INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

Established by the Computer Security Act of 1987
[Amended by the Federal Information Security Modernization Act of 2014]

MEETING MINUTES

October 26, 27, and 28, 2016

NIST

West Square Conference Room, Building 101,
100 Bureau Drive, Gaithersburg Maryland

Board Members Chris Boyer, AT&T, Chair, ISPAB John Centafont, NSA Greg Garcia, McBee Strategic Consulting Jeffery Greene, Esq., Symantec Corporation Patricia Hatter, Intel Toby Levin, Retired Ed Roback, US Department of Treasury Gail Stone, Social Security Administration **Absent with Regrets** Annie Antón, Georgia Institute of Technology David Cullinane, Security Starfish, LLC J. Daniel Toler, US Department of Homeland Security	Board Secretariat and NIST Staff Matt Scholl, NIST, Acting DFO J.P. Chalpin, Exeter Government Services, LLC Robin Drake, Exeter Government Services, LLC Laura Hatzes, Exeter Government Services, LLC

Wednesday, October 26, 2016

The meeting opened at 9:24 a.m., Eastern Time.

Welcome and Remarks

Chris Boyer, Chair, ISPAB; Assistant Vice President, Global Public Policy, AT&T

Members of the Information Security and Privacy Advisory Board

The Board members provided brief updates on their activities since June 2016.

Mr. Boyer testified before the Commission on Enhancing National Cybersecurity in July. The work the commission is doing is important. The other big issue is the internet of things and the recent attacks. The Board can provide thought leadership in this area. The Board will be looking to examine how to improve policy. Security is, and will be, a central issue in the internet of things. Devices are being used to create threats to critical infrastructure.

Recent malware attacks have been launched from devices made in China. The Board asked, what

is the role of government, and how do we incentivize manufacturers to create devices that are sold to consumers, but are also being used to create threats by third parties. There have been hacks on the DNC and other government entities. The board can examine these areas. International also plays into the scenario.

Mr. Roback noted PPD 41 came out a few months ago. They have continued the program conducting exercises with the financial services sector, and held an exercise with energy sector as well. They are planning for the 2017 cyber initiative within Treasury. The initiative crosses all Treasury bureaus including IRS. The Financial services sector is also included. G7 published eight elements of cybersecurity. There was an announcement on Monday this week of FS ARC (?) for sharing information. It is a private sector initiative with government participation.

Ms. Stone reported they are involved with FISMA work at this time. They are looking at metrics to move away from paper, and get to core questions of how well agencies are protecting themselves.

Ms. Dodson (NIST) noted the Information Technology Labs (ITLs) have been very busy. The board will hear more about these activities over the next few days. Mr. Scholl (NIST) noted it has been a busy time in quantum resistant cryptography and light weight cryptography.

Mr. Centafont noted the National Security Agency (NSA) is looking at new and emerging technologies. The financial sector is coming to NSA on relevant topics, which has been good. Mr. Garcia's firm has a new name, Signal Group. They are working on a state cybersecurity preparedness coalition.

Dr. Charles Romine, Director of Information Technology Lab, NIST

Dr. Romine welcomed the board to the NIST campus, and spoke on information technology lab (ITL) context and direction. The ITL mission is cultivating trust in information technology and metrology through measurement standards and tests. Metrology is used to help labs improve their measurement science. There are concerns with balance between new research, allied IT research, standards development and technology transfer.

The mission of the National Cybersecurity Center of Excellence (NCCoE) is to build trust in the digital economy and accelerate adoption of standards-based cyber technologies. There are over twenty private sector partners at the center, and many other collaborators across multiple sectors. The new facility has room for twenty-three labs.

The National Strategy for Trusted Identities in Cyberspace (NSTIC) builds trust in the digital economy through trusted digital identities. Pilots in the program are ongoing. Last year, the appropriations bill for the NSTIC was folded into the NCCoE budget. It is a natural partnership that will produce strong results. The cryptography program has been active since 1972, building trust in globally interoperable encryption standards. We are working on building internal capability, and have hired two new Ph. Ds., as well as additional guest researchers. We are increasing international engagements, and broader communities including universities. International activities have included Belgium, Germany, Canada, and others.

NIST policies have been published. The most notable is the NIST Cybersecurity Framework. The cybersecurity framework is the most successful part of the executive order that created it. Our

goals are to manage and reduce cybersecurity risk for owners and operators of critical infrastructure. There is a minor update to the framework scheduled for winter, 2017. Thirty percent of businesses today use the framework in whole or in part. It has been translated into Italian, and other countries have expressed interest. Adam Sedgewick (NIST) has travelled to at least a dozen countries. NIST is partnering with the Baldridge Framework for Excellence in the cybersecurity framework to provide a self-assessment capability.

The Presidential Commission on Enhancing National Cybersecurity is on schedule to meet the December 1, 2016 delivery date to the President. The recommendation content in the report is not public at this time. Some activities of the commission will be discussed during the course of the Board's meetings this week.

Priorities for the NIST labs include:

- Cybersecurity and cryptography; reliable computing, how we help organizations to create less vulnerable software;
- Internet of things; there are large privacy impacts with delivering capabilities and preserving privacy; and the National Strategic Computing Initiative. NIST is one of the founding agencies;
- Machine learning and artificial intelligence: There are some initiatives in machine learning; initiatives in artificial intelligence are coming. How do we secure systems we don't understand? It brings a new level of complexity that has not existed previously. Such a system will exhibit emergent behavior. The question becomes how to establish the behavior we want.
- Transition planning for a new administration. We are working to ensure whomever is next will have the tools to go to the future. There will be a new NIST director at some point. We hope the priority for cybersecurity will remain.

National Telecommunication and Information Administration (NTIA) Internet of Things Report

Travis Hall, Domestic Policy Analyst, NTIA, US Department of Commerce

Last spring there was a request for comment on the internet of things. A workshop was held September 1, 2015 to get more details. Over 130 comments were received, and most were substantive. A green paper is being developed based on that content. Green papers often lead to white papers. The administration change makes the path to a white paper less clear at this time, but it is a starting point for further conversations. A full draft of the paper is in review now. The request for comment is the roadmap for what was in the paper. Cybersecurity policy, infrastructure and standards came up frequently.

It also raised questions in terms of the benefits and challenges of the internet of things. Internal deliberations for the Department of Commerce are also going on. The general result is that most likely the internet of things will result in new policies, or policy changes.

Last week was the first multi-stakeholder meeting to talk about processes. It poses topics to the broader stakeholder community, and facilitates the resulting discussion. There are five working groups: creating a communication plan for the internet of things; working on standards for patch –

ability; creating a platform for patching to help reduce costs and increase the capability to patch, including orphan devices.

The next meeting will be in the summer, allowing the groups time to work. Work is being done on transparency in the internet of things devices to give consumers understanding of what the device can or cannot do in terms of security. There is some overlap with vulnerability disclosure. The NTIA processes do create results that tend to become branded NTIA best practices, but really NTIA's role is to facilitate. It is not expected the outcome will be an NTIA product. Consensus on the idea can benefit everyone.

It can take a long time to foster real change with multi-stakeholder processes. The internet of things presents a great danger. How can we move more quickly against this danger? The NTIA itself does not have regulatory authority. The harder mandatory requirements will not come from NTIA.

The NIST framework is a voluntary framework, because in security, one size really does not fit all. Many devices do not have connective capabilities, and will not need patching. