

This Administration is taking important steps forward on IT and cybersecurity policies building on prior efforts and yet much work remains. New policies can promote approaches and technologies through which government can continue to improve in predicting and preventing cyber threats. The following are three ideas for the Commission's consideration, focused on governance, innovation and the integration of privacy and security.

First, rationalize governance around key priorities by clearly identifying roles and responsibilities and focusing collective effort on improving cyber across agencies. This is especially important in a new administration that may have to take rapid action after a cyber incident, and by developing a short set of key goals and objectives, indicating how these goals will be achieved and measured. This could build on the comprehensive National Action Plan and enhanced cyber focus in the government's c-suite.

Second, drive innovation in light of the multiple policies that agencies must comply with many cyber security resources necessarily go to compliance and reporting. But as Secretary Pritzker said, one path to pivot toward innovation could be through the procurement system since most agency cyber security products and services are done by industry. Effective permit requirements

can incentivize sound cyber security practices allowing companies to bring innovative ideas forward as an expected activity. This could enable government to leverage the large 90 billion dollars spent on Federal information technology to attract more innovation from commercial partners.

Third, integrate privacy and security. Since safeguarding personally identifiable information is a key element of cyber protection, the recent reissue of OMB Circular A-130 addressed privacy and security in a more coordinated fashion. Greater integration of policies, programs and organizations can help align efforts to protect sensitive personal information. Collaboration of DHS's privacy office with NPPD provides an effective model of coordination. in addition to these three areas of government, Innovation, aligning and privacy security, enhancing public-private interaction can leverage best practices across sectors by extending real-time threat information sharing at scale, and working with industry to understand the risk landscape relative to mission achievement as part of enterprise risk management consistent with the NIST cyber framework.

Karen Evans, National Director, US Cyber Challenge; Former CIO, US Government

I'm here today to represent my previous role as the administrator e-government and information technology. This role is now known as the Chief Information Officer of the United States Government. I held this position for nearly six years during the George W. Bush Administration, and prior to this appointment I was a career Federal employee serving in multiple positions at various departments and agencies culminating in my appointment into the senior executive service as the chief information officer of the Department of Energy.

I'd like my comments today to provide examples of the recommendations that I included in my written statement. My colleagues today are going to outline the legislative landscape, but I would really like to briefly explain the relationships which were key to the success of the Federal Government's operations. During my tenure, there was a unique point of time of alignment. The Federal Government was reforming its intelligence community and it was standing up a new Federal department for homeland security. Information and the use of information was truly being analyzed. We were also implementing the e-Government Act, which was focused on citizen services, while we were implementing the Federal Information Management Security Act (FISMA), which was focused on securing those. My job was to provide greater citizen services while ensuring security, privacy, and record retention for the preservation of government information into the future.

My manager, Clay Johnson, was the deputy director for management and told me to get this work done, to integrate and institutionalize the necessary processes in to the Federal agencies. He made it clear I was responsible and he held me accountable. I'd like to digress just a little bit to explain who Clay Johnson was at the time because I think that that's critical as you make and consider some of your recommendations. Clay Johnson was a childhood friend of George W. Bush, he worked at presidential personnel, so every political appointee that was in the Bush Administration at that point had been vetted through Mr. Johnson.

Therefore, when I elevated something to my boss, I was really elevating it to the president of the United States. When I go through some of these other things I'd like to have that little frame work in there for you. With this background the statements provided today you can clearly see that the

authorities are segregated between civilian systems and national security systems, between the Department of Defense, the Director of National Intelligence and others. However, given the direction of my manager I worked with the DoD CIO who was John Grimes at the time, and DNI CIO, who was General Meyerrose, and they agreed that I was leader in all aspects of information technology including cybersecurity.

They publicly stated this in multiple forms and the deputy CIO of DOD was then appointed the vice chair of the Federal CIO Counsel. Additionally, at that time the President's management council had an e-Government committee. This was a very disruptive time, and so most deputy secretaries didn't want to have anything to do with technology. At that particular time the most outspoken of them was the Deputy Secretary of Commerce, Sam Bodman. I asked him to be the chair of the e-Government Committee off of the President's Management Council.

We had a scorecard that used the tool for accountability, and the CIO was responsible for the e-Government initiative. At that point, cyber security was included there. The deputy secretaries are responsible for all aspects of the scorecard. The President held an annual meeting where they sat in that meeting according to their performance. I viewed our office as a staff function to the deputy secretaries and appropriate management officials in order to accomplish their goals on the scorecard.

There is another example that I'd like to share generally with law enforcement authorities. Many of you may be familiar with the failed IT project called Sentinel. This was the case management system being implemented by the FBI. I had the unique opportunity to inform Clay Johnson that the FBI had expended90% of their funds and only had 10% of their functionality. Clay called the FBI director and Director Mueller requested a meeting immediately.

As we worked through the issues, Director Mueller realized it was not an IT issue but rather a business culture change issue, and took leadership for implementation. It is a little unsettling when you're commuting home and the director of the FBI calls. The FBI operator would call on the phone and ask for me to take a call from the director. The director really did want to have an open line of communication into my office, He worked to ensure that the project stayed very closely on track. He continues to be involved day to day with that project.

As it relates to technology innovation, public-private partnerships and the role of NIST, I want to highlight the work that was done in support of Homeland Security Presidential Directive (HSPD) Number 12, which was issued August 27, 2004. The title of this HSPD is, "Policy for Common Identification Standard for Federal Employees and Contractors". We now know it as two-factor authentication. At that time, the technology did not exist.

NIST was brought to the White House and the undersecretary told us it would take at least two years for NIST to run its process so that we could have what we needed. We told him he had six months. They are the smartest people in the world and that they could get it done. The General Services Administration was also brought in because they were going to have to receive the handoff from NIST, and it worked. OMB then requested cards from every department and agency and these cards were tested for the interoperability.

Finally, I'd like to bring the auditors into this. They are better known as the inspectors general

(IG) and they are critical to this effort. The IGs evaluated the management processes to ensure the rigor was in place in the department and agencies. NIST provided the checklist that the agencies used for the evaluation in order for us to have a confidence level in those processes. In order to have the partnership necessary with the independent auditors I personally attended every meeting which is now called the Council of Inspectors General on Integrity and Efficiency, to ensure that I could share the priorities of the CIO Council. This assisted with the integration of the IGs and the CIO, and their policies that were issued from OMB.

I do believe that the IGs are going to be the solution to this overall issue is they are independent and they are in place through multiple administrations. Their reports are used by Congress and should provide the baseline in order to measure the progress and improvement within departments and agencies but also across the Government as a whole.

Eric Fischer, Senior Specialist in Science and Technology, Congressional Research Service (CRS)

At the Congressional Research Service, our mission is to provide Congress with non-partisan, objective information and policy analysis on legislative issues. In keeping with that mission, we do not advocate or take positions. Consequently, I cannot make any recommendations or be associated with any made to, or by the Commission.

As you know, Federal IT policy exists within a larger and complex IT and policy framework. No single overarching framework legislation is in place, but many enacted statutes, more than fifty, address various aspects of cybersecurity, the most recent being the Security Act of 2015. Other panel members have discussed, and will be discussing, relevant statutes and policy directives. I thought it might be most useful for me to focus on a set of fundamental and difficult policy challenges that can impede the development of effective legislation and policy.

Now the existence of such challenges has been recognized for many years and of course by other people who have spoken before you. They can be characterized in many different ways. What I'd like to do is focus on four: design, incentives consensus, and environment. Four recently enacted statutes arguably affect aspects of them. I don't have time to go into specifics in this statement, but of course I would be happy to discuss it with you during Q&A. With respect to design, it is often said that cyberspace was not designed with security in mind.

Developers have traditionally focused more on features other than security largely for economic reasons. Also, many future security needs cannot be predicted with any certainty posing a difficult challenge for designers. Harmonizing security with usability is also part of this challenge. If cyberspace has not been designed with security in mind, it can also be said that security has not been designed with usability in mind. It makes it much less effective, as the recent debate over passwords has illustrated.

Education and awareness alone seem unlikely to solve this problem. It impacts Federal IT because, as has been mentioned, the Federal Government acquires its IT largely from the private sector. Research and development, and the education and training of IT engineers and programmers, and the use of Federal acquisition leverage may be helpful in addressing this challenge both from the Federal Government and more broadly.

The second challenge is incentives. The structure of incentives for cybersecurity has been called

distorted, or even perverse. It has been said that cyber-crime is cheap, profitable, and safe for perpetrators. Cybersecurity can be expensive, is by its nature imperfect, and returns on investments are often hard to measure. The question is how does one increase that cost of cybercrime and make cyber security more effective and affordable. This applies to some extent these arguments by some extent with respect to state adversaries as well.

An additional consideration is the degree to which users demand good security as an essential feature of IT. When does cybersecurity become an essential part of the value proposition that buyers and users demand? How does one shift the demand curve in other words for cyber security in the desired direction? For the Government sector with its inherently monopolistic features, trust is an especially important expectation for citizens. The demand for security should arguably be much higher than for many other sectors. From that perspective one can argue that the Federal Government should be a national and even global leader in cyber security. That does not however appear to be a widely held view at present. A question for the Commission may be, what should the Federal goal be with respect to national and even global leadership in cybersecurity, and how can it be achieved?

With respect to consensus, cybersecurity means different things to different stakeholders, as has been stated previously. Substantial cultural impediments to consensus also exist not only between sectors but within sectors and within organizations, even within Federal agencies. The structure of Federal policy has arguably made consensus within the Government difficult to achieve in some ways. FISMA requirements are arguably not enough.

There are significant concerns about centralization, as Secretary Pritzker alluded to. There's also a fundamental conceptual problem that may impede the development of a useful consensus in cyber-security. Cyber-space keeps growing because it connects things and applies computing power to them in unprecedented and useful ways. In contrast, security traditionally involves separation. That arguably creates, potentially at least, a fundamental conflict. Traditional approaches to security may not be sufficient, but consensus on a new conceptual framework has yet to emerge. Significant progress has been made on some aspects of this challenge in the last decade, but it is complex and a more comprehensive approach might be worth considering.

The fourth factor, or challenge, I'd like to talk about is environment. Cyberspace has been called the fastest evolving technology space in human history, both in scale and properties. This rapid evolution poses significant challenges for cybersecurity exacerbating the speed of the arms race between attackers and defenders, and arguably providing a significant advantage to the former.

New and emerging properties and applications complicate the emerging threat environment. They may also pose opportunities for improving cybersecurity. They provide defenders with opportunities to shape the evolution of cyberspace toward a state of greater security. Given the inherently non-agile state of the Federal Government, it may be particularly difficult for Federal policy to take advantage of such opportunities. At the same time that cyberspace is evolving so rapidly, there are core components that are highly conserved. That's analogous in some ways to the evolution of biological organisms, said by somebody who was originally a biologist. Geneticist Francois Jacob said evolution is a tinkerer, not an engineer.

It is easy to take such analogies too far. I think it's useful to point out that attempts to shape the

evolution of cyberspace for greater security need to consider the whole organism not just the individual components.

My final point is that the Federal IT policy environment is embedded in the larger IT environment, which should be considered in addressing the challenges that I've discussed. one example the Commission might wish to consider is election security it might be considered a special case given the role of state governments in running elections but it is an issue of national concern and it may not be as atypical as it appears given that most of the components of the Nation's critical infrastructure are owned and operated by the private sector.

Gregory C. Wilshusen, Director, Information Security Issues, U.S. Government Accountability Office (GAO)

Our mission is to help Congress discharge its constitutional duties and improve the performance and accountability of the executive branch for the benefit of the American people. In my position, I am responsible for leading audits and studies of security and information systems supporting Federal systems across the entire executive branch; as well as for reviewing Federal policies and practices where helping private sector entities to secure critical infrastructure and also protecting the privacy of personally identifiable information. As requested, I will discuss some of the key responsibilities for securing the Federal IT landscape and actions needed to address long-standing challenges to improve in the Government's cybersecurity challenges.

As has been mentioned, several laws and policies provide a framework for securing government information and information systems. Chief among these is the Federal Information Security Modernization Act of 2014, and its predecessor, the Federal Information Security Management Act of 2002. Both of these are commonly referred to as FISMA. Under FISMA, the director of Office of Management and budget is responsible for developing and overseeing the implementation of policies and standards, guidelines on information security in Federal agencies except with regard to national security systems.

OMB is also responsible for overseeing agency compliance with the requirements of FISMA to enforce accountability for compliance. Since 2003, OMB has issued a number of policies and guidance to agencies on information security issues including providing annual instructions to agencies and inspectors general for reporting on the effectiveness of agency security programs. As required by FISMA, the National Institute of Standards and Technology has issued Government-wide standards and special publications that provide detailed guidelines the agencies for securing their information and information systems.

At the agency level, the head of each agency is responsible for providing appropriate information security protections for the agency's information and information systems including those operated or maintained by others on the agency's behalf. They are also required to develop, document, and implement an agency-wide information security program that involves an ongoing cycle of activity that is intended to cost effectively reduce and manage information security risk to an acceptable level.

GAO and agency IGs have responsibilities under FISMA for evaluating and reporting on the effectiveness of agencies information security policies and practices. Our work has shown that they have not fully or effectively implemented these programs and activities on a consistent basis.

While the administration and agencies have acted to improve protections over their information, additional actions are needed.

First, Federal agencies need to effectively implement risk-based information security programs consistently over time. Agencies have been challenged to fully and effectively establish and implement information security programs. They need to enhance capabilities to identify cyber threats, implement sustainable processes for security, configuring their computer assets, patch vulnerable systems, to replace unsupported software and share comprehensive test in the evaluation of their security on a regular basis and strengthen security oversight of their IT contractors.

Second, the Federal Government needs to improve capabilities for detecting responding to and mitigating cyber incidents. Even strong security organizations can continue to be victimized by attacks exploiting previously unknown vulnerabilities. To address this, DHS needs to expand the capabilities and adoption of its government-wide intrusion prevention system known as the national cybersecurity protection system. Agencies need to improve their practices for responding to cyber incidents and data breaches.

Third, the Federal Government needs to extend and expanded cyber workforce in training efforts ensuring that the Government has a sufficient cybersecurity workforce with the right skills and training remains an ongoing challenge. Government wide efforts are needed to better recruit train and retain qualified cybersecurity workforce and to improve workforce planning activities at agencies.

In summary, Federal law and policy set forth the framework for addressing cyber security of federal systems. However, implementation of this framework has been inconsistent. Specifically, agencies need to address control deficiencies to fully implement organization-wide information security programs. Cyber incident response and mitigation efforts need to be improved across the Government. Establishing and maintaining a quality and qualified cybersecurity workforce needs to be a priority.

Panel 1 Discussion

Commissioners of the Commission to Enhance National Cybersecurity

Mr. Lin [*To Mr. Chenok, Ms. Evans, and Mr. Wilshusen*] In the written testimony, you called out the importance of procurement reform. Can you provide examples of the type of procurement reform that could make a difference?

Ms. Evans: Getting things fast isn't necessarily the issue. The issue is making sure we are buying what we need to buy, and then following up on the terms and conditions of the contract. There are a series of tools, mentioned in the recommendation that references back to the NIST checklist. That is a critical piece. Changing the checklist is the easiest, and then have NIST use those tools. The key is, CIOs don't check they actually bought what they said they wanted. If they don't run the tools, or run the checklist, it's not the contracting officer's responsibility. It's the responsibility of the person who receives the goods. The goods have to be checked.

As NIST builds more and more tools, then the market will respond if agencies are rejecting

products that don't meet those checklists and parameters specified for equipment being bought. That's the one piece that when we're talking about skillsets a workforce has to have, the IT community doesn't check what it buys. There needs to be someone on the other end checking the product to make sure it does what it supposed to do.

Mr. Lin: So, we are essentially buying the wrong things.

Ms. Evans: Yes, absolutely. As an example, NIST and DHS did a great job on this. They reached out to Microsoft. This plays to the public-private partnership piece as well. When an operating system changes, it is a good time to harden the environment. We reached out to Microsoft, and told them we will determine what the configuration should be for desktops coming into the Federal Government. We worked with NIST, DHS, and DOD.

Microsoft has a program set up with authorized Microsoft drivers. We required the systems to use authorized Microsoft drivers, which then allows agencies to have the flexibility they need to have. It was a requirement to go through that system. We asked Microsoft to distribute that configuration all through their value-added resellers. They used the existing market. The first time we attempted to buy a tool, it came out that GSA did not run the test needed prior to procurement. They ran the test and fixed the flaw within a month because they needed their stuff.

Mr. Chenok: I concur with Karen on using the check list. Let me talk about two other points from the seller perspective. There is a ninety billion dollar spend on information technology. There is a five hundred billion dollar spend on professional services. Many of those services are themselves powered by information technology in indirect ways. It is a significant amount of government resources that is invested every year.

When companies receive procurements with requirements that have design and mission parameters in one section of the procurement, while back in the back cyber requirements and checklists are given separately. The incentives for the designers are to focus on the non-cybersecurity requirements, because that's what they get paid for. The security is an afterthought dealt with by the security team. Procurements that take the mantra of baking in security, really do incentivize companies to deliver solutions across the vast span in more significant way of integrating security from the beginning instead of waiting to see where the holes are, and coming up with solutions later.

The second point is in regard to innovation. Companies are incentivized to deliver what they're asked to do properly by procurement. Good private sector partners will think more about what they can bring into the Government. Sometimes those discussions are not well received by the Government because things are not within the scope of the Government. There are then separate discussions on what is not required in the contract. Some agencies have added the statement to bring forth innovation as part of the contract process. There then is an innovation element in what the company delivers. It can happen in a number of ways. Companies can then bring innovation to the Government and it becomes an accepted part of discussions about contracts, rather than something extraordinary that must be handled out of the norm.

Mr. Lin: You've talked about a framework being in place but the framework is uneven. Would you say that the policy side is relatively complete, or are there gaps in policy that you see that need to be addressed?

Mr. Wilshusen: I think in terms of policies, FISMA addresses key policies that need to be in place. Some of the guidelines and standards NIST has developed are quite comprehensive, and are used by others outside the Government. I think policies and procedures are largely in place. It is a matter of consistent implementation over time, which remains a challenge for agencies to do.

It may be the case that priorities and skill sets may present barriers to implementation. I might also add that it is a good idea to have configurations and baselines hardened into systems before agencies receive them, because we often find that agencies do not adequately configure systems when they come in default mode, which is usually the case. By having operating systems pre-configured for security settings is a key benefit of the program mentioned by Ms. Evans.

Mr. Lin: In summary, it seems we would do a good pretty job, if only we do what we said we would.

Mr. Wilshusen: That is largely correct. One of the other things is making the vendor confirm or provide evidence they meet the configuration guidelines. There should be some onus on the contractor to prove it, instead of solely relying on the Federal Government.

Mr. Lin: As you look at the cybersecurity landscape in the Federal Government, are there agencies that are good at this, and how can we take advantage?

Mr. Wilshusen: There are some of those that do well, but they tend to be smaller. The National Science Foundation is an example. One of the complicating factors for large agencies is that the computing environments tend to be so diverse. They are geographically dispersed, highly dynamic and extremely complex. Complexity introduces risk. Many of the systems larger agencies use are often riddled vulnerabilities. These need to be addressed. They come from the vendor with vulnerabilities that need to be patched. We find this creates logistical challenges for agencies. We find they often cannot keep up with patching which increases vulnerabilities.

Mr. Lin: In your view, there is no large agency in the Federal Government that does a good job?

Mr. Wilshusen: I won't say there's none that do a good job, but that all need to do a better job. There are vulnerabilities at all agencies. Nineteen out of twenty-four agencies covered by the CFO act reported material weaknesses or significant deficiencies in their information security controls for financial reporting purposes in FY 2015. The IGs of those twenty-four agencies said their cybersecurity was a major management challenge for twenty-two of them. That may be in large part due to the complexity of the systems they are trying to operate.

Mr. Fischer: With respect to possible policy gaps, a lot could be potentially identified, whether those should be addressed by legislation is an open question. It may have to do with agency heads. They have responsibility for cybersecurity under FISMA. They also have responsibility for overall mission. In the board room one of the old criticisms was that the c-suite didn't understand cybersecurity. It was considered a tech issue, and they didn't do anything about it. It has started to change with the advent of other initiatives, including the NIST cybersecurity framework, which was aimed at helping. With respect to the heads of Federal agencies, when confronted with cybersecurity issues, the response is that they may have to compromise with respect to mission. Is there a way to give better tools to agency heads through policy than exist now?

Mr. Wilshusen: We just reported last week that 18 of 24 CISOs surveyed cited tension between

operations and security which, at least to a moderate extent, affected their ability and authority to implement security at their agency.

Mr. Donilon: *[To Mr. Wilshusen]* Have you done an assessment on the expressed adoption of the NIST Framework by Federal departments and agencies?

Mr. Wilshusen: We have not assessed adoption of the new NIST framework. We have been tasked to look at the adoption of the NIST Cybersecurity Framework for improving critical infrastructure cybersecurity for non-Federal entities in critical infrastructure. That was under the National Cybersecurity Enhancement Act of 2014. It charged us with looking at the development of the framework and the collaborative nature of it. We are reporting back in December. We will be looking at adoption by owners and operators of that framework.

Mr. Donilon: But you haven't been asked to look at express adoption and implementation by Federal agencies and departments? Do we have a majority of agencies of the Federal Government not doing what we see almost every Fortune 200 company doing?

Mr. Wilshusen: Under FISMA, we are supposed to evaluate and report on the effectiveness of agencies of the implementation of the provisions of that act. Our criteria that we use the provisions of the law, and guidelines and standards issued by NIST in accordance with implementing that law. We do that on a regular basis. We examine security implementations and policies at Federal agencies using that set of criteria, not necessarily the NIST set of criteria. There is a great deal of mapping and inconsistency between them.

Mr. Donilon: What's the percentage of adoption and implementation?

Mr. Wilshusen: We look at it more in terms of the controls that are in place at agencies and the effectiveness of that. I would say generally we find most have vulnerabilities and significant deficiencies, in a majority of the control sets that GAO looked at. Those are, for example, access controls, which are intended to detect, limit, and prevent unauthorized access to agency system. There is a series of different types of controls that we examine. We look at configuration management, segregation of duties, contingency planning and security management. There is not direct correlation per se to the framework, but the direct correlation to the types of controls that should be in place.

Mr. Lee: I appreciate all your comments on innovation, and the need to embrace innovation. I wanted to go deeper into the culture in Federal agencies with respect to innovation. I think there are three key elements:

- Procurement reforms and having the right tools and technologies at the leading edge.
- Find ways to reward development of new intellectual property, and its exploitation.
- A culture of empowerment, so that workers at the front lines feel from the bottom up they are empowered to make change. I would point out that malicious actors have all these elements in spades.

What can we do to improve how we reward development of intellectual property, and culture within Federal agencies? What can we do to promote culture that promotes risk taking, embracing new ideas, and to empower those on the front lines to make change? Are there things that can be

done in management to promote this?

Mr. Chenok: It is an important element. No matter how rules change, people will act in certain ways as they operate systems across government. There has been a lot of progress in the digital services world, bringing in innovation through strong information technology professionals who are with government in new ways coming in from the private sector. There are ways to ingrate people with those skills into agency teams.

So far, they are separate teams in government and have not been integrated. There is an opportunity to use the best of innovation that's coming into government through these new programs, and integrate them into the rest of government to make better use of the investment. It requirements leadership and people to work together to try new ideas. As agencies try new things and test new approaches and ideas, it can promote the attempt to seek out something new and reward the learning from that and celebrate success, and move forward.

Ms. Evans: I would caution the Commission not to overlay more hierarchy on top of what currently exists. Maybe the role of the CIO has come and gone. The CIO may now need to be the infrastructure officer or others. Get rid of some of Federal jobs so that responsibilities are clear. CIOs are not the police. They enforce compliance. Career people know what needs to get done and recognize the need to create a learning environment. Chief data officers may be more relevant. We need to create a learning environment. It takes leadership and management skills.

Mr. Chenok: Regarding CIOs, there are two paths. One is the path laid out by Ms. Evans. There are examples of strong CIOs in the Government that are taking a more integrative path and treating information and risk management as a strategic goal, and working within their agencies and other CIOs.

The CIO may or may not be a thing of the past, but it may be more of how to empower IT leadership to embrace innovation. The CIO is the legal leader of this process in the Government. Moving forward in that direction may be more instructive in working with the legal framework we discussed earlier. However, the risk is there of going down the other path.

Mr. Lee: It is an interesting set of comments. It is a trend at a company like Microsoft, and may also be true for IBM, that increasingly it is the enterprise customer is not the CIO but someone else. It may speak to that desire for innovation.

Mr. Fischer: Your questions brought up what happened with research in the 1980s. There were concerns Federal research is trapped in the Government. There needed to be ways to make it more applicable. That led to acts that were widely considered to have been successful at helping to develop the great engine of biomedical research applications. Whether or not that should be revisited with respect to cybersecurity is something I haven't looked at but is something that might be worth thinking about.

Ms. Evans: One other thing on innovation. I have a cooperative agreement with DHS in research and development from the Science and Technology (S&T) Directorate dealing with innovative tools for workforce, because workforce is an issue. The S&T Directorate has a partnership with private industry focused on cybersecurity. The Commission may wish to talk to them about their whole portfolio as it relates to innovation in this particular area, and how to get the intellectual

property out to private industry as well as adopted by Federal agencies.

Mr. **Ziring**: I'd like to add a couple things. First, within agencies, the integrated team approach would be helpful for providing additional avenues for empowerment. All too often information security is cited as a separate issue done by the CIO. It should be actively involved with the senior managers of the agency who are responsible for delivering services, and the fact that they need to assess and address cybersecurity within their sphere of influence. Having the integrated approach will help raise the level of risk relating to cyber as well as other operational risk. The other aspect is on a global basis in terms of new innovation is the Federal Government spends billions on research and development each year.

However, in years past there hasn't been an overall collective repository of information about the different types of different R&D projects underway related to cybersecurity. Who is performing research and development, what the results are, costs? Having a central repository can inform on what's being done and reduce duplication of efforts, possibly facilitate results sharing by the Federal Government.

Mr. Chabinsky: I wanted to touch on the hardware and software life cycle. It seems increasingly almost everything now is disposable. What we've heard is the way the Government is set up, does not allow for refresh as much as for operations and maintenance, which is a point that Mr. Chenok touched upon. It seems there is a lot of stickiness. Its what vendors want, to make it difficult to transfer out hardware, to export data readily between products. It seems there is a need to have the backend must be flexible to be able to find a way to refresh systems. Is it a procurement budget problem, a procurement problem, a vendor requirement problem? What might allow for more nimbleness in moving things in and out? What should the Commission consider to allow for more frequent refreshes and shortening the lifecycle of hardware and software installs?

Mr. Chenok: The answer to your question is yes. Secretary Pritzker referred to the appropriation cycle. The fact is, it takes CIOs working with budget offices two years in advance of when technology is actually implemented, working with a contract through the lifecycle of how agencies do their planning. Building greater flexibilities to pivot on implementations, particularly in the budget execution process is important. When we talk about the budget, we think it's all about budget formulation in the agencies, but it's all about budget execution. Having the CIOs work with their procurement shops and being able to shift as technology changes are not always written into the rules by which the money is appropriated, or the contracts that carry out the spending for that money would be of great assistance. That's one piece.

A second piece gets back to the culture question. Agencies believe they must follow the lifecycle through. It is hard to change. Building an agile approach into contract requirements will help. The Government is starting to adopt this as a practice. It needs to be accelerated, and to do that shifting more flexibly.

Ms. Evans: This is another area where I encourage the Commission to be bold. The reason why there is a challenge is that agencies want to own their hardware and software, or build their hardware and software. If you look at innovation and what's out there, a discussion needs to be framed about how the Federal Government can lead this effort. If we can figure out the issues of

data flows and how that works, that trickles down into the Federal Government and the Federal market.

Guiding principles (such as data ownership) will allow agencies to take advantage of the cloud. The CIO understands the principles involved and should be able to make determinations about the enterprise and building infrastructure. That would break the mold. Right now, we have data localization as the result of various acts currently in effect. All configuration would shift to the cloud. It allows risk management and better roles based access to systems.

Mr. Fischer: The problem with O&M has been a long standing problem in a number of areas with respect to federal procurement. It has become particularly acute in the IT area because of the rapid evolution of the space. There are two things I wanted to mention. One, the President in his budget proposed an IT modernization as working capital or a revolving fund. It has now been incorporated with an agency-specific fund. The draft is on the website. It creates two funds, but one is intended to work toward cloud computing. It is one way to solve some of those problems.

Also, some have suggested energy performance saving contracts as another way to accomplish the goal. They contract with provider who covers the capital costs, and the company accounts for it in their operational budget. The question of whether those sorts of models, available in other areas may be of use in this one.

Mr. Wilshusen: The complexity of the federal enterprise is influenced and exacerbated by the old technology that is still in use. The Government spends eighty to ninety billion dollars a year on IT. Fifty to fifty-five billion of that is spent on operations and maintenance (O&M). There are efforts under way including data center consolidation to help reduce the overall footprint and movement to the cloud. It is not going as fast as it should. There are still systems using 8 inch floppy disks at one agency for certain applications.

Mr. Sullivan: I have some questions regarding workforce. Do you have a sense of how large is the group of professionals in the Federal Government who are actual security engineers in the Federal Government as opposed to compliance or other types of auditing roles?

Mr. Wilshusen: OMB used to report on the number of individuals who did cybersecurity. It has not provided that information in the annual FISMA reports in the last few years. It is difficult to estimate. More recently, they have reported the amount spent on cyber activities, which can include shaping the cybersecurity environment, and protecting and detecting incidents. The third category has to do with training and some other aspects. This category does breakdown costs associated with those activities, as reported by agencies to OMB. No actual numbers are available related to cybersecurity engineering.

Mr. Fischer: For a number of years, there have been concerns about how exactly do we identify individuals working in cyber security across Federal agencies. Different agencies have different criteria for identifying it. This is reflected in the annual FISMA reports, which show budgets for cybersecurity. OMB has tried to adjust the criteria for submission of those budgets to harmonize what different agencies report. There is a requirement for OPM to develop a cybersecurity job code structure in the Cybersecurity Act, which didn't exist before. There are widely varying estimates of the number of people working in cybersecurity and what they did.

Ms. Evans: In there it also says competitions. It is another thing to think about for the Commission. This administration has moved forward with dealing with workforce issues, based off what happened with the CNCI, because the disparity in workforce existed. We were reporting on skills and needs based on the Clinger-Cohen Act all during my tenure. Cybersecurity is not viewed in terms of the distinction made between engineers and policy compliance is huge because the major bulk of the workforce is focused on that in civilian agencies. In DoD and the intelligence community, they have changed some of their workforce makeup.

The National initiative for Cybersecurity Education actually takes job descriptions and puts them into thirty-two categories. The idea was to make that distinction, and OPM would provide the job classifications. Currently, the Government has parentheticals which clarify the job titles. A bit more is needed to clarify job descriptions. As a result, most cybersecurity engineers are in the private sector, and the Government contracts for them. If we contract for that service, we should receive that services because we pay a higher amount for it. If we look at some of these agencies where breaches are happening, we're back to what did we contract for and what was the solution that was put in place in order to effectively manage the risk they were contracting the service for.

Mr. Sullivan: What should the Commission recommend to address the problem you describe?

Mr. Chenok: There is benefit in a diverse supplier base. I'm not sure decreasing the number of suppliers in the supplier base is necessarily the answer from a supply management perspective. We want enough people inside who can actually judge the work. We do want more people on the inside, through direct hire for cyber authority, which is an authority agencies have that isn't exercised as much as it could be. Getting more cyber expertise into government is a key element. Then, managing workforce with more skilled leaders and teams. Incentivizing a blended approach is how the work happens. The work gets done by contractors and employees working together with government leadership.

Mr. Sullivan: Why should we assume that a blended workforce of outside contractors is more effective?

Mr. Chenok: I don't believe given the number of people providing engineering services are necessary to securing government systems, that if they were all actually put in the Government, it would be a realistic approach. The number of government employees would then rise to an untenable level politically.

Ms. Evans: I believe it depends on what should the Government's long-term goal should be. Depending on what recommendations the Commission makes as it relates to the overall piece about data, and what federal agencies should do, how we get down to that may actually answer the question. If more is shifted out, and the CIO shop is more strategic, it means they need to have a different set of skills. There would then need to be more engineers who understand it, and some people on the front lines that I like call first responders. They would have the ability to detect and know how to elevate upward to the appropriate people. This would work internally. Depending on how it's envisioned, the Government may be able to call more on a different skill set. CIOs would know how to actually manage procurements and have engineers who can test the different types of things they need to have in order to be able to go forward. It shifts us away from compliance and more toward innovation. GAO measures points in time, and those points become outputs. They can

be indicators that something isn't right. But if the overall goal is data center consolidation, we'll get data center consolidation.

What is the goal the Nation is driving toward with respect to the Federal agencies? If agencies are to manage citizen information in the best way possible, with record retention into the future for preservation of that information for how we made decisions. That's what we want. How do we figure out the right mix to achieve that?

Mr. Ziring: I would add a couple things. I'm not sure measuring outputs is really what GAO does. The agencies and the government need to better define and measure outcomes. The government is good at measuring outputs. As far as measuring outcomes of activities in terms of success and achieving the intended goals, it is a more difficult challenge for the Federal Government. Also, to the extent work is being done by contractors, the government needs to have the employees and the capabilities to ensure that whatever services are being provided by contractors are appropriate, sufficient to meet requirements for the product or service. Too often we find that agencies do not do a very good job at assessing and reviewing the work of the contractors they hire.

Mr. **Sullivan**: How do we structure it so we get more of these people into the government?

Mr. Fischer: The question I have in response to your question is, what do you want them to do and how do you want them to do it? People have two goals that compete: one is stability. We need people who can understand the mission of the agency and what is needed, and make sure those needs are filled. The other is flexibility, to bring in people to meet problems as they change. When we bring in a civil servant, then that's what they are. The question then is, can we keep educating those people and bring them up to speed? Or should we allow the private sector to handle the education.

Ms. Evans: If we're looking at this specifically for cybersecurity, we can examine some of the models this administration has brought out. We also need to look at how NSA recruits very early. They start early in college, and have students apply for jobs a couple of years early. The Executive Exchange Program can play a role. The intent of that was to bring engineers in for specific projects and to rotate them out for them to have a better understanding of what was going on. That provision has sunset. DHS attempted to get it re-authorized and Congress refused, due to a host of other issues. It is a way to look at that, and that authority could be brought back to the agencies, and the agencies could do that. In times where there is a surge, they can hire engineers available right away that are part of the Government. When they are not needed, they can return to industry. It helps them understand the Federal Government more, so that they can provide better solutions.

Mr. Chenok: Here is a specific idea that you might build on from the current administration. The additional services teams started with a program called the Presidential Innovation Fellows. People came from industry for a period of time. An offshoot of that could be the Presidential Cybersecurity Fellows. It would be a way for people to come into the Government and drive leading edge activity along the lines described by Ms. Evans.

Ms. Wilderotter: I've spent most of my career in the private sector and, as I hear about the intricacies of how the Federal functions, my eyes glaze over. So I want to talk about thinking boldly. What I would like to hear from the four of you, is political incorrectness. You have all lived in the system for some time and what I hear from your comments is things are not working when it comes

to cybersecurity. I don't know if the issue is accountability, or incentives, or all of the above, or maybe just structure.

But I know that all of you, when thinking and talking privately, have some ideas about how you might shake things up if you had the opportunity and authority to change things. From a policy perspective, maybe get out of what you know, and use your experience to give us some thoughts on really bold change. I invite you to tell us what policies might require a paradigm shift that we could implement, that could truly move the ball down the court, not years from now but with a sense of urgency.

Ms. Evans: I have a couple. As an example, suppose there is a particular policy in place, and we are following that policy regarding configurations or whatever it might be. My view is, DHS should use its authority to shut down an agency, and take an agency offline. In my career at the Department of Justice, when I was running networks, we found a computer not doing what it was supposed to do. We took over the computer, and didn't let them function. When they turned on the network they were busted. We need to be bold, and if we say disconnecting agencies is the policy, then DHS should turn them off. DHS has been reluctant to act.

If we're running operations, and someone is not doing what is required, then they should be offline. They are introducing security vulnerabilities to everyone else. They should stay offline until the issue is resolved. The courts have done that to the Federal Government. For example, the Department of the Interior website was taken off the internet because of the Indian Trust Fund, and the department was not doing what it was supposed to do. The court then shut the department down. I don't think we should go that far. DHS should say don't do it, and take them offline.

As far as CIOs, if they have negative attitudes that keep them from doing their jobs, then they are not the right person for that position. We are talking about people who need to partner with others. If three is a continual string of excuses about why they can't comply and get things done, they should be moved aside. They are political appointees that serve at the pleasure of the President. The President is not pleased. I have had to have those conversations with CIOs. It is not an easy conversation to have. It only needs to happen once or twice, and the message is out there, and people do their jobs.

Mr. Chenok: A couple of ideas. One idea might be a Cyber National Guard in which students could train for a specific period of time within an agency, then serve in a reserve capacity subject to call-up when a cyber incident occurs. Within Government and critical infrastructures, there has been talk about creating this. The administration added the ability to create a cyber national guard to the budget last year. It would tap in to the private sector, and increase a sense of citizenship.

The second is, we now have CIO teams and CISOs, who are organizationally in their own line in an agency. Then there is the program side. They work together, and we've talked about integrated teams. It may be that embedding a cyber leader on every major mission team, and making that the rule that every team has it. That is a cyber leader is part of major agency operations providing services to Americans every day. They would provide awareness on how technology impacts the mission every day.

Mr. Wilshusen: Possibly the elevation of the CISO within an organization and elevate risk

management into the overall architecture of the enterprise. We now have situations where CISOs don't have strict any line of authority over the component level. Often they have a line of reporting to the head of a component of an agency. In some respect, we need to elevate cyber security and the risk management of cybersecurity to into the overall risk management of the enterprise. Too often in the past the priority given to cybersecurity has not been as high as it should have been. Our intelligence community has said that cybersecurity is one of the greatest threats to national security. Should we not consider it as such, and treat it that way within our Federal agencies, and give it the appropriate resources.

Ms. Wilderotter: Does the CISO report to the head of an agency?

Mr. Wilshusen: No, not now. Normally they report to the CIO.

Ms. Wilderotter: Where should they report?

Mr. Wilshusen: That might be something to elevate to a higher level. Should that position be a peer to the CIO? Perhaps, because one of things we found with our recent survey was seventy-five percent of the CISOs interviewed said that that tension between operations and security affected their ability to secure their systems. Typically, CIOs focus on providing services and on the operation side. The goal should be to provide those services securely. Yet, while security should be supported at a higher level, it is not the end of the process.

Ms. Evans: I have had the opportunity to be eight years on the outside, so I appreciate the opportunity to appreciate private industry and how private industry looks at this. I am disagreeing with Mr. Wilshusen because the title he is talking about is Chief Information Security Officer. It will cause more confusion because of the word "information". If I were a new secretary coming in, I would want a Chief Risk officer. If we are going to a risk based framework, and we want to go to a threat based approach, we need a risk officer who is looking at the overall environment, and can identify the mission and risks. Then, it would perpetuate down the line.

If an agency is going to have a CISO, that position stays under the CIO because it's information security risk. If there is a risk officer where cyber could reside, then the secretary is looking at risk to the enterprise as a whole. It becomes a comprehensive risk approach based on all risk.

Ms. Wilderotter: It then becomes a report to the head of the agency?

Ms. Evans: It could be a report to a head of the agency, or work with the inspectors general, because there is an internal audit function, as with corporations, and GAO is the external auditor. The risk officer can report to the secretary, but also work with the inspector general, and work with GAO periodically.

Ms. Wilderotter: It also opens things up more to integration with public-private partnerships too, as the structure is similar to what businesses have.

Mr. Wilshusen: It is appropriate to have a chief risk officer. Where there is a danger is where there is a CISO, his/her input may go to the CIO where there are different focuses than what may be on security. If we are talking about risk, it should be input to the chief risk officer.

Mr. Fischer: Suppose that, in the State of the Union, the president states that the United States should be at the top, or among the top tier when it comes to cybersecurity practices, followed by

proposals related to attaining that goal. If done right, it could lead to Congressional activity, as was the case with the establishment, in 2002, of DHS. This was followed by a prolonged period of Congressional inactivity until President Obama initiated the Cybersecurity Policy Review and proposed legislation. It took three or four Congresses before those policies became law. A number of the things that were enacted were administration proposals. They are now law. One is the cybersecurity scholarship program. It is a small program. One of the things the Commission might consider, is should that program be expanded and changed so that it really becomes a draw for recruitment.

The cybersecurity framework is another example of an Obama administration initiative issued after Congress failed to enact the Cybersecurity Act. The framework came out of an initiative in the113th congress. Now, it is law. The administration advocated for expanding the use of ISACs, and proposed use of ISAOs to promote sharing information. ISACs for critical infrastructure sectors were created in the Clinton administration. They were somewhat limited.

What the Obama administration did was to stretch it as far as possible and propose development of specific information sharing organizations. One of the reasons they did that was give the entertainment industry its own ISAC following the Sony hack. There are many things people trying to do, but leadership is needed from the top to make it happen. It depends what the next president thinks is the top priority. The question is how bold do we want to be? The Commission can propose what the new president might do to move the ball forward.

Ms. Anton: I'm curious about the GAO reports. When you go in to do one of these studies, it seems a lot of emphasis is placed on management practices, business practices, but not as much on a technical review of the systems that are used to support different things. For instance, looking at how the Government is securing sensitive data, how we do notifications of data breaches. My question is, it seems we focus a lot on reporting of incidents, and complying with regulations, as an auditing and oversight activity, and I'm wondering whether we have an equally important engineering activity that should feed into the design and implementation of advanced analytic systems that might thwart data breaches instead of calculate when people should be notified.

Mr. Wilshusen: Our audits do have technical aspects to them. We examine the technical security controls in depth that are designed and implemented into the systems. The results of those reviews are typically not available publically. They are issued to the agency and to requestors in Congress. It may appear from the publically available reports that we focus on processes and other aspects, but we also look at the technical security controls. As an example, there may be fifteen or twenty recommendations in the public report relating to the security program, but we can have a hundred to a hundred fifty or more recommendations relating to the implementation of technical controls over the networks and systems that are reviewed. That information is not available publically, as this information might be exploitable.

Ms. Anton: What sort of follow up is taken after that?

Mr. Wilshusen: We follow up annually to see that recommendations are implemented. We verify that agencies have implemented our recommendations. We look for evidence to verify the effectiveness of the implementations. We track that, and it is one of our performance metrics. We look at the percentage of recommendations that have been implemented after four years. Some

recommendations take time to implement. Agencies will implement nearly 90 percent after four years.

Ms. Anton: It seems tolerating vulnerabilities for four years is not effective.

Mr. Wilshusen: That is not the case. What we're doing is checking regularly to see if the agency is correcting vulnerabilities. We return every year. The performance metric we measure for our work and performance is based on the four-year period.

Ms. Anton: It seems like a great opportunity to shut some things down.

Mr. **Wilshusen**: We are getting ready to issue, or have issued one report on FDA within the Government. It will be released publically possibly this week. That report will identify processes and the number of technical recommendations we made. Since the LOU report has been made, the agency has been taking corrective actions on the technical control weaknesses we identified. We will be working with them to verify the effectiveness of their actions.

Ms. Anton: How can we better incorporate the findings of non-public and public reporting into system and process design rather than being a completely separate activity that never helps inform the way we need to design systems in the future?

Mr. Wilshusen: There should be a way to do that. The NIST Cybersecurity Framework provides the structure to arrive at the results you've described.

Ms. Anton: How does that coordination happen?

Mr. Wilshusen: We can report to NIST on that. In compliance with FISMA regulations, we report every two years on the status and quality of implementation, without mentioning specific agencies. We report on it broadly, but how that information may be used for development of NIST guidelines, there may be a gap.

Ms. Evans: The law says the OMB director is responsible for this. The job of CIO has a lot of authorities that allow activities to occur. It goes to the CIO having operational capabilities, and not just policy. When the information comes in, and we're asked who is supposed to take care of it, it used to be my office. It was my office that did the analysis, and where responses were needed from industry or NIST. That was the role of the OMB director. If there was a job description of this position in the White House, I could be bold there as well. People get this job for a lot of different reasons. It should be clear what the job is supposed to do, because many of the things you're asking is what we did. We have the authorities through the e-Gov Act and others. It needs to be clear what the role includes when someone takes the job.

Mr. Chenok: – It is especially true now under FISMA 2014, because it changed the dynamic to operational cybersecurity as the paradigm agencies should strive for. The previous version said, we will certify and accredit systems for three years. Now, we do a much more continuous review. It is moving in the right direction. Leadership must be provided to implement them.

Mr. Banga: A private sector approach to this: When you define a big problem in front of a company, in this case cybersecurity and related threats for the Government and country, the first thing is to define a strategy to solve the problem. Once we have the strategy, then figure out who is responsible to execute the strategy, assign a budget, set up metrics to assess progress, and make

determinations. Then we celebrate success, or they're fired. We have spoken a bit about ownership of assessing a bit of success or people being fired. I'm still not clear who owns the strategy in the Federal Government to do something about this? It is dissipated across every department, CIO, CISO and a bunch of watchdog agencies that then come in tasked with examining the problem. It is not the strategy that for the executional elements of the process. I'm trying to get to who owns the strategy for this mission critical issue for the next five years?

Mr. Chenok: It is an excellent observation. Having a clear statement of priorities from the president would be another bold activity, especially in the first month for the new administration. This administration has brought together many of these authorities, and many of the offices work together now after a period of years. Starting at the presidential level and working down to NIST and DHS creates a governance framework where it's clear from the chief executive, the way to drive cybersecurity across the Government, and as Ms. Evans pointed out, holding agencies accountable. A version of the CIO scorecard could be a version of a metric system that could be used to track new priorities of the president.

Ms. Evans: The President owns the strategy. Cabinet officials are responsible for their portion of the implementation. The law is clearly set up that the Executive Branch and the President is clearly in charge, and agency heads have pieces of the strategy, which is why I was urging that the Commission not layer more stuff here because the President is our boss. All roads on this subject go to the OMB director. They know this is the President's priority, and what has to be done. The bottom line is the President is responsible for this to the nation. We can make all kinds of recommendations, such as for a risk officer or others. The Executive Office of the President knows how to support Presidents through transitions. The other part is, the President needs to stay on it and hold the secretaries accountable.

I'm sure in the OPM situation, that director went to the President, and said, do you want me to resign? Whether someone in that position is hurting more than helping is a discussion that has to happen at the agency head level, not at a CISO level or any other. It is clear and there needs to be accountability.

Mr. Fischer: On that, the President is constrained by statutory and constitutional authority under which they operate. It is something to be taken into account**.** With respect to cybersecurity specifically, I would point out that the agency heads are responsible for cybersecurity, but the primary responsibility is fulfilling the mission of the agency. If they're in a situation where given budget restraints and other problems, they find there is this kind of tension between making sure the cybersecurity is right and making sure other aspects of the mission are fulfilled, how do they balance those out? It is not always clear.

In the case of OPM, one of the things that was said was they had to keep fulfilling their mission. It was difficult to deal with these other problems because of limited budget, etc. At the same time, if agency services are brought down, there will be pushback. It is complex to try to balance, but under the law, it is the agency heads that have the responsibility. OMB does have some authority to go into agencies and possibly cut budgets, or give another party authority to solve the problem. DHS has authority to act under imminent threats to act, and also to require agencies to use EINSTEIN. They can issue binding operational directives. However, DHS cannot enforce those

directives. Only OMB can do that.

Lunch

Readout from the August 3, 2016 Subcommittee Meeting –

Sam Palmisano, Vice Chair of the Commission on Enhancing National Cybersecurity

We met on August 3, 2016 for the working group session. We were briefed by the White House. OMB, GSA, DHS, DOD, DOJ, NIST, and NSC were represented at the meeting. They were very responsive, and we thank them for their attention. They identified some issues and some challenges for the Commission. What we've heard in many other hearings is that there's many people responsible. There is a lot of work going on, but connection points are weak. Therefore, coordination sometimes is a challenge, especially when it comes to the civilian side of government versus national security.

They also identified areas where there's a little bit of a conflict between the mission of an agency and cyber and how to bring those two together. What gets the priorities of cyber and mission? That's a challenge that they have. They all have challenges around skill-sets which is not unique given our country has a problem with the skill sets around cyber. There a lot of practices under way that are good and they're effective but there's more that can be done as far as cooperation. I would like to thank all the agencies that spent some time with us. It was very helpful.

Panel 2: Growing and Securing the Digital Economy

Alan Davidson, Director of Digital Economy, U.S. Department of Commerce; Senior Advisor, Secretary of Commerce

Rick Geritz, CEO, LifeJourney

Mike Walker, Program Manager, Information Innovation Office, Defense Advanced Research Projects Agency (DARPA)

Neal L. Ziring, Technical Director, Capabilities Directorate, National Security Agency (NSA)

Alan Davidson, Director of Digital Economy, U.S. Department of Commerce; Senior Advisor, Secretary of Commerce

I'm the director of digital economy at the Department of Commerce I can offer perspective from that role of trying to harmonize our digital economy policies across the Commerce department and across the Government. I'd like to explore three main themes with you here today. The first is that the digital economy is something you all know, a central feature of our broader economy and our future prosperity. The second is that we know that the digital economy will not thrive if people cannot trust their security online. We also know that any solutions we pursue need to be consistent with our values and with the strategic goals that we're pursuing across the whole of broader internet policy in the digital economy agenda.

I'll start by talking just very briefly about our digital economy and how we look at it and how it might inform how we think about cyber security. In our work at the department.

We were driven by this conviction that the internet and the broader digital economy are critical parts of the future success of our broader economy. There are lots statistics I could give you about how big the digital economy is. It is still actually an active research area as we try and think about how to measure the digital economy. Even those numbers wouldn't really capture what we think of as the true impact of potential. Every company today is a digital company.

With websites, back-end systems, the internet of things; technology is really making it so that it's very hard to be in business today in America without having some big digital component. The success of the digital economy, and we really do believe it's been very successful, is that at it's here, we believe a function in some ways of the architecture of the modern digital economy. its open its gatekeeper free it allows innovation without permission it allows access to anyone around the world with a connection to get access to the world of human knowledge and commerce and it and that has enabled it to grow at scale.

We have millions of organizations, billions of people, tens of billions of devices now all connected. We do believe that that is very much a function of the approach that's been taken to the digital economy. We also know that the success that we cannot take for granted, we should not take for granted. Technology is changing rapidly. Increases in computing power and new increases in activity greater data usage, all the trends that we see out there, the internet of things.

We could talk more about what we see as the most impactful. They are definitely changing business posture and will be changing the cyber security posture. We know that US business faces intense competition overseas. We can take the success we've had to date for granted. We will see new forms of regulation rise over the internet. The old conventional wisdom was you couldn't stop the internet. It's a force for freedom and opportunity. If you have the internet you have an open economy. You've got an open social platform.

The new conventional wisdom is very different that actually countries around the world are regulating in ways that we don't always find comfortable and we think may be jeopardizing much of the digital economy as we know it. We find ourselves situated in a broad debate about the future of the digital economy and the future that none of us can take for granted. We have an agenda to Commerce Department that is deeply involved in all these different pieces I tried to lay out some of it in the testimony you have.

You're probably familiar with promoting a free and open internet around the world, working on issues like internet governance and the privacy shield, promoting trust online, and all our cybersecurity work that you are probably familiar with. Our work on privacy, and work on encryption, we have internal debates in the White House about those kinds of issues. We do a huge amount of work on access to the internet. A quarter of American homes still don't have access to broadband. We work on Spectrum, to promote adoption and access to the digital economy.

We also do a lot of work on promoting innovation, smart intellectual property rules, engaging with new technologies early in the lifecycle. I say all this because the core point I want to emphasize is that we have been pursuing probably for 20 years now an approach to the digital economy that embraces these kind of basic tenets of openness, decentralization, technology neutrality, a humility in the face of when we think about regulation in this space. That has

arguably been very successful. It's something that we've had going on for three administrations now since the late 1990s. Anything that we do when we engage in this space we need to think about that broader strategic posture, and we need to think about the broad that we're were having around the world in many ways between open and closed societies about what kind of fuel economy we're going to have.

I say all that because I think that's the right context for looking at cyber security. I tried to lay out in my statement what you folks have some of the high-level approaches that we think are important think about. We know that comprehensive effort to address cyber security is going to have many facets. There's no silver bullet. You folks have discovered that. This is not something that that the Government can do alone, and it's also not something that any one country can do alone. There's a huge international convention to anything that we pursue. I'll just take off some of the highlights of approaches that we think are worthy of your attention. I say this because each one of these merits a session of its own, in some ways you had sessions on many of these topics. We could discuss them more in the Q&A. I just wanted to mention, obviously a starting point for us, is pursuing recipes approaches to the issue.

We focused on public-private partnerships and processes. We worked arm-in-arm with the private sector on the cybersecurity framework which you're very familiar with. We think that is a great model for how to pursue solutions in the space. We believe that openness and Innovation or ultimately going to be important in building and building the solutions. We got to harness the power of the private sector we've got to use the openness and decentralized approach to that we embrace for the digital economy. We've got to put it in a harness in service of promoting cyber security solutions. Private sector engagements security by design, you've heard our secretary and deputy secretary talk about these issues.

We don't think that these are empty words, security by design is something that people talk about a lot, figuring out how to get cybersecurity baked in. We need to do more to make sure that there are incentives and tools for companies to build in cyber security from the very beginning. public education I know this in there you've also explored we think it's just to underscore obviously truly essential to give to help the American public, the broader internet public, understand how to protect themselves online, understand what tools are available. I would just underscore that it's also businesses, particularly small and medium-sized businesses who need those tools who will be looking for them. Any public education efforts, and there must be a public education and awareness component to this needs to have those audiences in mind.

Building the workforce is something else the Commission has looked at and broad challenges of creating a highly skilled and adaptive security workforce. How do we make it so that there's a good incentive in the career path of technologists to be part of government and to be part of solving these issues?

I do believe that we have a generation of millennials that cares about these issues and wants to be engaged. In closing, this is going to be a long and hard fought struggle against a growing cybersecurity crisis, which is why we are all here. I encourage you as you think about your recommendations to consider the broader context of this digital economy that we've been pursuing. and we need to make sure that anything that we do in internet policy including our

approach to security doesn't undermine our values and doesn't give aid and comfort to those who are taking a very different approach globally to how the internet and the broader digital economy of all.

I think we really do believe that we need to make the case the people around the world that an open decentralized, innovation without permission, digital economy is good for all of us and could be something that we can keep secure.

Rick Geritz, CEO, LifeJourney

I am CEO of a company that developed a tool that takes the nation's STEM and cybersecurity leaders, and reverse engineers the journey they took to become successful. It allows students of any age or any means to test drive what it would be like to live a day in the life of their journey. We started building this technology a few years ago. The driver behind it was the skills challenge that we're facing in the nation around cybersecurity. Depending on what article you read, I think the latest one by Forbes, showed an estimated 1 million open and unfulfilled cyber security jobs in the world by the end of 2016. Then, if you add on to the other types of positions in cyber-law and cyber-insurance and all the peripheral careers that surround cybersecurity and data science that numbered grows by 2 or 3 times.

The country right now is in a space race. The last time we saw a situation like this was in the sixties, when there was the rush toward space. Right now, unfortunately cybersecurity is not part of the curriculum of our of our Nation's schools and high schools. It is becoming available now in in college mainly due to the NSA's program with the cyber centers of excellence, making its way deep into the universities.

There are millions of students that are coming up through our Nation's high schools. When you ask them what they want to be when they grow up they still are answering doctor, lawyer, and football player. They're not saying doctor, lawyer, or forensic analyst. They're not saying doctor lawyer, data scientist or exploitation analyst. Furthermore, when they go home and they have discussions with their moms and dads about what they're going to be, or what major they're going to choose. The parents are not aware of these careers either. They don't know what a CISO is. I think that what we're dealing with right now is the issue around how do we create a new generation what is called the cyber generation

I was recently in Perth, Australia on Thursday last week and I was at a presentation because cybersecurity as we all know, does not have a zip code. It is a global supply chain issue and every one of our five partners around the world are dealing with the same issue. Then there's a number of other countries that are not part of the five-that are dealing with this as well. Cybersecurity is a global skills issue and a global issue that many countries are dealing with. In this presentation the professor of a major university in Australia made the comment that the United States, the country that invented the internet, is also the country that is leading the way in securing the internet. The secret weapon that that they have is this thing called NICE, the National Initiative for Cybersecurity Education. They held up a brochure and talked about a framework and a place where our universities, industry and so on could collaborate.

The outside world views us as leading the way. The outside world views us as is being number

one. But as we all know there's still a lot of challenges and a lot of steps we have to make to do that. My company powers a program called the "NSA day of cyber", where the student can go online and live a day in the life of one NSA's cyber leaders. When we first launched this, we didn't really know the appetite for cyber security. There was a lot of concern that asks, does cyber security actually have a brand out there with middle school, high school, community college, and university students? After the first 7 months, we had 3.5 million students sign up and say, I want to explore what my life would be like, if we were going to do that.

I think we're at a moment in time right now in our country where the most important asset that we have on the cybersecurity challenge out there from a technology and from a skills level is our people. to raise the Cyber IQ of the of the nation as fast as we can because we're sitting in a great position with a very good framework and also motivation by most of the organizations and the CISOs of the major organizations wanting to have the highest cyber IQ that we can of the Nation.

We all know the rankings of Science Technology Engineering Math (STEM), as the United States relates to the world. We have the opportunity as a Nation to become the number one cyber IQ nation in the world. Fundamentally my recommendation is that we look at the assets we have in place with our frameworks, our universities and push that down into organizations all the way back as fast as we can into middle and high schools and raise the Cyber IQ of the United States.

Mike Walker, Program Manager, Information Innovation Office, Defense Advanced Research Projects Agency (DARPA)

We have spent the last three years at the agency building a global challenge program called Cyber Grand Challenge, to explore the possibilities of artificial intelligence (AI) and automation in computer security domain. That challenge concluded about a month ago. I want to talk a little bit about why automation and AI has a potential role to play in the future of unlocking the economic potential of the internet. The commerce and communication today is just the beginning of that potential economic growth. Moving major infrastructure and life safety to the internet emerging industries like connected cars, medical devices, connected homes is going to see even more growth. However, with the potential for growth comes the potential for lack of confidence. A couple in Cincinnati, OH were awakened in 2014 to the voice of a stranger from the internet shouting at their baby over the baby monitor they had purchased, that was a connected device.

I'd like everyone to think about what testing should come with that device, what kind of information, what kind of testing, what acknowledgement of vulnerabilities, should have come with that device. Baby monitors are just the beginning of this problem. We hear many messages we need to build stronger software systems. Strength has to be built in, and part of the design. Right now, how to build stronger software is an open research question. Many brilliant people are working on how to build stronger software tools and better software systems.

Instruction should always be guided by an ability to measure how weak the end result is. Structural safety in the software domain happens in the presence of an intelligent adversary. In the same way that NIST has studied fire science for decades and has studied how spark becomes flame, how a flame moves through buildings, and how buildings burn down. It has made a catalog of building codes that reflect all of this institutional knowledge about how buildings fail. We need to know how software fails. Our adversary is not fire, but the human mind in most cases. The

human mind is getting constant adversarial pressure against software that guards data. In the future, it's going to be exerting adversarial pressure against software that guards life safety, enterprises and infrastructure.

The problem with understanding adversarial pressure against software is the kind of testing is incredibly expensive. It requires experts and few of those experts possess the skills to audit code at a very high level. None possess the endurance, scale, or speed to be able to audit millions of lines of code, which is the size of most major software projects. We need to be able to do constant code monitoring on the networks that run our civilization.

Emerging automation techniques have the ability to transform the economics of being able to understand the weakness of software. A system called Mayhem, developed at Carnegie Mellon University, was able to automatically find and prove the existence of 13000 flaws in the Linux operating system. A system named Sage, which operates at Microsoft, is constantly looking for new flaws in Microsoft code during its development, and removing them before it is ever released to consumers. At Google, enormous amounts of compute power are put into automated systems that search the Chrome browser for weaknesses and remove it before it ever shipped to consumers.

A month-and-a-half ago at the Cyber Grand Challenge final event, we asked the question, what if we gave the entire security lifecycle to automated systems. We did so within a very simplified context. I will tell you a story from our results. In the space of 15 minutes, one autonomous system completely disconnected from any operator or person was able to discover a new flaw, never before seen by person or machine. There was unknown binary code that the system just examined for the first time. It was able to figure out how to attack another system across the network and it did so. It took data. The other system detected the breach, and diagnosed the flaw. I was able to feel the patch that shut that flaw down.

We have the word "zero day" to describe flaws that are unknown. The term describes its place on a timeline of days. This occurred in the space of fifteen minutes. It is a completely revolutionary time scale for dealing with the knowledge of vulnerability in software. Machines that can discover software vulnerability at machine scale and become the foundation for measuring vulnerability of code. They can upend the economics of measuring vulnerability of code, and make it so that we do not require expert red teams to constantly scour code.

We can democratize it. We can make it something that is available to the entire community that is developing devices for the internet of things. and that automation can also be the foundation for not just measuring how strong software is during its development process but also for inspection, for rating for quantification of weakness, and potentially pricing risk and potentially pricing risk and understanding what it cost to insure software. I think that it is it is critical that we actually be able to quantify weakness in software, not just say we need stronger systems but how much stronger they need to be before we can hand over control of life safety applications to software.

Neal L. Ziring, Technical Director, Capabilities Directorate, National Security Agency (NSA)

I have to note that my remarks don't represent an official position of NSA. They're my views as a technical leader coming from that environment. with the topic of this panel being growing and

securing the digital economy, the primary point I'd like to make is that growing that economy can only be achieved by sustaining, building up, and improving all of the stakeholders' confidence in the underpinnings of that economy. In other words, a confidence in cyberspace. There are a lot of key stakeholders to consider. We know what they are. They're all working towards this common purpose. I think the question we should consider here today is how can we enable and promote further that purpose .and so you have my prepared statement.

I'm just going to try to hit some of the highlights. I won't spend a lot of time on current state of cybersecurity. We all know it has a lot of problems. There are just a couple of highlights I'd like to hit first. Security is not consistent, and while our security has gotten a lot better, if you're going from 80% of your systems being secure to 99 percent of them being secure, you haven't really given attackers a much harder problem. They find that 1%, they get in and then move laterally etcetera.

A lot of systems are getting better. Tradecraft for securing systems is getting better many cases. As Mike just said and I agree there are areas were that's not the case today. It is the case particularly in cyber-physical systems, internet of things, where we're embarking on a path that incurs a great deal of risk by giving systems with demonstrably and published paper established poor safety and control of life safety, industrial, medical, etc. systems.

The next point is the trust relationships are everywhere. No matter how good a system is at protecting itself, a super secure individual component is never enough because it has to trust other things around it to which it's connected. Then we'll get back to that in a bit. The last high point I'd like to make is today defense with in cyberspace is largely an individual activity. Each a cyberspace user be it a consumer, an organization, a government agency, etc.

This came up a bit this morning is in some sense on their own. They're mostly on their own in securing their own systems and defending them. That's very serious problem.

I'm going to get to some recommendations again just highlights. First, in hardening and hygiene, I think it's hard work, but we have to raise the bar on a lot of software systems. A lot of companies are already engaged in doing this. There is wonderful research going on in this space, as we just heard about. There needs to be better and incentivization to actually apply that stuff. In many cases that can be government helping that by collaborating with industry and in various contexts to set what does it mean for this type of device to be secure enough. What's that floor that all the devices of that type should reach? We've had some very good luck at NSA collaborating with companies in establishing those and publishing those.

Two other areas that I think are especially important: the first one is identity and credential protection. This applies to all sorts of organizations and individual consumers. Online providers of identity have to provide a certain foundational level of service in terms of identity proofing, compromise recovery, fraud detection, etc. this is another area where government and industry could collaborate to set with that floor should be. then government could say we will accept that and act as a driver for bringing services that provide this up to that sort of foundational level.

Next there's certain key infrastructure is in the internet that are critical to overall confidence. I believe the most critical one is the domain name service. That's an area where it's consistently

abused by threat actors. Methods for improving it and improving security for those who consume it as a service are fairly well understood. If we could establish that a large-scale probably through some kind of industry partnership that would have a huge impact.

Next shared defense hardening can never be perfect. Compromises will always occur at some point. Possibly trust relationships I mentioned earlier and we have to be prepared to defend systems against attack. Fundamentally we need to get out of the mode of every man and organization for himself in a sense and get into a mode where defense is a shared, cooperative activity because it scales better that way. Fundamentally today, attackers get to leverage an investment in an exploit or a piece of malware over and over again in attacking lots of victims. We see that certainly happening with ransomware today, just to pick one example.

Several things can help. First, essential but not sufficient, but essential is broad information sharing both industry to industry, industry to government. There's some standards in that space that are excellent. They could be more broadly applied such as Styx, for example. Second, we need a more robust and instrumented network infrastructure. This is primarily going to fall to the network operators, become the common carriers. There's a lot of potential for collaboration there as well. A certain core infrastructure such as signaling System 7 and Border Gateway protocol BGP, the technologies for securing those are known and understood and they're not getting applied in a consistent, universal, basis especially at the seams between network providers.

Third, we need to build mechanisms for timely automated coordinated defense on a national level. If we truly believe that the defense of our cyberspace on which our digital economy depends is a national problem. We need to have mechanisms that allow us to take a national level action and in time frames that are enough to actually prevented an event from having a significant negative impact. International partnering is going to be essential. Cyberspace is fundamentally global.

Trust relationships between U.S. consumers, firms and government agencies span the globe so cooperating with our partners both in a bilateral and a large treaty group contacts is going to be very important. There's great work going on in establishment of international norms from the State Department and various private groups. We need to continue to support that. Next, true coordinated defense at a multinational level should be supported. There's no reason why we couldn't have the U.S. and its close allies take coordinated measures against the sizable cyber-attack, in other words, pool our visibility, work together and understand what threat actors are doing.

This is already taking place in defense intelligence arenas. I see that firsthand from NSA. But it needs to go beyond those limited arenas to a broader government. Last, preparing for the long term. This overlaps a little bit with what some of the other panelists said about education. The U.S. is actually number one in this space right now, but we can't rest on our laurels. We have a lot of universities that teach cybersecurity, both at the two-year bachelors and up to the Ph.D.-level. We could be doing even more there in building up that capacity, and in particular encouraging students to go into that both directly and indirectly.

The NSF scholarship for service cyber corps program has been tremendously successful at the size it is, but if many kids are really interested, it could be a lot bigger. Finally, on that aspect, certainly extending down the secondary school level is important as well. But let's talk about the top end a

moment. To truly have a vibrant economy in this space and a long-term protection of our internet and our cyberspace we need to have a strong R&D sector as well. There are companies active in this space, there are universities active in this space DARPA and NSF. We are in pretty good shape there. The missing link is technology transfer. I am the head reviewer for the centers of academic excellence in cybersecurity information-assurance research. I see a lot of the research that our universities are creating. However, very little of it makes it into use and that is an area word for a tech transfer could be a lot stronger.

Panel 2 Discussion

Commissioners of the Commission on Enhancing Cybersecurity

Mr. Chabinsky: *[To Mr. Ziring]* You mention common carriers, and I think we need to move problem away from consumers to common carriers. If we put the money currently used by the private sector toward paying the common carriers, how much of this problem can be taken care of at the technical layer?

Mr. Ziring: Substantial slices of the problem can be addressed. There are areas in which consumers and small businesses are regularly being compromised today that, if they would take advantage of the things you suggest, many of those compromises could be taken off the table, going from "common" to "very rare." That would allow us to focus on awareness campaigns and product improvements into areas that will have a better effect. The notion that I might be beaconing-out to a weird DNS name from an infected computer in a small business, a consumer can't defend against that. They don't have the resources to do that. That service should be provided them by private sector companies privy to information-sharing along with possessing government resources.

Mr. Lin: *[To Mr. Walker]* You described automated patching. Do you have any sense for what fraction of the security flaws were found? Are you talking 10 percent, are you talking 90 percent?

Mr. Walker: One of the things about counting vulnerabilities is that you can only speak to the percentage you know about. My most recent data point is still from qualifiers as of June, 2015. Of the binary code we released, machines were able to prove a flaw existed in 79 percent of 131 samples. There are two axes you want to measure against.

One is: can machines find everything detectable by experts? If we put our best automated system up against our best experts in competition, the winner continues to be the experts. Cybersecurity has not yet reached the "Deep Blue" moment (referring to a chess competition in which an automated system – Deep Blue – won against a human). But that is certainly our goal.

The other is scale. While automated systems are not yet as good as experts, their ability to scale is enormous. So finding 13,000 flaws in Linux is an accomplishment achievable only by a computer. So, it's the scale and speed properties that we're after. And the expertise is what we continue to strive for in research.

Mr. Lin: In the Commission, we talk a lot about information sharing. The vision that I would like to imagine is automated information sharing about cyber threats and automated feeding into patch systems. I was wondering if you've given any thought into integrating those two efforts.

Mr. Walker: Information sharing is usually about established threats. So, regarding malicious

software, the automation we've worked on was about flaws in software. So, the information we deduced was a little different. The best use for vulnerability information is during the development process and to be able to remove it before the software is released, and then in a constant monitoring role, so that, as a system learns more about breaking software, it can instantly alert and instantly fix.

Finally, if you're still up against an adversary who knows about a flaw unknown to you, the system can engage in a monitoring role. But when information sharing is practiced today, it is usually around families of malware and the actions of threat actors on the network. All of which takes place after software has been broken.

Right now, when you purchase an IoT device, there is no label on the back disclosing that the device has been audited and which lists the discovered flaws, so the way I like to think about a future role of automation which can measure software weaknesses, is in a monitoring capacity.

Mr. Lin: *[To Mr. Davidson]* In your presentation, you discussed baking-in security at the start. Do you have any ideas as to incentivizing baking-in security at the start?

Mr. Davidson: There are a couple of components to it, one being awareness. For large companies, that isn't a problem. In an environment in which we've got hundreds of thousands of app developers education, it is critical to ensure that they have the tools they need.

The other component is incentivizing people to share information with government. As it is, many companies are still leery of interacting with government or accepting help from the Government.

We also need to think about establishing educating companies about the consequences of acting unwisely. We are encouraged that the Federal Trade Commission has embraced many risk-based approaches enunciated in the CS Framework. This, too, will be part of the solution.

Ms. Murren: *[to Mr. Walker]* To expand on what you were talking about regarding consumer labeling, I know there's been a lot of discussion about putting labels on devices to indicate how secure the device is. There's also been discussion about crafting regulatory legislation in that area.

Could you talk about the "how" of labeling? I ask because, when getting into the weeds, the discussion breaks down as to how labeling would be accomplished. For example, should labeling be done by the manufacturer or could it be done on a more universal level? And, related to that, who would be the body who would create those standards?

Mr. Walker: Speaking on my own behalf, where to assign the role is out of my scope as a technologist, but I would like to speak to the "how."

At DefCon last month, Mudge spoke about how to create a nutrition content label for software. Rather than base it on a rating scale, it's simply a list of what's inside, the choice of whether or not to use the device would be your own.

There is a lot of established best practices on how to armor code against intrusion – everything from stacked cookies to library randomization. There exist many well-known ways to make software much more expensive to attack, and we already have the mechanism to implement "nutrition" labeling for software.

The automation which searches for new vulnerabilities and to lists them is more of a future technology. It will take more engineering effort to build into a conformative label.

I would like to talk a little about software which is secure by design. DARPA builds a project known as "Hack 'em" to formally verify, though mathematical proofs that no vulnerabilities existed within small amounts of code of approximately 50,000 lines. This is important because, though 50,000 lines of code is not enough to run your desktop computer, it *is* enough to run pacemakers and automobiles.

As it is, we cannot presently distinguish between code with no vulnerabilities and code riddle with them. Through automated verification, we will be able to make much more informed decisions. So the "how" to implement automation which can address vulnerabilities in code requires a research and engineering association to apply automation to the market sector.

Mr. Ziring: Some of the fundamental security properties of some of our software systems could be viewed in a much cheaper "black box" manner. It wouldn't be as good as a "white box," but it would get us something. And that kind of testing can also be automated. If you look at the mobile app eco-system today, several research papers attest to the fact that many egregious vulnerabilities which are simple enough so they can be addressed in an automated way. This might be enough to establish a baseline below which a device would not be ready to secure personal data. It might contain simple instructions like "don't disseminate PII in the clear." This might constitute one of the lines on a "nutrition" label.

Mr. Walker: I agree that this would be a great first step.

Mr. Geritz: I also agree that getting at the low hanging fruit should be exploited.

Mr. Davidson: The "nutrition" label is truly worth pursuing. We should also focus on auditing our software in order to earn and keep consumer trust.

Mr. Lee: *[To Mr. Walker]* There is the potential to up-end the economics of cyber-attacks. If there were widespread deployment of automated vulnerability testing, and possibly a certain amount of automated patching, what would that look like from the perspective of a hacker or cyber-criminal?

Mr. Walker: It is incredibly cheap to break into incredibly expensive software. At the annual Pwn2Own Contest, in which a $200,000 prize was offered to anyone who could hack any of four fully-patched browsers. No browser survived a hack attack. We've found that, absent information sharing, flaws last approximately 300 days. As of 2010, it takes vendors an average of 24 days to patch a system. Our goal, in automating threat detection and remediation, is to make the $200,000 expense a one-time use, making attacks enormously expensive.

Mr. Lee: I think we have to assume that the hacker has access to the same technology. Do attackers have that automated technology, and would your economic argument hold up in that world?

Mr. Walker: The democratization of the technology favors the status quo. The technology that hacked the browsers at Pwn20Wn, is now available, as The Mechanical Phish, as open source technology.

Mr. Lee [*To Mr. Ziring*]: I found your discussion trust relationships very interesting. We've thought a lot about one particular topic area is the prospect of billions of devices connected to the IoT. What

do we know about the manageability of trust relationships in light of this potential growth?

Mr. Ziring: We have to be able to issue short-lived and inexpensive identities and associate them with short, inexpensive attributes in contrast to having to issue ten different identities to do ten tasks, you should issue one identity with the attributes allowing the user to do those tasks. This will necessitate the need for an attribute infrastructure which is significantly simpler than an identity infrastructure. I envision our moving away from a preponderance of identities to a proliferation of attributes. In my opinion, that's the only way we can scale to anticipate the growth in IoT devices.

Mr. Lee to Mr. Ziring: Are there any market forces to drive us to that future?

Mr. Ziring: There is no market disincentive to set up independent identity structures which may or may not be especially secure. We really need a set of core requirements defining a secure identity infrastructure. In that space, the U.S. Government can lead by example, then incentivize those who comply, which will help consolidate the market.

Ms. Wilderotter: Regarding education for consumers and the public, is there a way to implement an automated service which consumers can contact regarding any type of hardware or software to determine if the device meets a certain set of standards? It might be set up as a search engine, similar to Siri or the one used by Microsoft in order to access information related to a specific device. And, if that is possible, where would that fit in the Government?

Mr. Ziring: A microcosm of what you're referring to is that the Government, under the National Information Assurance Partnership (NIAP), uses the Common Criteria Evaluation and Validation System (CCEVS). It serves as a viable model to identify which testing the software or device has passed. I don't see any obstacle to scale-up that idea.

I would guess that the effort would be done by private industry with governmental oversight.

Ms. Wilderotter: Who currently uses that service?

Mr. Ziring: Federal agencies purchasing security-enabled IT.

Ms. Wilderotter: Is it voluntary?

Mr. Ziring: No. They are mandated to use it.

Ms. Wilderotter: Do any of you have any ideas on how the public can build trust in hardware and software products?

Mr. Davidson: At present, I don't think it exists. It is very difficult and is so for very good reasons, one of which is that the Government has avoided a "one size fits all" approach to CS, and something we would like to avoid at all costs. As a user of Government systems, I'm not sure I would want to impose similar restrictions on the general public. I say that not in a pejorative sense but the fact is that we are slow, and I don't think that's what private industry needs. I think we want to continue to have decentralized mechanized systems.

What the Government can contribute is to craft and incentivize best practices, where none currently exist, to address things like IoT field upgrades.

Mr. Sullivan: We on the Commission would like to see automated testing, scorecards, and a government agency crafting best practices. What government agency should be doing these things?

As it is, it seems some government agencies are on defense and some playing cleanup. The FTC will reach out to companies not doing well enough. The FBI and DHS will go after the bad guys. But who is going to help build the highway on which all of us will travel? And whose mandate is that?

Mr. Davidson: At present, it is unclear, and that is an area in which the Commission might be able to offer us guidance. It's also an issue above my pay grade.

I suggest that there are different roles for different agencies, but, overall, we have to work on building trust and simplifying public access to information across the Government.

Mr. Walker: I would like to add some evidence. As software assumes new roles in our civilization, the problem of software security is bubbling up to different agencies.

As an example, if you look at the connected car the problems related to control systems that impacts agencies responsible for vehicle safety like the Department of Transportation.

This same dynamic is also impacting agencies responsible for certifying implant devices.

What is interesting is that the code that controls vehicles and implant devices has much in common. Both are very localized, and have a clearly-defined job to perform.

It might be that a non-profit, private organization, like the cybersecurity testing lab, would be in a position to advise the Government in addressing these issues.

Mr. Ziring: Using the Government authority to leverage knowledge in the private sector is very powerful. The expertise to secure each of these apps exists. The model of a sector agency for CI could serve here as well.

Mr. Geritz Who do you think is more motivated: government or private industry?

Mr. Sullivan: I know that when I go to work each day, I'm not counting on anyone else to defend my company.

Mr. Davidson: We don't have a Department of the Internet, but we do need centers of excellence as well as integration and leadership in order to get qualified people into the Government. Creating centers of excellence will be an important component to attract good people.

Mr. Sullivan: Should some declare code to be critical infrastructure? We would love to see the Government addressing code in the same way Linux approached the challenge.

Mr. Davidson: We're seeing companies avoiding being classified as CI because of the regulatory over structure.

Mr. Sullivan: I don't suggest labeling companies as CI

Mr. Gallagher: I think that we are pitting experts and policies against an environment which changes at unprecedented speed. To me, that lies at the core of our frustration, not a lack of enthusiasm to address the problem. So my question would be, is *any* policy construct capable of generating a collective defense posture to address this imbalance at network speed?

Mr. Gallagher [*To Mr. Ziring*]: You were talking about the vulnerabilities in the trust infrastructure and I think you mentioned DNS. One of the things we've heard in previous testimony is whether or not this should be a distributed system and whether technologies like blockchain might be relevant.

Mr. Ziring: I don't think we need things like distributed ledgers and blockchains to secure the foundational infrastructure we depend on. The technologies are proven. They just need to be applied more universally.

My reason for using DNS as an example is that there are a number of standards waiting in the wings which could be powerful enablers for other facets of the digital economy that we can't yet take advantage of because DNS is not yet solvent enough to host them. One example allows you to tag a domain in DNS with the associated private key certificate so that when you visit there, you can be sure you went to the right place. That can be tremendously enabling for business on the internet because it could eliminate the problem of a certificate being spoofed.

Ms. Anton: We keep hearing about consumer concerns about online privacy. According to a RAND report, about 25 percent of the population has received a breach letter. But it seems that consumers prefer convenience over concerns for their privacy.

What is needed for the consumer to be motivated to the extent of changing their online behavior?

Mr. Davidson: Consumers see great value from services and don't feel harm. We may need to heighten awareness of actual or potential harm. The opportunity to do this would center on a breach having taken place, such as an attack on vehicle security. Though we would prefer these events *not* taking place, they do represent teachable moments.

Mr. Geritz: Currently, credit card companies and banks play a shielding role. They have done a great job shielding consumers. Right now there is trust, it is a testament to those people.

Mr. Davidson: One issue largely neglected is "what do we provide the consumer as a glide path? We have responsibilities to help people with better pathways to action.

Mr. Walker: It's easy to do something bad on the internet. It increases exposure to threats. I would like to see a day when a computer would be designed in such a way that the consumer could click where they want, with bad choices made unavailable.

Mr. Ziring: Today, the burden is on education. Even with my experience in the NSA, I am still uncertain about some of the security risks on my home PC. If the information was made more evident to consumers, it wouldn't require as much education.

Mr. Donilon: You've identified two problems. One is we have persistent and unacceptable levels of flaws in software. We have the resources through research and development to address this more cheaply, efficiently, and effectively through automation. So it seems to me that that would be a major research priority for the Government as well as for the private sector.

Secondly, we should have agreement on which core software flaws should be avoided, and list them on a label as already suggested.

Mr. Banga: We should do the work to protect the weakest link, whether the individual consumer or the small business. We can implement system security without forcing them to become nerds.

Mr. Walker: Any attempt to standardize what is or is not a threat is pitted against a bar that is constantly moving. This brings up something which hasn't yet been discussed, and that is bug bounties: If a vendor offers a prize for demonstration of a flaw in their software, and that prize is

very low, they end up writing many checks. But if the prize is substantial, they write fewer checks or none when the prize is unclaimed.

Bug bounties are enormously widespread in the private sector and beginning to surface in the public sector. The advantage of these is that it provides the chance to compare the effort to prevent a breach against the effort required for an attack.

Mr. Lee: These same tools are used by hackers as quality assurance checks on their own exploits.

Mr. Ziring: That is why automatic patching is so important.

Mr. Donilon: Regarding the IoT, we have been told that this is a looming problem without an obvious market incentive to solve it. But it's a health and safety issue. This should spur the establishment of minimum standards required on such devices.

Mr. Palmisano: Why would you not follow the model of penalties which already exist in the physical world, such as policies and notification regulations governing consumer electronics? Why would this not be applied to specifically dangerous elements of the IoT such as healthcare or automobile control?

Mr. Davidson: I don't believe the barn door is already open. And I think you will see increased sectorial regulation.

Panel 3: Embracing Innovation in the Government and Preparing for the Future

Dr. Evan Cooke, Senior Policy Advisor, Office of Science and Technology Policy, The White House
Tom Donahue, Research Director, Cyber Threat Intelligence Integration Center
Eric Mill, Senior Advisor on Technology, Technology Transformation Service, U.S. General Services Administration (GSA)
Mark Ryland, Chief Solutions Architect, World Wide Public Sector Team, Amazon Web Services (AWS)

Dr. Evan Cooke, Senior Policy Advisor, Office of Science and Technology Policy, The White House

The background we will discuss today will be on U.S. Digital Service (USDS) which hopefully will provide useful lessons and examples for your deliberations. On August 11, 2014, the President directed his administration to create the U.S. Digital Service, or USDS. This continued the work the President and his administration had already done to support innovation and technology transformation, including creating three new high-level positions in the White House; the U.S. Chief Information Officer, U.S. Technology Officer, and the Chief Data Scientist. over the past two years. More than 170 Engineers, designers, data scientists, and product managers have answered the President's call and signed up for a tour of duty with USDS.

I was one of those engineers that dropped everything, moved across the country, and joined up. This team has delivered more than twenty projects and initiatives including making it easier for veterans to access health care, helping students, parents, and families make more informed decisions about college selection, to the college scorecard, strengthening information security at the Department of Defense (DOD).

The Defense Digital Service Team, as we heard in the last panel, launched a program called hack the Pentagon. The first bug bounty program in the history of the Federal Government to

strengthen the security of DOD's digital assets. More than 1,400 outside researchers participated, and more than 250 submitted at least one vulnerability report with reports going to a team for remediation in near real time. The U.S. Digital Service was created based on a simple theory of change. Bring top technical talent into public service and deploy small empowered teams that partner with career civil servants and agency leadership to solve high priority problems. USDS is organized as a federated set of connected but autonomous agency teams that work hand-in-hand with agency senior leadership. The concept of operations is best illustrated by the USDS core values.

Number one, hire and empower great people. Number two, go where the work is. Number three find the truth and tell the truth. Number four, design with users not for them. Number 5 optimize for results not Optics and number 6 create momentum. Together these values define a culture of delivery. Change is accomplished by focusing first on results that improve the lives of citizens and customers. This model has been successful improving citizen facing services, a challenge that has several parallels to the problem of improving Federal cybersecurity. I share the following few thoughts as an implementer who has worked on U.S. digital service delivery teams and from a policy perspective in my current role in the Office of Science and Technology Policy.

