Commission on Enhancing National Cybersecurity

Briefing on Current Federal Initiatives for the Federal Governance Sub-Committee
General Services Administration
1800 F St, NW, Room 6151
August 3, 2016; 12PM-5PM

Attendees:

Executive Director, Commission on Enhancing National Cybersecurity
Kiersten Todt

Commissioners:
Tom Donilon (Chair), Sam Palmisano (Vice Chair), Herb Lin, Keith Alexander, Peter Lee, Steven Chabinsky, Heather Murren

Agency Representatives:
Department of Commerce (DOC): Bruce Andrews (Deputy Secretary)
Department of Defense (DOD): Robert Work (Deputy Secretary)
Department of Justice (DOJ): Joe Klimavicz
Department of Homeland Security (DHS): Alejandro Mayorkas (Deputy Secretary), Jeanette Manfra, Eric Goldstein, Amy Mahn, Andy Ozment, Thomas McDermott, Luke McCormack
Federal Trade Commission (FTC): Raghav Vajjhala
General Services Administration (GSA): Denise Roth, Matthew Cornelius, David Shive
National Institute of Standards and Technology (NIST): Donna Dodson, Kevin Stine, Adam Sedgewick, Matt Scholl
National Security Council (NSC): Michael Daniel, Samir Jain, Andrew Grotto, Grant Schneider, Lisa Monaco
Office of Management and Budget (OMB): Margie Graves, John Lynch, Andrew Mayock
The White House: Kristie Canegallo

Agenda:

I. Welcome
II. Introduction
III. Welcome from the White House
IV. Federal IT and Cybersecurity Roundtable
V. Case Studies Presentation and Discussion
VI. Closing

Welcome

Michael Daniel, National Security Council

Mr. Daniel opened the briefing at 12:06 p.m. Eastern Time.

Denise Roth, GSA Administrator

Ms. Roth thanked the commission for the opportunity to host the meeting at GSA. She gave an overview of the GSA building at 1800 F Street, noting it is a unique space in the federal government. The building is one hundred years old, and held 2,500 people prior to extensive remodeling in 2013. It now holds 4,400 people. It is considered a standard for federal government modernization efforts.

Introduction

Tom Donilon, Chair, and Sam Palmisano, Vice-Chair of the Commission on Enhancing National Cybersecurity

Kiersten Todt, Executive Director, Commission on Enhancing National Cybersecurity

One of the express orders for the commission is to look into governance, process of cybersecurity, IT frameworks, and procurements, in order to be able to come up with recommendations for how federal IT systems can be upgraded and modernized. We are here today to do the following:

1. Attempting to learn what the base line is and how the federal government works today;
2. Learning what is working and what isn't, and how the next President can do it better. We like to have folks provide recommendations; and,
3. Speaking to leaders on their roles and responsibilities, and on what they do in their agencies and how cybersecurity is working.

We will build on a lot of what is going on, so that we may be able to accelerate best practices and fundamentals. One of the challenges facing us is cybersecurity, so any suggestions that may be important to mention, please do so.

Welcome from the White House

Lisa Monaco, National Security Council

This session has two goals:

First, to assist everyone here. We hope to enable everyone to ask further questions and delve deeper into cyber efforts that are ongoing. Second, this ought to be a series of intensified engagements between the commission and federal experts. The President was clear with the cabinet that they should be available and accessible to the commission's efforts.

There are a combination of things that have created the need for the Commission on Enhancing National Cybersecurity. Our infrastructure is aging, outpaced, and outdated. Intrusion technology is evolving, and protection technology is evolving. The threat landscape has accelerated. Things are not slowing down. The number of nation-state actors and criminals are increasing. The federal system is stuck with an infrastructure that is plodding.

The federal government is uniquely challenged in trying to resolve these issues. We have a budget process that is not conducive to IT planning. These things thwart efforts to accelerate the pace of change. In the last 24 months, we have had Heartbleed, the OPM

breaches, and other significant intrusions that have occurred on top of the known cyber-attacks. These attacks have pointed out some major deficiencies.

The Cybersecurity National Action Plan (CNAP) and other sprint efforts from this past February are still ongoing. Some of these efforts will be short term, and some will carry on through the next administration. However, within many of those initiatives, we discovered uneven security and unprotected high value equipment. There is high value in targeting adversaries. We still face recruiting and retention challenges. There are gaps in the federal government. These findings come from the Office of Personnel Management (OPM) and Heartbleed responses. There will be discussed more in the sessions this afternoon.

Federal IT and Cybersecurity Roundtable

Mike Daniel, Moderator, National Security Council

The session today is made up of a panel of experts that will provide cross-agency perspectives, interactions, and challenges. Candor is crucial, and I urge hard questions from the commission, and straight responses from the experts. It is worth understanding how we've used tools and responsibilities across the federal government to get the response down on paper. What are the proposed chief information officer (CIO) challenges in each different agency? What is the utility split, and how are the CIOs interacting with their leadership and are they brought in as a risk management team? For agency leadership, how are they thinking about risk management, and cybersecurity across their agencies?

For the final session, how is the Deputy Secretary thinking about risk, and bringing in CIOs and leadership at the policy table? They should ask questions directly related to policy, related to defense issues with cybersecurity risks. Additional questions to ask are, how has the federal government lifted itself out of its technical rut?

That's how I see the day's work and areas of questioning. It is hoped we'll give the commission a foundation for further research and asking questions. The federal side is ready to continue and intensify the engagement over the next few months.

Senior agency experts from NSC, OMB, DHS, NIST, GSA, DOJ

Commissioners of the Commission on Enhancing National Cybersecurity

Mr. Donilon: What does it say about the structure of the federal government that it took so long to make a response? What is it about the way we are organized that caused it to take longer?

Ms. Monaco: Two things. It is not unusual for there to be disagreement about who is responsible for responding first following incidents. Setting out who is the cybersecurity chief responder would help increase the response speed. Additionally, we were able to take in some lessons learned from recent events. There are a number of agencies including the FBI, NSA, and DHS with legitimate roles in investigating cyber-crimes, and there is a set of expertise for mitigation.

Mr. Donilon: What about a more centralized response and having one agency responsible for cybersecurity? Would you consider that?

Ms. Monaco: Like a cyber agency? We have broadly thought about that. The agency provides incident management coordination response. We adopted some of a FEMA-type response model. We adopted some of that approach in the Unified Coordination Group (UCG). There is a lead agency that draws upon specialty agencies. We have recognized there is no one agency that holds the entire response.

Mr. Donilon: When it comes to the role of CIOs in the government, they succeed with varying degrees of authorities. Have we considered a model set of authority for CIOs?

Ms. Monaco: We have done some of that through OMB. What is lacking is enforcement and accountability of CIOs and implementing best practices.

Mr. Daniel: We have moved in that direction. The issue is the diverse culture across the federal government. There is a misalignment between where risk is taken, and where it comes home to roost.

Ms. Graves: Legislation on CIO authority is a starting point. The culture in some agencies does not support what we are trying to achieve here, but things are changing. More people in leadership are trying to create change in this area. It's those kinds of changes we are trying to create.

Mr. Donilon: It sounds like a leadership issue. Is it that we are not imaginative or intuitive enough to solve this problem? We are we always reacting as opposed to being ahead.

Mr. Chabinsky: Is it the information we've been collecting, is the type of reporting enough, or is it the right kind? Are the right resources available to review? What do we hand off to the next administration to give them what they need?

Ms. Monaco: It is cultural and structural. We have seen both sides of the question. We have seen data getting collected and not used by the C-Suite. There is a culture that reporting is voluminous and needs to be accessible to people that make decisions. Things get done when there is accountability for them. The President has made accountability important in the last few years.

Mr. Chabinsky: The follow-on question is, in order to hold leadership accountable, should it be DHS or the White House?

Ms. Monaco: It should be DHS with an appropriate oversight function. We don't want to bring too much operational responsibility into the White House. After Heartbleed, agencies were at least reticent, or at most, hostile to DHS coming in; if only to scan for the vulnerability. Prior to DHS, there was not a mandate authority. It should have been done prior to Heartbleed.

Mr. Lin: To your knowledge, is agency leadership responsible for technical IT testing equipment and infrastructure? Meaning, is their personal performance being rated in leadership?

Ms. Monaco: The President has cybersecurity as a top agenda priority. Agency email is part of vulnerability testing. There are anti-phishing campaigns for agencies. They are not singled out. Their leadership performance is evaluated. There is consideration of expanding the Development Innovation Ventures (DIV) program. There are critical infrastructure programs.

Mr. Alexander: There has not been discussion of attacks on major sectors to do us harm. IT must be rehearsed government wide and work with industry.

Mr. Lin: If there was an attack of major sectors in the future, we may need to be test different types of scenarios.

Mr. Daniel: We have not assimilated what digitizing records really means. It became possible to steal 21 million records and get away with it. We fail to appreciate the transformation of the threat involved in moving to digital, and what it means to the physical and digital world. And we don't understand what it means in terms of cyber threats. We have not appreciated what would be targeted. We have not recognized what a digital world means.

Ms. Monaco: I would agree that we have not sufficiently appreciated what would be targeted. We were concerned about intellectual property theft and espionage. We did not think about impact in other areas, and what would be targeted.

Ms. Todt: What are the consequences when agencies don't follow through? Is there a process in place? Should there be?

Ms. Monaco: There should be consequences and agencies have to know what is going to be measured on cybersecurity within leadership, specifically agency leaders. Recommendations and thoughts of how to do accountability without being self-defeating is needed. There is something about sitting across the table from the President and having to explain why the agency fell short. That may be the biggest enforcement mechanism we have.

Mr. Daniel: There are three pillars to cybersecurity:

1. How do we raise the level of cybersecurity? We will spend a lot of time today on that.
2. How do we disrupt and prevent the bad guys?
3. Because those two things will fail sometimes, how do we respond when that happens?

This is not an NSC process. The goal is not to arrive at an NSC consensus. The structural challenges cited by Ms. Monaco were highlighted by three things:

1. Legacy systems: Some of this is shared by the private sector. The government has a budget system that is a problem. It is easy to get money to maintain systems, but impossible to get money to modernize.
2. Cyber security of the government: It gets pushed down to the sub-structural level. We live in a world where if we want to deploy a new system we must negotiate with all agencies.
3. Staff retention: It's not just about the coders. It means having cyber-smart acquisition, lawyers, managers, etc., who incorporate good practices into everything they do.

The Comprehensive National Cybersecurity Initiative (CNCI) binder from 2008 consisted of twelve initiatives: EINSTEIN 2 and 3, trusted connections, active defense, research and development, connecting centers, protecting classified networks, education, workforce, deterring adversaries, supply chain and critical infrastructure. All these things are still being pursued today and have shown good developments. Some have changed dramatically since eight years ago. If we look at CNAP today, it is designed to get at structural challenges. The structural issues are deeply embedded in the federal government.

The commission must think through and arrive at steps for the next administration. Spending on cybersecurity in the federal government has risen to 19 billion dollars a year. The government is

spending a tremendous amount of money. We need to make sure those resources are properly allocated for cybersecurity.

Ms. Graves: OMB's role is policy and requirements for other agencies to hold accountable standards. We are ensuring and tightening up our policies that will continue within the CNAP. Taking the short term view has led us to the issues that we are facing today. However, we should focus on current technologies, development, and modernization. Circulars like the A-130 are important for keeping written track of what we are doing.

The IT Modernization Fund (ITMF) is the lynch pin for working past the infrastructure challenge. Even modern portions still tie back to old infrastructure. We are taking the opportunity through The Federal Information Technology Acquisition Reform Act (FITARA), and budget authority, to make sure the right things are prioritized in budget. We can incentivize the right behaviors through budget. We have established the OMB 300 form to establish cyber priorities, but it doesn't work unless the entire C-Suite works to get things done. It must be monitored and enforced. We need to determine what data elements are important and track those. As we see the landscape change, then we will shift our priorities. In order to do this we have to change the budget process for federal agencies.

Mr. Donilon: Can you describe the outlines for these priorities to get funded?

Ms. Monaco: We have asked agencies to assist with business case evaluations. We also look for people to submit cases for shared uses, and evaluate shared mission space. We are only as strong as the weakest link. Modernization must occur across the spectrum.

Ms. Graves: Cyber is one element that is difficult to budget, if agencies are willing to look over their shared business cases together.

Mr. Donilon: Is it like a grant system? For example, providing the most important things we need to fix.

Ms. Graves: It is more like, what your mission functions are, and which ones are the ones you are most in need of. Every agency may require different things based on its mission.

Mr. Donilon: Does OMB have a concept of the required investment over the next 15 years? Is there a high level estimate?

Ms. Graves: It would be helpful to pursue the same funding for cyber as other defense agencies. The expectation is that it is a revolving fund, and will be replenished over time. It must support continuing to keep technology current.

Mr. Donilon: How do we know we are spending money on the right stuff?

Ms. Graves: How do we know the next dollar is decreasing risk? Assess top risks, say here is what we do to mitigate those risks, and evaluate the dollars to do that. Combining risk models with the NIST Framework provided the ability to see where the money was going.

Mr. Daniel: I'm not sure we have a good handle on the modernization backlog. One of the problems is that people give up. They decide trying to get money is futile. When money does come, the backlog of projects grows. Even if there was an estimate, the amount will grow. Secondly, I would

draw a connection to the Framework. One of the things we don't have is how do we think about measuring. We don't have metrics that are as well developed as they should be. It is an area that needs a lot more development.

Ms. Todt: How do we demonstrate return on investment (ROI) and what are the metrics for doing so?

Ms. Graves: Greater visibility has helped identifying actors and domains.

Mr. Ozment: We should think of IT as a pyramid. At the bottom is the money and the people. The next level is a sub level, with a CIO, but possibly not. The span from the bottom to the top of the pyramid presents an interesting array of questions. Most CIOs do not report to a deputy secretary. Politics can be a disincentive to agency level CIO responsibility. Book software code is law. There is a degree that it is true that software architecture is also law. We should be down to 65 agency connections to the internet, and four others. The architecture problem mirrors the governance problem.

There are good questions about measurement and motivation. There is no trustworthy data. There are different tools, some automated, some not. The worst agency underestimated its measurements by a third of the actual number. There are problems in status reporting.

Mr. Donilon: Who is responsible for the audit function?

Mr. Ozment: Offices of Inspectors General (OIGs) and CIOs are responsible, as it is self-reflected data. Agencies collect data. There are continuous diagnostics and mitigation (CDM) programs. We will have computers measuring computers. We will have dashboard computing by the end of FY17. We will have data we trust then. Phase 3 will be at the agency level at the end of FY18, government level later. We are on the cusp of a massive strategic shift. We've been telling people what to do for 20 years.

Many mandates have been issued, with little follow up, and no money tied to them. DHS got the authority for binding operational directives. Agencies are not listening to DHS. Orders should be follow-able, and measurable. The first was to measure vulnerabilities in systems that connect to the internet. It took a long time, and still is going on.

Ms. Todt: Why was DHS entrusted with this, and why did it take so long?

Mr. Ozment: It is important to say that my portion of DHS was not always viewed as super competent. I think it has turned around, but maybe people are being nice. I don't believe in federal doubt and there is now a statute. There was doubt, but I think it's more the White House having to deploy Einstein. Still, there are three agencies refusing to sign agreements and implement as there are privacy issues. Two control mechanisms to leverage are the budget and the internet. We should get the small agencies to stop providing their own IT.

Mr. Chabinsky: Why isn't the answer you [DHS] taking over the system?

Mr. Ozment: The pendulum can swing too far. For the smallest agencies, we need to get them out of the business of running their own IT. At large levels, you take it too far from the mission owner.

Ms. Dodson: It's a risk management approach. How do we help them manage that risk? Cyber people are good at talking to cyber people, but not good at talking about risk. We want to do this like good practitioners, and then back away from the cyber controls.

Mr. Chabinsky: Things do take too long. The problem persists. It's within the power of the executive branch to solve it, but they don't.

Mr. Ozment: Some heads may need to roll. Getting rid of department heads because they don't know cyber may be self-defeating. There needs to be some sort of action; we need to make an example.

Mr. Chabinsky: This may be an unacceptable model that is not reaching success. This is self-defeating in the issue.

Ms. Graves: Enforcement mechanisms need to trigger more quickly.

Mr. Daniel: We have not made the shift in how we want to manage risk in the digital world. In the past, the risk was disclosure or misuse of information by the government. Now, the primary threat is not disclosure to the government but disclosure to adversaries. We want to have mechanisms in place that ensures federal government information is protected. We don't have the speed to do things in less than eight years of negotiations.

Ms. Todt: Who is accountable for data loss?

Mr. Palmisano: First, ask, who can give me a plan to stop losses? As the President, who would be the appropriate person to provide a plan on data loss?

Ms. Graves: Tony Scott is Federal CIO and he reports to the OMB director.

Mr. Palmisano: The OMB director should provide a plan. It has to start at the top. It is a very serious issue. The issue is what is the governing (memorandum of agreement) MOA? How do we make the transition from yesterday to today? The transition is complicated.

Mr. Ozment: Two additional things. First, the biggest concern a lot of the momentum of the CNCI was squandered, and we did not use it the way we could have. We are at the cusp of a strategic shift. With CDM we will have way better data, later phases starts adding security. Einstein is essentially creating a monitoring and security mechanisms at will be a platform. It would be recommended to the incoming administration to not build a new platform but work with the current Einstein.

Ms. Dodson: In terms of being nimble, and thinking ahead we need to see trends that are coming. It will change the nation even more. How are we architecting changes? We are too present-focused, making it harder to look ahead and there is not a mechanism in place. We are partnering at the National Cybersecurity Center of Excellence (NCCoE) to do this.

Mr. Donilon: If the government will be an adopter and purchaser of cloud services who will have standards?

Ms. Dodson: NIST is working with government and industry and standards bodies. NIST is trying to look ahead to see how they can really be used. Everything we are talking about here is about creating that culture of cyber security here and across the country.

Mr. Donilon: How is the sharing information mission going on? How do you feel about a joint exercise and working with industry in the private sector? How is the Einstein model working?

Mr. Ozment: There are pros and cons with the Einstein capability. There are three ISPs that are working for the federal government. Network address translation is an issue. We need to start looking at what the architecture should be. We need to distinguish between indicator and incident sharing. In indicator sharing, I see positive signs but I wonder if those are going to scale. We should know in a year. We have 50 entities signed up and DHS is sharing out but no one else, federal or industry, is sharing.

There are multiple interpretations of the standards. Some are waiting for the final standards to come out. Agencies have not been early adopters at this point. We are working with first private sector company. They do get private sector indicators through the industry group, not the portal.

Break

Case Studies Presentation and Discussion

Joe Klimavicz, Chief Information Officer, U.S. Department of Justice

Raghav Vajjhala, Chief Information Officer, Federal Trade Commission

Luke McCormack, Chief Information Officer, U.S. Department of Homeland Security

Commissioners of the Commission on Enhancing National Cybersecurity

How is an acquisition agency involved in cybersecurity? The ITMF was mentioned earlier. How we vet prospective projects and programs, we play a role in that process. What we assess is cybersecurity stance, and assess value for dollars. We are assessing threats is another roles, especially in financial and other systems.

It will be a natural space for shared systems going forward. When OMB and others create policy, GSA has an ecosystem for that policy. It also has the Technology Transformation service. IT plays in how agencies respond to policies. Every agency interprets policy differently. We are in the place where agencies can take steps toward new technologies for their agencies. We assist agencies that do not have skills in new technologies, and assist with implementations.

Mr. Daniel: Ms. Graves introduced the CIOs. We would like to have each speak about the cybersecurity program within each agency.

Mr. McCormack: There is a distinction between DHS and the National Protection and Programs Directorate (NPPD). We work with them when programs are being developed and through early adoption. We are somewhat federated, and somewhat united as an enterprise. Everything rolls up to some sort of enterprise capability. We have homogenized some tool sets, but not mandated them. We want the CIOs and chief information security officers (CISOs) to make those determinations. We give them a set of standards we want them to follow. There are many contracts they work with that process sensitive data. We are involved with GSA and DOD in certifying cloud vendors. The work is to impose a set of standards based on the NIST Framework for cloud vendors. Every operating component or vendor can then adopt those standards.

Mr. Klimavicz: The challenge we have is managing risk and complexity while enabling the mission. Within the department, there are two primary orders. One is on insider threat, the other is on

cybersecurity. They are fairly mature. There are other controls in place to monitor orders. With respect to governance, there is an oversight committee. One of the biggest challenges we face is the revolving door. We clear and train staff, only to have them leave. Every component is reduced to a numerical security risk, and these are reported to senior management. The budget is one of the reasons why components are in security issues.

There are opportunities for economies of scale, but missions must be understood. We spend a lot of time on strong identity and access management. We have one of the best insider threat capabilities in the government. We are trying to build security into the architecture.

Most money is working capital funds. Money given this year must be spent this year. It is not the best way to plan ahead. We're able to trace additional tools that are put in place and the benefit. It creates a positive return on investment. We're building additional tools for high value assets. There are now cloud solutions.

We are looking to secure cloud solutions. We need to look at better contract language for all federal contracts. The language needs to be tightened across the board. Many partners are not IBB6 compliant. It can hold things up. Data poisoning can be an issue. As we build out technologies, we need to actually implement them. The insider threat is mostly geared to classified systems. It needs to be expanded to unclassified systems.

Mr. Vajjhala: A little background on the FTC/ we do file cases against companies that do not protect consumer data. There is tremendous energy in the FTC for what goes into the report that goes to the Hill. The benefit is great interaction with senior management across the FTC.

What works well? We realize our adversaries do not read NIST guidelines. We think most about insider threats. We need to balance the needs of the mission against cybersecurity. There are about 1,500 people in the FTC and it is easier to communicate agency-wide with a small agency.

Information sharing for a small agency can be more challenging. Change has been slow in the government for many years. It took ten years to repeal a law about data collections from cookies. We see a tremendous opportunity for better price points in moving services to the cloud. The challenges are that prices for security features are higher than for commercial entities. Cost benefits need to be revisited. It comes down to the role of the authorization official. That person has impact in terms of cybersecurity. It may be someone from the business.

At the same time, it is highly concentrated, and a lot to review. The challenge of competing for talent is completely true. Some agencies offer higher rates of pay. People know how to work the system. Once people get into one agency, it's easy for candidates to move up quickly. We accept the challenge of people cycling through. We understand that they may leave in three to four years. Otherwise, we make a compelling case for them to stay.

Ms. Graves: How do we think these challenges have been addressed, or need to be addressed?

Mr. Klimavicz: More emphasis needs to be put on insider threat and greater tools. We need to really address using the cloud in a standard way. We see a lot of people trying to do the right thing with cybersecurity, but they're doing it in their little part of the world. We spend a lot of resources looking for solutions. We should do it once and do it right. There needs to be more sharing what's working and what's not.

Mr. Ozment: We evolved from terrible architecture to an OK architecture and then we stopped. In some ways, we have the worst of both. We need to continue the evolution so that things are truly good.

Mr. Gallagher: What is the scale of the multiplier? Is that the only trade-off? The amount of internet access we get is equal to the use of two families at home. Yet, we pay seven figures.

Mr. Klimavicz: It is not cost effective.

Mr. Daniel: For years, it was not known where the government was touching public switch internet. When the decision was made to go to trusted internet connection (TIC) architecture, there were no cloud services. We need to build in the capability to update for things we can't conceive of now.

Mr. Ozment: Are we understanding connectivity or monitoring control?

Mr. Chabinsky: We sat through numerous meetings to determine how to measure success for the program. We reported quarterly to the President on the overall imitative and underlying initiatives. Risks were reported quarterly and assessed. The policy review said we need to keep having a multi-disciplinary group to continue reporting. If you can't measure, you can't understand.

1. The current administration would need to provide a quarterly report where the money is, what we did with the money, and what was measured and whether it is it good or bad.
2. There should be a group that reports this data to the government. Suggest making sure that coordination inspects itself and understands the funding and reports back to the government at the highest level: directly to the president.

Leadership and Accountability Roundtable

Kristie Canegallo, The White House (Moderator)

Alejandro Mayorkas, Deputy Secretary, U.S. Department of Homeland Security

Robert Work, Deputy Secretary, U.S. Department of Defense

Bruce Andrews, Deputy Secretary, U.S. Department of Commerce

Andrew Mayock, OMB Senior Advisor to the Director for Management

Commissioners of the Commission on Enhancing National Cybersecurity

Ms. Canegallo: To start, please tell us what are the most important things that are working and what is still not working? Let us talk about the government space, but take your regular hat off and speak frankly.

Mr. Mayorkas: What I would say is working well, is the decision to identify one agency, DHS, to defend the government cybersecurity space. We have identified tools to improve the security of the .gov space. What's not working are a number of things: First, I think enforcement mechanisms are not fully identified, employed and accountable. If agencies are non-compliant, there are few consequences. Secondly, we need to better identify the truly significant resources that need to be allocated for the effort. We need to examine the procurement rules relating to cybersecurity.

Mr. Mayock: I agree with the procurement statements. This is a high priority for senior members of the administration. I also agree with investment in creating a cornerstone capability in DHS. Things

in the government are different than five years ago. What's not working? Challenges of modernization and OMB, not being able to plan to modernize. One of the good things the administration did was examine what's been spent on cybersecurity. We need to understand what value has been received for that money.

GSA: We are primarily partnering with DHS. Looking to implement tools, and the right security posture. We are concerned about decisions made by individual agencies. We need to be able to have a choice of vendors and competition on pricing. Ensuring agencies make the right decisions on what the purchase.

Mr. Andrews: We have been focused on the funding aspect, and also need to elevate for CIOs to understand the importance to their jobs. The continuous diagnostic program in DHS has been successful. There has been positive progress. On the challenges front are money, people, governance. We appreciate OMB has made this a priority. There is a recognition of the need for funding. Metrics has been a mixed bag. We need to improve there. Hiring is challenging due to competition. Poaching between agencies goes on to get people. Can we create a common hiring pool? Third, governance: internal and departments. The question is what to turn into shared services. We are looking at things that can be done in common. We should retain the capability to retain mission critical systems.

Mr. Work: We have found in the DOD what works well and should be done government wide. Cyber must be high priority at the top level of the department. There must be a cyber score card. It tracks 13 measures. It has had a remarkable effect on errors. We have tried to make it easier for users and departments, and instead make it hard for bad actors. All cabinet secretaries should be reporting to the President annually. It is starting to work well in DOD, and this should be implemented throughout the government.

Individuals are held accountable. Cyber incident clean up comes out of operation and maintenance dollars. What's not working well; workforce gaps. We are all trying to get people out of the same pond. There should be a separate schedule and pay scale for cyber people. We may not get all the people we need. There could be a U.S. Cyber Service, which would be helpful. Information sharing has greatly improved. It is a technology problem. It could be a priority for the next administration, to increase transparency and speed. Modest improvements are happening. DOD is moving to Windows 10 exclusively. The government should move to a single operating system, whether or not it's Window's 10. Old applications of the system should be removed.

Mr. Donilon: DHS has been given this role, but it doesn't appear it has the muscle it needs. True cyber hygiene will not stop a state actor. There is not a government wide effort. The sprint was an indictment, because we were not doing what we should. It is positive because there was progress. Why has the government asked DHS to lead the effort to create more and better cybersecurity? You talked about mandatory finding of operational vulnerabilities. How do we know what the vulnerabilities are around the government? Is more authority needed?

Mr. Mayorkas: I would say we have the authority we need, but not necessarily the enforcement tools to address non-compliance or slow compliance. We have a range of responses to DHS leadership, from phenomenal conduct, to complete non-compliance. Some object on privacy grounds. There are enforcement issues, capability issues, and funding capability to make repairs as

well as overall agility. There are many reasons why we are not further along. A number have employed EINSTEIN. We need to further empower DHS, or make use of the enforcement mechanisms of the White House or other entities to get the right conduct. We inspect agencies, go in and diagnose.

Ms. Canegallo: Each agency did its own review of its high value assets. DHS is now doing a follow-on review of the assessments made by the agencies.

Mr. Mayorkas: We drive and direct, OMB has the muscle. The muscle must come from someone other than DHS. What are OMB's levers? Even OMB's muscle is not as robust as what's needed. There must be the threat or promise of presidential oversight.

Mr. Mayock: On the partnership of DHS and OMB, the sprint should not have needed to happen. OMB has created a cyber tool. It enables them to go into agencies and take a look at the issues that exist. It is a powerful tool for accountability. It is a mistake to give one agency too much power. The danger of one agency dictating to another is that they don't understand the unique issues in that agency. Resources are limited. We need to make sure it's a fair discussion. It's only recently that all agencies have come to recognize cybersecurity as a priority. The standards being discussed here are separate from mission priorities. It may not be clear that every agency has the capability to handle what's being discussed.

Ms. Canegallo: A larger pool is needed. It's hiring, procurement, and the normal way of doing business hurts us in the cybersecurity realm. Time is the enemy of cybersecurity. Agility must be achieved. Managing cyber risk is in conflict with mission. There is a tradeoff between managing risk and mission critical functions.

Mr. Gallagher: There is a fracture between cybersecurity and the mission.

Mr. Mayorkas: If we can't manage cybersecurity, the mission will fail. One is the prerequisite for the other. It is similar to other tools that are being built out. We need to find a balance between cybersecurity and other areas. It is a false choice.

Mr. Work: Internet of things, and there is no choice about what to do. It doesn't have to be one department. DHS does not have the ability to drive other agencies. They make recommendations, and call out best practices. It is up to a central authority to make sure compliance happens.

Mr. Donilon: The commission is looking for ideas on which to make recommendations on how to recruit and retain people. Ideas on enforcing standards and have more buy in on the other side. How can we make some concrete recommendations?

Mr. Mayok: Provide multiyear money by applying some creative thinking to the annual budget process. That concept will help provide flexibility. As far as procurement and HR, we should think about the kinds of people we need and the procurement and management experts who are part of the process. The average contracting officer may not know the types of people that are needed. Funding has to catch up and get ahead of the problem.

There is a question of the allocations of certain responsibilities in certain functions. The way money and authorities are allocated, we have a compartmented view of how things are done. OPM is having DoD provide security for the new national background investigation agency. OPM is not the

best at protecting data, DoD has the real capability. Can we enable OPM to really focus on its mission, instead of dealing with security? If it's done right agencies can focus more on their primary missions.

Mr. Mayorkas: There is not necessarily one agency doing the work. It is important everyone applies the same standards. Updated and current infrastructure is cybersecurity. It is focused on choices in technology buying. We will still make choices every year on buying. There are other places for the commission to help with the discussion. There has been a shift in perspective in assisting other agencies.