Cyber-security as we know has an inherently technical basis and we won't as a government have a full understanding of the issues we face or the available solutions unless we bring the technical experience and understanding to our most senior discussions. We've observed time and time again the organizations cannot manage their way out of bad technical architectures. We need technologists at the table. one way in which USPS seeks to address this problem is by ensuring the position description for job openings even for senior roles require a certain level of Technical and operational experience. There may be an opportunity to increase the rate at which this transformation is happening. The USDS model of bringing technical talent to do tours of duty and Federal Government may also be a helpful tool in tackling important cyber security challenges.

A few key features of the USDS model are: the opportunity to work directly with senior agency leadership on critically important problems, the mandate to make difficult decisions that may challenge the status quo; and the autonomy to build and maintain a unique culture with leadership that is Technical and has private sector operational experience. These can be difficult requirements to realize but they have proven important components of success. In addition to the engagement model and organizational structure our work on Projects is also surfaced experiences that may be helpful points to the Commission.

First, many policies and processes design with good intentions to improve cybersecurity in past years do not necessarily the envisioned security outcomes. for example, rules put in place the strengthen the process of obtaining an authority to operate or ATO can sometimes lead to inconsistent security outcomes, longer view timelines and significant of duplication of effort across and even within agencies. Another example is Federal guidance to departments and agencies on trusted internet connections, a policy that was originally put in place before the wide adoption of cloud and mobile technologies. It could be modernized to support new more secure tool. as we consider a more agile Federal policy framework for cybersecurity, our experiences suggest that policy for cyber security should be tied to measurable results where possible and designed with Evolution built-in or Sunset as technology matures.

Second, our work has demonstrated how difficult it is for a highly federated system to consistently implement a large number of complex changes quickly. Consolidation of critical common Federal services and platforms such as email and productivity applications will help provide the visibility and control necessary to provision the Federal Government for the more automated world of advanced machine learning in artificial intelligence and defend against the next generation of threats. A small team responsible for all Federal cybersecurity oversight, that can deliver memos but not services, is a difficult way to ensure consistent outcomes across the Federal Government, the USDS has shown us one model for

Change and innovation and also demonstrated an important point: how change can be achieved could be just as important as the question of what needs to be changed. In an organization as large and complex as a Federal Government. There is no simple answer, but empowering those who are close to the problem and understand the technology will get you a long way.

Eric Mill, Senior Advisor on Technology, Technology Transformation Service, U.S. General Services Administration (GSA)

I am more recently the last few years have gotten into a lot of information security policy and practice so 18F has a deep investment in the cloud and hosted applications in the cloud for us and for other agencies. We are hiring information security practitioners and been trying to do that the right. We are working on standing up a bug Bounty and vulnerability disclosure program that we put in a special amount of effort on https and TLS encryption. I really try to help make the U.S. Government's public web service secure and encrypted by default. Hiring technologists and security practitioners is not enough. They need to be elevated in an organization. They need to be given autonomy, but they also really need to be involved in the strategy of the agency and the policy of the agency in a way that's not often contemplated.

Agencies are very accustomed to relying on legal staff as an example for more than just a really straightforward legal analysis. Legal offices for agencies are brought into the strategy and policy efforts of that agency. Technologists need to set direction for the agency from a technical level and not necessarily be weighed down with supervisory responsibilities. You do want your supervisors to have these technical abilities, but you also want to make sure that your senior practitioners who are given authority to direct the posture of your agency, of your office. Their job is to do that work directly. This is not something that comes naturally to a lot of agency org charts.

In the Commission's work, encouraging those sorts of changes in the Federal Government, having technologists involved would be a positive fit with the technologist positions being hired at 18F It is also important to disintermediate, to the greatest extent possible the technology grand truth as experienced by practitioners in the field with policy and oversight bodies. It is not something that comes naturally to the Federal Government.

It includes legislative interaction you shouldn't always just have the only direct interactions between technical practitioners and legislative oversights that happens in back channels. That should be something that happens in a regular safe way. A little bit information sharing this information sharing. Broadly speaking, in security is not something that the Federal Government does naturally across agencies. In particular, I want to talk about the value of public information

sharing of security relevant policies documentation software. This is especially important because there is no better way to disseminate information throughout the Federal Government and throughout all its agencies to its staff then publication for public release. It takes more than a kind of command control dissemination of information to actually reach the people and agencies. This is always a concern very much conferences that is the community as quickly as possible.

The private sector is not always fully open, but there is sharing over best practices and security failures. There are conferences, blogs, and interactions. That is the life blood of a technical community. It spreads best practices quickly. It is something that needs to change in the Federal Government. Lastly, I'd talk about avoiding unnecessary centralization and avoiding a focus on the perimeter.

There is a tremendous pressure on the Federal Government to focus on centralizing computing resources, centralizing networks, and to rely on the idea of a trusted network. This is this is really a stark conflict with modern technology and security trends. At the most basic level, everybody is moving to the cloud and for lots of really good reasons. They move into the cloud to use computing resources that are not in the direct control of the agency. That's all the cloud is, somebody else's computer.

There are lots of other benefits that come with the cloud computing and information. The conflict arises because the cloud involves having agency controlled information go into someone else's control. Privileged separation is the trend in the computing world. The Commission should focus on removing policy pressures, and removing pressures that force agencies to unnecessarily centralize their infrastructure and to rely on logical controls rather than physical controls. Logical controls mean software, rather than physical separation to the greatest extent possible.

Tom Donahue, Research Director, Cyber Threat Intelligence Integration Center

I'm from the Cyber Threat Intelligence Integration Center. I'm speaking to you informed by a Federal career of 31 years and I've come to this conversation with a threat and a targeting perspective of an engineer and an intelligence officer. I also spent four years at the White House working with other people such as Mr. Donilon, while working on the National Security Council staff. I participated in the cyberspace policy review. However, there's a lot of this conversation that I think I've heard before. It's not a bad thing. There's some good ideas that are worth bringing up, but I wish you luck in finding a breakthrough.

I am speaking from my personal views. I'm not representing any particular organization. I have two simple premises in this conversation. Number one, that the question before you should not just be, how we secure networks, but should also include how we manage risk in business processes. In my observation, most of the truly catastrophic failures have been root cause failures of business organization and business process.

I will also say that only targeting point of view when I'm looking at something, that's where I start. I do not start with technical flaws. I start with organizational flaws. For a nation-state, there is no economy or economic calculation, it's a national security calculation. I think there's two different problem sets that need to be considered. One is the consumer problem. However, there's a national problem and it's a very different problem with very different calculations. Looking at the

Federal Government in particular, I would note that we are essentially trying to secure industrial age business processes in environments of concentration and global connectivity that essentially increase risk by nine orders of magnitude.

This is not a matter of semantics as it shifts responsibility from the engineers to include the business process owners, who must be accountable for the choices they made. I can think of some specific instances where business process choices were made that had personal effects on me as an intelligence officer. I've gotten those letters, along with 22 million other people. It also influences the question you want to address of who is in charge.

I would also note that when we look at organizations, nation-states don't depend on flaws. Eliminating flaws is an essential condition but not sufficient. As an example, in the case of a flaw in a car, I would not go after the car, I would go after the car dealer. I don't think I need to describe it any further. We must redesign our business processes that take into account well-established security principles that have been understood certainly in some parts of the financial sector for literally thousands of years. If you'd like, I'm happy to explore that issue from thousands of years ago. Essentially, about 25 years ago we actually walked away from those principles as we applied the internet.

This issue that has raised about centralization and decentralization is not answered by those principles. In fact, I think part of one of the principles have to looked at is how can we manage, how can we shift from someplace where it cannot be managed to someplace where it can be managed. Then examine the new risks that have come on board in the process of doing so and mitigating those risks. The question to ask at the end is, is the business process better now? Has the totality of the risk been mitigated, and if in fact progress has been made? I would submit that by doing so the problem can be narrowed. It is purely the technical cybersecurity risk. I would also submit the notion of perfecting the infinite complexity of all software does not solve the problem, even assuming we can get there.

What is the way ahead? The second idea is that research and development in the Federal Government has always been essentially a lot of stapling interesting ideas together and filing it under various categories in what is purported to be a strategy. What we really need is a unified purpose. The different elements must come together, and work on helping solve the problem at least for the Federal Government. Perhaps it would have also some use to the private sector.

My experience at the White House also goes back to the comprehensive national cybersecurity initiative. We have spoken to this issue previously. I would say we have not succeeded. I would also note that we are heavily burdened by legacy investments in technology and legacy investments in business processes. We're going to spend money changing that anyway. The question becomes, is there a smart way forward, that as we go forward we will mentally move into a smarter and smarter space. In other words, we need a road map for how we will move from the current place to a much better place, and allow ourselves the time to do that and to make the investment. First, we need to have that underlying philosophy that will guide the decisions that we will make going through that process.

Mark Ryland, Chief Solutions Architect, World Wide Public Sector Team, Amazon Web Services (AWS)

The theme is about embracing IT innovation in government in order to gain many of the benefits we have been talking about with cyber security. I want to be clear that although I'm going to use Amazon examples as AWS is a leader in this industry, the examples apply more broadly. I'm really talking about a paradigm shift. In terms of how IT services are prepared and utilized, it's much broader than our company. It does represent the next large phase shift in IT, and also the theme of automation which is been here very present throughout this afternoon as a big theme about what I call true clouds.

One of the issues to be faced is that the industry has this phenomenon called cloud-washing, which is taking an existing product just put the word "cloud" on it because it helps sales. What I'm talking about are large-scale highly automated systems, so large in scale, that they must be automated. You cannot manage and run a system at the scale that the large-scale providers such as our company, Microsoft and others run at unless it's built from the beginning as a highly automated environment.

Starting 10 years ago, AWS began offering access to our cloud-based infrastructure based on our expertise, highly skilled infrastructure, and service oriented architectures. Now it's a decade later, a vast range of organizations from the small startups to large enterprises and of course, government agencies are taking advantage of this flexible, secure, powerful, and highly efficient way of accessing IT resources.

Before the cloud, business and government agencies spent a lot of time and money managing their own data centers and colocation facilities. It meant time not spent on their core organizational missions providing products and services including citizen services to customers and citizens. With cloud, organizations like government agencies can now function more like startups that move at the speed of ideas without upfront costs or worrying about new future capacity needs. Today, AWS has more than a million active customers in 190 countries including thousands of government agencies, educational institutions, and every kind of industry you can imagine. These include companies like Shell Oil, BP, Johnson & Johnson, Pfizer Merck, and Bristol-Myers Squibb. These are highly regulated industries making very dramatic and major shift towards cloud infrastructure.

It's fun to just look around this table when I recognize a lot of partners. For example, CloudStrike is an AWS partner and customer, and Digital Services. Agencies working so effectively to modernize IT in the Government are also very strong users and advocates of cloud technology. We're very happy to have them as customers as well.

In my written testimony, I provide some the examples. In the beginning, there was a certain degree of reluctance to trust these large-scale utility style public clouds. There's no business unless everything customers do in these environments is completely isolated in private. However, we will call them commercial clouds. This is understandable considering that anytime a powerful abstraction appears in the IT industry it takes time for users to understand and become comfortable with it.

Fifty years ago, compilers were considered kind of scary. Think about it. There's code generating the actual code. It's kind of scary when people had been writing assembler for years. Even ten years ago, virtualization was considered very scary and potentially dangerous. It's natural that if

there is something new, and it's not well understood there's a certain reluctance toward it. As customers and IT professionals have learned about these modern large scale cloud technologies, the initial concerns have turned around completely. Now, there's a growing realization that commercial cloud service providers offer fundamental security benefits over traditional IT infrastructure. As U.S. Federal CIO Tony Scott has stated, "I see the big cloud providers in the same way I see a bank. They have the incentives. They have the skills and abilities, and they have the motivation to do a much better job with security than any one company or any one organization can probably do."

I think today the better bet is to get to the cloud as quickly as possible, because you're guaranteed almost to have better security than in any private thing that you do. In my written testimony provide a summary of 7 reasons why the cloud is more secure. I will really focus on just a handful. One is economies of scale. They apply to this issue of security and security through automation. The large scale providers can hire the best in the industry, given some of the toughest challenges and yet at the same time, if we measure the number of security professionals and the ratio of the number of people versus the number serviced under management it's a really good ratio. It's really efficient because the amount of infrastructure they are managing and building tools for is vast.

The next point is that it's not a panacea. Cloud doesn't solve all problems. What it does do, is that it shrinks the surface area that security professionals need to be concerned about from everything from the stack from the concrete up to the application to a much smaller surface area. It is essentially application security and to some extent operating system security. Although with certain types of services that even that's taken care of. The customer still has to do a really good job with their responsibilities, but those responsibilities are narrower. That's a real benefit. It's a real win across the cross the industry.

We talked about using the cloud to secure the cloud. The cloud provides the analytics, data processing, and storage capabilities that allow you to actually process the logs that you may be accumulating today and not even looking at. One of the mild ironies for this space is some of the top security companies in the industry now run in the cloud, and yet their security infrastructure on prim that some of the customers are reluctant to actually go to the cloud with. Companies like Crowdstrike companies like Splunk and many others such as FireEye , they all run in the AWS cloud, but with some of the tooling and the agents and so forth in their sensors are running on trim.

It's an interesting shift. The security is a leading edge of many respects with this major transition. In short, commercial cloud and the accompanying automation and agility that they provide is really an opportunity to enhance system security and privacy. As a former senior government official said recently, I was present at a meeting on cybersecurity threats at the American Enterprise Institute. He said someone asked him, it seems helpless. What do we do? His answer was, cloud gives us a mulligan, a chance to do it over again do and it right.

In sum, we believe the evidence to support the proposition that security should no longer be seen as a barrier to cloud adoption really should be seen as an argument in favor of that. That's why I think it's come up before in the Commission's discussions. It is a very interesting example of the

C2S region, which is a special region that we built for the intelligence community. Again, there were many reasons for that very innovative decision. Perhaps most importantly the customer had the vision to say what does industry do when they want the most powerful, actual and cheap and capable analytic capabilities? We want one of those. So, they put out a contract for one of those. Again, you find a very common theme that when people get into the cloud, they will say this is more secure than my own physical and on premise environments.

In terms of recommendations, we applaud the administration's emphasis on cybersecurity with a specific focus on securing Federal networks and planning for building security into emerging technologies such as the internet of things. We would recommend the cloud-first policy should continue to serve as the foundation for proving Federal Government cyber security posture. Some additional things that can be done to fully realize the goals of the President's Cybersecurity National Action Plan (CNAP): first, the Commission could recognize that the most important step forward in the effort to secure government communications networks and IT systems per CNAP is through effective and long term and lasting technology modernization.

Another big theme of the Commission today in the testimony has been modernization as a theme. I would note in that regard the advent of dev ops as a new way of developing and deploying applications. It is a very relevant and highly important technical change that's going on in the industry, which reflects the themes of the Commission and then the panelists today.

if you talk to someone like Mark Schwartz, who is a CIO of immigration and citizenship services, and part of the Department of Homeland Security, what he'll tell you is his security compliance officials are part of the daily stand-up meetings of his Agile development teams. The code that they run to check for security flaws or issues in the code is part of the dev ops pipeline before the code is ever deployed, and they deploy code on a daily basis, just like a startup would. All that code is being run fully through a very strong security vetting process and of course if they discover any flaws, they can be remedied instantaneously. Things like advanced persistent threats don't exist in these dev ops worlds because the code is replaced constantly as part of the normal way that applications are being deployed and built.

That's a really important theme I think that the Commission should be aware of. As Tony Scott noted here recently, the Federal Government should stop using a "bubble wrap approach" putting fragile security lawyers around inherently insecure legacy systems. in the private sector IT modernization is happening because businesses of all sizes and across all sectors of the economy are moving their applications and work loads into commercial cloud, yet policy, regulatory procurement, and cultural block. A lot of the cultural will still remain to prevent a lot of the movement of Federal workloads to the cloud.

A second recommendation is further emphasis on FITARA. It is designed to empower the agency Chief Information officers to have procurement resources to modernize IT systems and to do that as quickly as possible. Additionally, the Commission should review and perhaps support the passage of the recently-introduced of modernizing government technology in the GT act, which was approved by the House Oversight and Government Reform Committee last week. In the GT act, it provides a mandate for IT modernization through commercial Cloud adoption .and the replacement and retirement of outdated Legacy systems that are vulnerable.

The third recommendation is the importance of FEDRAMP. We talked about labelling and certification. I think the Federal Government has a really good job on this particular topic. There are plenty of standards in this area. The 800-53 is widely recognized around the world as a really good security standards baseline. The question is, will the standards be implemented properly. FEDRAMP assists through the use of third-party auditing organizations and diving very deep into their code and their business processes. Peeking behind every curtain is their job, to generate thousands of pages of evidence and documentation. They actually prove to interested consumers that these large scale cloud providers have actually doing what they say they do. Now with the high FEDRAMP standard, we're able to host even things that are considered very sensitive data. There's a lot going on in this space that is worth recognizing as it is an achievement and perhaps doubling down.

Panel Three Discussion

Commissioners of the Commission on Enhancing National Cybersecurity

Ms. Todt: It's a broad question that ties in the three panels we've had today. It is a broad question looking at R&D. One of the key missions of the Commission is to look at R&D efforts. When we talk about innovation, one of the questions that was referenced in a previous panel is how to incorporate innovation in an R&D effort that balances what industry is doing with the private sector. Many efforts and initiatives have been referenced in the current plan. Are there other key efforts you recommend we enforce?

What are key elements we missed on CNCI and other efforts? Why have they failed and we are still looking at them: And finally, we talk about R&D, we talk about innovation, but in all five of the meetings, we haven't heard anything about mobile security, mobile devices, and what the Government is doing to look at this next frontier of attack. In the previous panel and some of the innovation discussions we've talked about, when we look at the Pegasus attack on IoS, we're not examining that at all from a government perspective. We're looking at how to stay ahead of curve, and that would seem to be a key element.

Mr. Mill: I'm going to speak less from the point of view of agencies, and more from how I see agencies working with or supporting mobile. Currently, the unfortunate answer is it is largely compliance and check-box driven, more than it is an analysis of threats unique to mobile security or any deep understanding of what privacy concerns in mobile security are. There is no single answer for why that is. There is a lack of in-house software engineers that can build these apps directly, and have some political clout within agencies to help set the direction for these types of applications. If application development is being outsourced to a third party, that third party may not have the same clout as someone inside an agency.

Mr. Donahue: In terms of mobile, I want to make the point that different agencies have different risks, and need the flexibility to treat them differently. My government mobile device, is pretty locked down. There is one element that there is a risk on, and that is email. It's been further containerized within the device. It is managed in a centralized way at the enterprise level. I would note as we look at these issues, that the cloud does not necessarily equate to the internet. In fact, we AWS cloud on our infrastructure. It gets to the issue of internet based risk. It is a concentrated

discussion. As we consider separation of roles and capabilities, we cannot have a small number of people with total access to all the information on the cloud. The control system of the cloud becomes the target. We need to be mindful these are not single point solutions, they are tools that we can make full use of and adapt to the entire business risk management view, and understand that risks vary from organization to organization.

Dr. Cooke: First, on innovation I would first point the Commission to a recently released report on the cybersecurity R&D plan. It is an updated version that lays out R&D research specific to cybersecurity. The second point I'd make is about how to think about integrating innovation into policy process. The administration is focused on ensuring that it has the appropriate processes and tools for tech policy making. It includes a group in the white house that includes the tech policy making council and embedding tech leadership directly. One is the Tech Policy Taskforce, and it helped support the federal open source policy as well as an initiative on artificial intelligence. Those are two concrete ways innovation is being integrated directly into policy. I would bring the Commission's attention to the challenges of MFA in mobile devices. One of the forms of authentication across the Government is a PIV card, or HSPD-12 form factor, and plugging a PIV card into an iPhone is a difficult thing to do.

There is good work ongoing on with derived credentials that NIST has been the lead on, looking at how do we take an identity management process with a secure root of trust and propagate that into the mobile ecosystem. That work is still new. It is an important component ensuring an overall strategy that manages risk appropriately in the use of mobile devices across the Federal Government.

Mr. Ryland: On mobile security, what is interesting there is, when people build mobile applications, they start to think of security but not in terms of network perimeters. Phones must reach some end point over the internet. It is a very healthy thing. Customers begin to focus on mobile apps, and makes them think more broadly about API endpoints. It becomes building defense in depths to the point where it doesn't matter if a packet can be delivered to an end point or not, because it doesn't guaranty access to what's inside the system.

When we worked with GSA on the TIC overlay project, which showed how we could meet the requirements of the trusted internet connection compliance standard using cloud technology. The cloud has this massive capacity and ability to reach huge numbers of customers, but if all that data has to be funneled back through some special device on the government side, it defeats a lot of the value and the purpose.

We were able to show with FEDRAMP and TIC requirements that mobile and web applications were well designed. There is a healthy development that comes with focus on mobile. Digital Services, Defense and 18F teams are doing some innovative things. There is an explosion of capabilities when innovative technologies and government get together. Government must push through resistance to new technologies and move to more innovative approaches.

Ms. Wilderotter: This panel is about embracing innovation and thinking about the future. If we think about the context of the different trends you have highlighted, like hiring great people that would deliver results. These are current technologies, which are legacy oriented and centralized. The policies associated with it and the way it's built are really last year's trends. It's not the

direction which we're headed. The cloud is one of the answers because of economies of scale, built in security. Business process and practices and organization is where trouble occurs. For our recommendations, what are two or three things to focus in this area that will help move things forward?

Mr. Donahue: Current research and development lacks critical mass. It's not self-reinforcing. It's too dispersed, and has no effect. It gets to the technology transfer problem. The research gets done outside the context and environment where it will ultimately have to work. The work needs to be organized to move toward one comprehensive goal. Then we need to understand if we have the pieces in place to create a comprehensive solution. It must account for where we are now and look at where we're going. Technology transfer only works if it's built into the R&D program up front.

Dr. Cooke: I would think about your R&D question along two lines: First, how do we get people who do innovations into the organizations that need it. That's one part of the problem. The second part is how to overcome barriers that are in front of them so they can do the work they need to do. I touched on a few ideas in my earlier comments. Perhaps there is a way to bring talent that may not necessarily have joined the Federal Government to solve some high priority security problems. I understand the Commission has discussed the recruiting problem at length. There are some great ideas there.

The second piece is how to overcome the barriers to getting things done. There are two ways to think about that in the Government's context. First is making sure people have the right empowerment to make difficult decisions. Finding a way to give the innovation leaders the way to make important decisions. The second piece is, it may not be leadership, but policy. How do we know we are making good decisions about policies that are on the books, and thinking about how to make policies are evolving in the right way, and making new policies that make sense?
In thinking about the ATO process, digital teams have run into issues. The second is internet policy, which governs how applications connect to the internet.

Mr. Mill: There has been much recent activity to push for more sharing source code in the Government. There is no mandate or pressure in the Government to release code developed for the Government to the public as open source. The value created by the Government is reusable to the greatest extent possible, at least in the Federal context. Agencies should be asked to challenge their assumptions so that they are able to talk about releasing some artifacts publically. The Government needs to focus more on higher level function based system requirements, instead of one specific solution.

There is something crucial today about how the private sector approaches information security. It is really key in the Federal Government, and that's the blameless post mortem. It means staff will be comfortable reporting incidents and agencies should not feel like they are punished for discussing security incidents. It is vital these things are shared. It requires changes in agencies and recommendations to oversight bodies. There are some policies that may be able to make a big difference in driving innovation.

Mr. Ryland: The Commission focuses on IT modernization and best practices, things like cloud. There is the intention to move the Government away from legacy systems. I don't know if there is

some way to encourage agencies to shut down legacy systems. It may be something to consider. The key is nearly ninety percent of spending is spent on maintenance. There is little on modernization. Anything the Commission can do to change that balance in the name of security can only help.

Mr. **Donahue**: Some agencies have statutory requirements to how they do things, so there are obstacles in some areas. Social Security and IRS, the Census bureau handle national statistical information and operate under very severe legislative requirements.

Mr. Lee: *[To Mr. Ryland]* it would be wonderful if Federal agencies moved to the cloud in a big way. It can be a challenge for enterprises to take a mission dependence on a sole source provider such as cloud services. What advice would you give to agency directors who express reluctance in this situation?

Mr. Ryland: There is a great deal of similarity between services. They can make business judgements about what is cost of optimizing the risk of individual providers. There are ways to genericize virtual machine access. Most major providers have ways of automating that. Truly, the bulk of code is not cloud code, it is the application code. The dev ops portion tends to be more cloud specific. The bulk of the application code is not specific to a particular cloud provider. Software can solve these problems. It becomes a business judgement. The technology stacks are generally very simpatico with one another.

Mr. Gallagher: A comment on the question on culture and role of technologists, because it may touch on the discussions of workforce in a way that I had not thought of before. In other fields, there is a process management- centric view, skill management process view. I think we tend to be biased toward process management and procedural controls. From the comments I heard today, I start to think there is no reason to not have both. Some jobs have procedural and skill based activities. What you are pointing out is there are skill based conversations where senior technologists need to play a different role.

That is true, but it has an implication for what we're talking about. Skill is managed with skill. There needs to be a discussion on what is the right skill set for these organizations? I'd be interested in your point of view.

On R&D, the Government's effort has always been biased toward discovery, and looking at new ideas. You are suggesting something quite different, an outcome based R&D agenda. In other words, a moonshot, where we decide doing something and laying out a roadmap. Do you have any thoughts on what that moonshot might be?

Mr. Donahue: It's an organizing principle about the research. It's organized what the Government does as a business. It identifies issues, and tries to understand what we have to accomplish. Part of the problem is that we lack bases for making decisions. There is not a road map to minimizing risk. It would be a research problem in and of itself. We need to identify problem sets and work down by layers. We can then contextualize those discovery ideas into something that will get done on a timeline.

I am advocating going back to basic security principles in terms of our conversations and building them in. It means things like identity and key management, network duties, securely moving data

across domain movement of information. There is a litany of challenges. It means applying modern technology to what needs to be a new business environment. We are using essentially Victorian processes, and adding security later. Cloud is not a security process, but a business process; but it brings the potential to look at security in a different way. That's the mind shift we want.

Mr. Mill: In regards to staffing and technology in a skills based way. Something that is worth understanding is how software development and wielding code is changing. At my organization, we have code being written by the operations staff, by development staff, by management in order to do their job in the most effective way. It is similar to how most organizations use word processing or spreadsheet management. Spreadsheets and word processing are essential to work in an office today. That is how we approach software. It is challenging to environments that are not skill oriented. It looks at things in terms of capabilities instead of formal job titles.

Mr. Alexander: There are a number of profound consequences to that. One is, with procedure based control, there can be proscriptive requirements. It argues for performance based standards, which provide much greater flexibility, but require more skill levels to implement. An interesting question is, does every federal solution require this level of expertise built in, or is it more of a specialty activity. Business innovation will allow a concentration into cloud technology.

Mr. **Donohue**: Part of the issue here, is understanding who owns the risk. There are people who are responsible for activities on behalf of the U.S. Government, and they are responsible for risk. They are informed by many different kinds of expertise. Part of the challenge is identifying the actual risks and benefits and bringing those together. People with the right expertise can make the right choice for the particular situation and possibly take the risk. We must empower someone to make those decisions, and be accountable for those decisions.

Ms. Murren: There are a number of different processes or policies, or cultural norms that inhibit enhancing national cybersecurity. You've spoken of it more generally. I'm wondering if you can identify any that might be low hanging fruit. Can you think of areas where if we eliminated something or made dramatic changes, it might give us more resources, time or money to re-deploy for better use?

Mr. Mill: In terms of recruiting, it won't be a radical theme to note there is pay gap between public and private sectors. Some efforts have been made to change it across the Government, but they're not evenly distributed and not generally evident at the moment.

Ms. Murren: Is a policy change required for more money?

Mr. Mill: Policy and legal changes may be needed. Another area is security clearances for people whose jobs intersect with information security. It is something agencies should be more flexible about. Recommendations on those lines specifically would be helpful.

Mr. Donohue: Another cultural shift to get away from is that physical separation is somehow superior to cryptographic separation. In fact, cryptographic separation introduces other activities to mitigate risk in terms of audit and fine grained control about access to information and knowing who got access to information, and knowing what they did with it.

Mr. Ryland: The idea of low hanging fruit is what I'm struggling with. Many problems are not

simple. It may have more to do with incentives that don't exist at the moment. It's not part of how the Government is structured, or how people think of their career. They don't seem to be oriented toward solving security problems, or modernizing systems. The right incentives doesn't seem to be in place. It's not a low hanging fruit, but it strikes me as being a major issue we struggle with. It may be unique to the Government. Bringing in a new generation of workers, and giving them the tools they are accustomed to, and the modern technology can help change that. It may get to the compensation issue, between the public sector and the private sector. It would be healthy and beneficial if we can figure out a way to solve some of those issues we can begin to see big improvements.

Mr. Chabinsky: *[to Mr. Donahue]* One topic in your brief really resonated with me. You were talking about how we've had a lot of failed strategies to date, and we tend to take recommendations, divide them into groups and 'staple them together', and then realize they don't really add up to a strategy. Instead, your suggestion is that we need a unified purpose to help solve specific problem. Dr. Cooke talked about efforts his group made to solve high priority problems. For us to not repeat that sequence, we need to start figuring out what the goals are, What the specific security problems are, for which the recommendations get formed together for that metric-based goal.

Earlier today we heard some areas where that was done. In the international discussion, Mr. Painter talked about China's economic espionage problem Focused efforts were made to resolve it as a security problem. The last panel brought up other ideas, such as reducing lines of bad code as an objective in itself. Things like not clicking on links can be an objective for an organization, getting rid of spoofing, and getting widespread distribution of malware. There is another discussion, in discussion the solution set as though it were the problem set.

Information sharing is not a problem. It's a solution to some problems, but not to others. Relating this back to all of you, and it includes anything I've already said, what are the specific problems we would have as that goal? In speaking about the moonshot, we knew where the moon was and what direction we were going, and we knew we had to come back. What are the specific goals, considering everything we've spoken about to form it?

Mr. Donohue: It gets back to understanding our businesses in the modern era better than we do. We need to understand our risks entail when we do share, and we should understand what information shouldn't have existed in the first place. We also need to understand where it's important we do share, and how to do that in way that we are sharing what we should, and not sharing what we shouldn't. It becomes fundamentally down to understanding our workflows, and what is necessary about them, and how to improve them and take advantage of new technologies. There is a synergy between design and organizational architectures that needs to be brought together into a single thought process.

Mr. Chabinsky: Is the goal to reduce collection of over-sensitive information?

Mr. Donohue: The goal is to understand what's been brought together and why. It gets back to risk. We're not thinking of it at a system level. We think of it in bits and pieces, and we need to bring it together. It is a non-trivial problem that will require thought. We need to think about how the current missions of the Government need to be executed in the current digital environment.

The outcome should be better security and better processes. The problem with cyber is, it is part of everything. Cybersecurity cannot be separated from the mission. It is an organizational problem that needs to be addressed, and the cyber needs to be brought up into that level. It's not a detailed technical checklist, because it's not exclusively a technical problem.

Mr. Chabinsky: It's also hard to know when we get there. What are the goals by which we can measure success?

Mr. Donahue: Part of the research is to measure the risk. The average manager in the Federal Government does not understand how to measure or evaluate risk or understand what the possible alternatives are so that they end up in a better place.

Mr. Ryland. When high level goals are stated, it's not clear what actions need to occur. As the level of generality comes down to more specific things, the applicability also narrows. The key is to find mid-level principles that are specific enough to feel actionable, but general enough they apply to lots of things. It may be you are looking for concrete kinds of things. Another example that came up today is automated software testing. That can be a goal for which some actionable principles can be developed. We may be able to think further about it and provide some follow up.

Dr. Cooke: One of the things that has come up from panelists today is the notion that the world is moving to software. One way to approach the vision, is to look at what does the Federal Government look like in a world transformed to software. Then, how do we get there? We need the right culture, and a process to hire the right people to live in a world of software. There are ways to measure success. In a world of software, we need tools to automate processes and infrastructure.

As we heard in the last panel, there is some interesting research in that area. We can measure our progress in automation of cybersecurity tooling and infrastructure. We can also measure our ability to use that automation. Across the Federal enterprise. Investing in policies and governance frameworks that provide hooks to support automation. We should think about where we need to consolidate. If we live in a world of automation, we need software to control that infrastructure. We can measure how long it takes to deploy patches, as an example.

Mr. Mill: What is a government that is run by software, still controlled by people, and the logical barriers are the logical barriers the Government puts up. It is an important idea. I think one metric we might look at is how long it takes to get an ATO. If that number decreases, all that implies is varying levels of organizational maturity, a commitment to automation, and a belief in automation. Belief in automation leads to better security outcomes.

If we're picking specific metrics, that might be one that gets considered. We'll know at least part of the work is done, when we hear people talking about the private sector the way they talk about the private sector. There is an automatic level of authority that comes when certain names in the private sector are mentioned, like Google or others. It would be nice for some agencies to have that level of credibility. That is a sign of success, and it takes a community of all the things panelists have spoken about.

Mr. Lin: *[To Mr. Mill and Dr. Cooke]* – You are both newcomers to federal service from the private sector. You could have done any number of things in the private sector. Yet, you chose to accept

starvation wages in federal service compared to what you could have gotten in the private sector. From your perspective, what would you tell your peers to entice them to come into the public sector?

Mr. Mill: I do make pretty good money even in the public sector. I came from a non-profit previously, and did not take a pay cut. The thing that brought me into government was the promise of having a real impact. We would be given the ability to run and deploy code, and the ramifications of those acts would be taken seriously inside the agency. We would have the ability to do a good job and do the right thing. That promise can be sent out as a signal by agencies. Letting people know what agencies are doing with developing code will reach the audience it needs to reach to get people interested.

Dr. Cooke: One of the questions that people have when taking a job is, what is the impact could I have in this organization and the world. One of the things that hasn't been clear, at least in my experience in joining the Government is that one person can have an impact. Hearing that there is an opportunity to work directly with senior agency leadership on critical problems is an important factor. Hearing there is a mandate to make important decisions that will change the status quo in government is important. Hearing there this an opportunity to build a unique culture of leadership with private sector experience is very helpful. It is also helpful when the President of the United States says, it is important for technologists to come and serve in the Government. I think that message really makes a difference.