Mr. Lee: I'm wondering about the language relating to enforcement. It seems it has been important to talk in terms of reward, and not just enforcement. Has thought been given to changing how we incentivize change in cyber?

Mr. Work: I'm not comfortable with balance between enforcement and reward. There must be positive incentives. We have been trying to emphasize the importance because there really can be serious consequences.

GSA: Our work building tools is based on needs identified in other agencies.

Mr. Work: If we could agree on some number of metrics to be measured across the government, we can then work for an automated system that reports the data. We might also consider that we all have common business operations. If we went to common business operations, we might get there faster. Every department will start from a different place,

Mr. Alexander: In working on roles and responsibilities, how can the commission help in executing those responsibilities if we were attacked, what can the commission do?

Mr. Mayorkas: If the nation is attacked, the Presidential Policy Directive (PPD) just signed by the President applies.

Mr. Alexander: We have had other panelists that have asked what happens before attacks, what is it now that DOJ, DHS, and the White House, do to prevent these attacks and how can the commission assist?

Mr. Mayorkas: We are talking today to protect the .gov domain and about developing tools to close the gaps that exist and focusing on the standards right now.

Mr. Donilon: Where are we in these key areas that are discussed today, and can information sharing help with industry?

Mr. Alexander: It goes back to the 2012 attacks on the financial sector. There is now legislation that allows sharing. What is the action if it is a nation-state that attacks the private sector?

Mr. Mayorkas: It is a million dollar question. We have a cyber incident response plan draft to be published in September, that outlines what the planning and preparation will be from a prevention perspective. We hope to deliver a revised draft to the president in December.

There is the idea of creating a weather map for cyberspace. Once that picture exists, how do we get ahead of what we are seeing? One of the things we are doing is identifying Section Nine companies that are most vulnerable to a cyber-attack. Then, we get the information out in time for companies

to protect themselves. Disintermediation removes government away from coming face to face with adversaries in cyberspace. We will need new models on how to operate with the private sector. We have the right building blocks, now we need to finish.

Mr. Alexander: The U.S. should lead the effort, or someone in NATO will. Industries are looking to the government for protection. What they really want is to have attacks stopped. The real question is, how do we help? There is an evolutionary approach to cybersecurity. We want to make sure the commission has the resources it needs.

Mr. Gallagher: Looking at protection, we all agree we would protect the .gov. domain. If government assets are stored in a private cloud, who protects that? Is it the government, or critical infrastructure? It needs more thought.

Mr. Mayorkas: I would like to consider General Alexander's question further. As more and more of our functions move into the cloud, we may need to consider the cloud as critical. We may not know answers to these questions. Some European countries are trying different things. We have been trying different exercises, including against financial sectors. We have tried to have those conversations. There are misunderstandings on both sides about what would be done. We are still in the beginning parts of the process.

We can do what DoD is doing, cyber storm exercises. People will question what the government is prepared for. It might be a way to discuss who does what. In some way, the commission must help get it right. The commission can bring external insight.

Ms. Canegallo: Are there other issues we haven't discussed?

Mr. Chabinsky: Following FISMA reform, DHS was that agency. There seems to be disagreement about that today. Is there room for a process that allows for variance from binding operational directives? Is it the commission's role to recommend the authority for the agencies to say they need a variance and appeal to higher authority? It might help things get done, and not take years doing it.

Mr. Donilon: We did not get to talk about R&D. Is cyber recommended in the R&D plan?

Ms. Canegallo: Is it represented, yes. As to whether it is represented enough, probably not.

Mr. Donilon: What are the range of ideas on the workforce issues range and flexibility to make a single set of recommendations?

Ms. Canegallo: Could you provide your report on constraints?

Mr. Donilon: I would like more information on procurement, when thinking about getting technology timeframes. Regarding the budget on modernization, and regarding a basic principle in terms of long-term investment in cybersecurity, is there a grantee program that would come in with a proposal? Is there a way to give more flexibility and multi-year investments? From a government contracting perspective, from other civilian services, they are not allowed to give this information to DHS, which sounds like a missed opportunity.

What about being flexible and agile with vendors that are in a standardized group, so agencies don't feel locked in to contract and vendor if they want to change out technologies. More research is needed into utilizing and not feeling locked into a vender.

Ms. Canegallo: We really appreciate all of the time you have put into this.

Closing

The meeting adjourned at 5:13 p.m.