Mr. Lin: *[To Mr. Donahue and Mr. Ryland]* What I'm about to say is not a serious proposal, but so that I can understand some of the issues that cloud brings to the table. The intelligence community is not putting its cloud on Amazon. Why would Amazon not be the right place for the intelligence community to put its cloud?

Mr. Ryland: The capabilities are the same, the same software and hardware that we sell commercially. However, the difference is that it is connected to a different network. It really is a copy of the commercial cloud that we run everywhere.

Your question is still an important one, because I've thought about this. When will come the time that even a top secret, secured, compartmentalized workload could run in a commercial environment. I believe that time will come, and it's not that many years away. It will come not only because of technological innovations, but separations that provide strong cryptography, absent separation of duties, and incredibly strong audit control so that the customer will know better what is going on in that large scale environment than what they will ever know with physically separated equipment.

That is my personal opinion. It might be ten years away; it might be more. It will happen and we will all be better off. Small capacity pools are inefficient. When we build small capacity, no one is happy. Large scale capacity is what works. Having large capacity with strict logical separation is the future. It will take a while to get there, and once we get there technologically, it will take a while to convince people.

Mr. Donohue: The answer to your question is, it's our threat model. We're considering nation-state threats who look at our data as the ultimate crown jewel. Therefore, we must provide a degree of logical and cryptographic separation and a degree of physical separation on top of that.

Separation against human threats, surreptitious entry, emanations. It gets to the issue of having a different subset of people managing data as opposed to everyone else.

Mr. Ryland: I'm not stating Amazon's position but I'm speaking as a technologist giving my thoughts on where things might go. There may be a lot of issues, and some people may not be convinced that logical separations, and separation of duties is the key thing. Blocking access between segments of data helps to keep all of it safe. Details will need to be worked out.

Mr. **Donahue**: We are working against people who are literally willing to devote their lives to getting access to our information. We are dealing with organizations for whom there is no economic answer to the problem of getting to our information. They have skill sets that are unparalleled.

Mr. Lin: *[To Mr. Donahue]* Is it a fair statement to say that you push the time when this happens out farther into the future, or if ever?

Mr. Donahue: I think I'm in the "if ever" category at the moment. I don't see the technology by itself as being sufficient to defeat the full scope threat.

Mr. Lin: What I hear that since you are going to the same technology, but in a different network, is that you are talking about air gap.

Mr. Donahue: Air gap is a misnomer. Cross-domain is another challenge, but I think it's something we think we know how to manage. The risk that comes along with what we've done here in concentrating in a facility, is a risk of physical damage. That's what we worry about. That's why we invest in multiple locations.

Public Comment

The following read prepared statements for the Commission.

Larry Clinton

Eighteen months ago, we asked each member of the United Security Alliance Board one question: "If you had thirty minutes to advise the next President on cybersecurity in your sector, what would you say? The result is *The Cybersecurity Social Contract* book which we've given you today. We've designed this book to be credible, comprehensive, coherent, and concrete. We believe it is *credible*, because the heart of the book was written by the CISOs of major corporations representing eleven different sectors.

It is *comprehensive* in that we don't confine our analysis to the "usual suspects" of critical infrastructure like defense, IT, telecommunications, financial services, and utilities, but also address cyber threats in manufacturing, education, healthcare, and agriculture. These sectors have experienced cyber threats equal in sophistication to those directed toward sectors defined as critical infrastructure. Yet these last-mentioned sectors have received little or no attention.

Chapters 3 through 11 analyze what is unique from the cyber perspective for each of these sectors, what specific challenges they face, and then offer specific policy recommendations directly related to those needs. It is *coherent* in that we organized our recommendations in the context of the hard-won, bi-partisan, industry-supported consensus approach to cyber security: the Social Contract. Chapter 1 describes how the consensus was developed and explains in detail

why the outmoded regulatory models developed in the 19th and 20th century are inadequate and, in fact, counterproductive to address the cyber security problems faced in the 21st century. To solve the cybersecurity problem, we first need to understand it.

The cyber threat is equivalent to the invention of gunpowder: mandating thicker armor is not going to work. It's not so much that the technology is bad, as it is that the technology is under attack, primarily because all of the incentives belong to the attackers. Cyber-attacks are cheap and profitable, defense is difficult after-the-fact, we can't show return on investment regarding prevented incidence, and we have virtually no law enforcement. If we intend to adopt a traditional regulatory model, we will be creating a cyber Maginot Line that will sap our cybersecurity resources and undermine our actual security in favor of compliance.

We offer recommendations on three levels:
1. The first deals with the tone which must be taken by the President, such as the need to attack this problem with greater urgency, as well as to significantly increase funding for the effort, although we included a blog regarding "ten cheap tricks" to address cybersecurity.

2. The second addresses cybersecurity at the strategic level, such as the need to move away from the IT-centric approach and better integrate economics into the effort. We should increase our appreciation of cybersecurity from the perspective of law enforcement, over and above cybersecurity as a critical infrastructure issue. We must also focus on the needs of smaller organizations who presently receive, at best, only lip service from the Federal Government.

3. Finally, we conclude with operational recommendations, such as a specific plan to develop metrics for the cost-effectiveness of the NIST Framework in order to stimulate greater use of the tool. We recommend altering the backward-facing, compliance-based, pass/fail model in favor of a forward-looking risk management maturity model which is much more appropriate to the problems we face.

The back section of the book consists of six chapters addressing cost-cutting issues such as the evolving role of corporate boards, the need for corporate and government structural changes, the need to rethink our methods of cyber audits and assessments, how to better use insurance, how to balance the competing needs of law enforcement, privacy, security, and intelligence communities, and, finally, the best ways to actuate the public-private partnerships desired by all of us.

Finally, I ask you to turn over the book and look at the back cover.
Any recommendations submitted to the President, must be supported by Government, Industry, and Academia. <Quoted Chertoff and others as illustrations>.

The report consists of 400 pages, 100,000 words, 17 chapters, and 106 recommendations. Mr. Clinton stressed that the Government, industry, and consumers are all on ONE SIDE. The BAD GUYS are "out there" attacking all of us.

Mari Cevikes, College of Healthcare Information Management Executives (CHIME)

Ms. Cevikes spoke to highlight cybersecurity issues specific to healthcare. Attacks have been directed at hospitals, clinics, and the healthcare providers they serve. Healthcare records are considered to be several times more valuable than credit card information. It is estimated that over 112 million healthcare records were breached in 2015. Ms. Cevikes then shared some of the

high-level comments and recommendations submitted to the Commission concerning healthcare as a critical infrastructure:

1. We are pleased to see greater attention placed on the need to secure healthcare information, including the work being done by HHS's Healthcare Cyber Security Taskforce. We are also pleased to see an increased focus by NIST on risk management in the Framework as well as the FDA focusing more on cyber security, particularly concerning devices, and the growing attention by C-suite executives and the Federal Government on cyber security.

2. We see the following barriers and challenges as well as offer a few recommendations:
We believe that federal agencies must improve transparency on known threats so that the healthcare industry can better implement risk-mitigation strategies. We need more plain-English guidance on addressing current threats. We also believe that, since there is a growing number of medical devices which are now connected to the internet, cyber security should be seen as a patient issue and not merely an IT problem.

We also believe that, when it comes to compliance, providers need guidance to assess controllable threats as opposed to those outside of their control. For example, leaving a laptop in your car is a controllable threat. An example of a threat outside of their control would be a threat posed by a nation-state such as China.

We also believe the existing audits are more punitive than providing guidance on addressing cyber security threats. For instance, if an organization is slapped with a hefty fine, they are less likely to make the investments necessary to comply.

Lastly, we feel that more help is needed for resource providers, specifically protections under business associate agreements such as HIPPA, by more evenly redistributing responsibility for security among providers and their contracted business associates. Additionally, incentives must be removed for stolen HC information. It might include better monitoring of suspicious business transactions as well as reduced reliance on SSNs for patient identification. These issues should be viewed as a national priority and that attacks against the HC industry should be considered as important as attacks against other critical infrastructure sectors.

Michael Nelson Head of Global Policy, Cloudflare

Cloudflare is a San Francisco-based web security firm with approximately 100 data centers in more than 35 countries, protecting over 4 million websites (often free of charge) against DDOS attacks as well as providing end-to-end encryption. Last year, we doubled the number of websites supported by HTTPS. Each day, we managed about 10 percent of the world's web requests, and that number is growing very quickly. Mr. Nelson shared "a few tweetable thoughts."

He was glad to hear the hearing focus on all three pillars of cyber security: confidentiality, integrity, and availability. In most meetings, the focus is almost exclusively on privacy and confidentiality, ID theft, and data breaches. But not much is heard concerning websites going down, and DDOS attacks.
Mr. Nelson was also glad to see, and learned a lot, from the panels on procurement and innovation, both critical issues. But most important, sixty percent of his time is focused on what is going on outside the U.S. and eighty percent of his time is spent on addressing bad policy. So while

he was glad to hear Tom Donilon speak of *best* practices, he would be equally glad to hear something about *worst* practices, for instance:

1. The Wassenaar Arrangement (developed in Dec. 2013), which was designed to impose export controls on "snooper ware" which dictatorial governments could use to snoop on their own people. Unfortunately, it was expanded to cover the export of information on cyber vulnerabilities. It could have a huge impact on international research collaboration and on the work we do with other companies around the world.

2. The new UK firewall, announced a few days ago and designed to block malware. Initial reports indicate that this will have a huge impact similar to the effort to block pornography – the problem being a "one size fits all" solution.

3. What Mr. Nelson did not hear discussed concerned law enforcement access to the cloud – an incredibly important issue for any company operating in the cloud. There is not clear, transparent policy governing when government law enforcement agencies can get access to information stored in the cloud. The result could be a major trust problem concerning the cloud with a resultant impact on implementing security policies for worldwide cloud usage.

Concerning workforce development, he didn't hear the term "immigration reform." We need very esoteric skills, often found outside the United States, in countries like Bulgaria and Japan. Each time we attempt to hire anyone, we have to play "visa roulette."

The last issue is standards: to consider the small companies whose product is not covered by policies crafted prior to developing and implementing those products.

Charlie Tupitza Global Corps to Advance Transparency

Regarding IT service management within the Federal Government and the commercial sector, we need to be circumspect regarding the terminology we use and to use the lexicon commonly used in strategy as practiced by government and private companies.

Meeting Adjourned

The meeting adjourned at 5:15 p.m., Eastern Time.

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

Tom Donilon
Chairman
Commission on Enhancing National Cybersecurity

These minutes will be formally considered by the Commission at its November 21, 2016, and any corrections or notations will be incorporated in the minutes of that meeting.

Annex A – List of Attendees

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

Last Name	First Name	Affiliation	Role
			Officer (DFO), Commission on Enhancing National Cybersecurity
Barrett	Matthew	NIST	Attendee
Christopher	Painter	US State Department	Presenter
Donahue	Tom	CTIIC	Presenter
Nelson	Camille	Dean, American University Washington College of Law	Presenter
Delaney	John	Dean, Kogod School of Business (KSB) at American University	Presenter
Lewis	Rebekah	Deputy Director, Kogod Cybersecurity Governance Center (KCGC)	Presenter
Pritzker	Penny	Secretary of Commerce, US Department of Commerce	Presenter
Chenok	Dan	Executive Director, Center for The Business of Government, IBM	Presenter
Evans	Karen	National Director, US Cyber Challenge; Former CIO, US Government	Presenter
Fischer	Eric	Senior Specialist in Science and Technology, Congressional Research Service (CRS)	Presenter
Wilshusen	Gregory C.	Director, Information	Presenter

Last Name	First Name	Affiliation	Role
		Security Issues, U.S. Government Accountability Office (GAO)	
Davidson	Alan	Alan Davidson, Director of Digital Economy, U.S. Department of Commerce; Senior Advisor, Secretary of Commerce	Presenter
Walker	Mike	Program Manager, Information Innovation Office, Defense Advanced Research Projects Agency (DARPA)	Presenter
Ziring	Neal L.	Technical Director, Capabilities Directorate, National Security Agency (NSA)	Presenter
Cooke	Evan	Senior Policy Advisor, Office of Science and Technology Policy, The White House	Presenter
Donahue	Tom	Research Director, Cyber Threat Intelligence Integration Center	Presenter
Ryland	Mark	Chief Solutions Architect, World Wide Public Sector Team, Amazon Web Services (AWS)	Presenter
Mill	Eric	Senior Advisor on Technology, Technology Transformation Service, U.S. General	Presenter

Last Name	First Name	Affiliation	Role
		Services Administration (GSA)	
Clinton	Larry	Internet Security Alliance	Presenter/Public Participation
Nelson	Michael	Cloudflare	Presenter/Public Participation
Tupitza	Charlie	Global Forum to Advance Cyber Resilience	Presenter/Public Participation
Cevikes	Mari	CHIME	Presenter/Public Participation
Potter	Bruce	NIST	Event Staff
Knake	Robert	Orkestrel	Event Staff
Smith	Matt	G2	Event Staff
Drake	Robin	Exeter Government Services	Event Staff
Chalpin	John Paul	Exeter Government Services	Event Staff
Barrett	Mark	Exeter Government Services	Event Staff
Cressey	Roger	Liberty Group Ventures	Event Staff
Petrella	Evie	Exeter Government Services	Event Staff
Stine	Kevin	NIST	Attendee
Dodson	Donna	NIST	Attendee
Boyens	Jon	NIST	Attendee
Souppaya	Murugiah	NIST	Attendee
Schlan	Ivan	PMM	Attendee
Dean	Danielle	National Conference of State Legislators	Attendee
Jamie	Mccary	Kogod	Attendee
Sedgewick	Adam	NIST	Attendee

Last Name	First Name	Affiliation	Role
Russell	Michael	State Department	Attendee
Rosendall	Emily	ZRA	Attendee
Morris	Andrew	NAFCU	Attendee
Not given	Eric	Not given	Attendee
Mahn	Amy	DHS/NIST	Attendee
Banghart	John	Venable, LLP	Attendee
Shankles	Stephanie	Booz Allen Hamilton	Attendee
Larberry	Sean	FCW	Attendee
Ahrens	Nick	RILA	Attendee
Egger	Matthew	USCE	Attendee
Hoscorn	Nick	MITRE	Attendee
Linh	Vijay	Canon	Attendee
Rosero	Diego	Not legible	Attendee
Raleigh	Kimberley	DOJ	Attendee
Codlen	Michael	Boston Consulting Group	Attendee
Smith	Angie	NIST	Attendee
Townsend	Mariel	EBP	Attendee
Morgan	Sean	Palo Alto Networks	Attendee
Penagos	Melanie	Publicknowledge	Attendee
Cucchia	Bruce	MasterCard	Attendee
Nogglo	Lanco	CUNA	Attendee
Zuidena	Liz	Microsoft	Attendee
Shannon	Greg	OSTP	Attendee
Roman	Sonia	WCL	Attendee
Keben	Jason	DoS	Attendee
Delone	Bill	American University	Attendee
Golusten	Elil	OIS	Attendee

Last Name	First Name	Affiliation	Role
Peneus	Mark	MITRE	Attendee
Greene	Jeff	Symantec	Attendee
Valencia	Sharon	Axon Global	Attendee
Martinez	Israel	Axon Global	Attendee
Garland	Knolt	Kogod American University	Attendee
Porier	Heidi	Self	Attendee
Torres	Daniel	KCGL	Attendee
Lahsrarec	Andrew L.	National Governors Association	Attendee
Grunstra	Karen	UL LLC	Attendee
Prominski	Tom	Patonal Global Partners	Attendee
Romine	Charles	NIST	Attendee
Miller	John	ITI	Attendee
Glassok	Tom	Property, Casualty Insurers Association	Attendee
Mushrick	Ashley	Commerce	Attendee
Pence	Jennifer	US Bank	Attendee
Boyer	Chris	AT&T	Attendee
Emokpae	Michelle	Kogod	Attendee
Bartol	Nadia	BCG Platimon	Attendee
Shimizu	Takeshi	CSIS	Attendee
Dantzler	Will	WCL	Attendee
Miller	Jason	WCL	Attendee
Dandar	David	The MITRE Corporation	Attendee
Nelson	Michael R.	Cloudflare	Attendee
Cooper	Steve	US Department of Commerce	Attendee

Last Name	First Name	Affiliation	Role
Landfield	Kent	Intel	Attendee
Perera	David	ISA	Attendee
Myer	Robert	Not legible	Attendee
Garriott	Ashton	MITRE Corp	Attendee
Hill	Jonah	US Department of Commerce	Attendee
Rob	Jen	Not indicated	Attendee
Khona	Mimeer	Rising Sun Advisors	Attendee
Cooke	Evan	EOP	Attendee
Darl	Celeste	DoD	Attendee
Vaughn	Milar	WCL	Attendee
Islam	Ayan	WCL	Attendee
Steele	Bert	ISACA	Attendee
Niejelow	Alex	MasterCard	Attendee
Crofton	Andrew	Sprint	Attendee
Lyeber	Rick	Inside Cybersecurity	Media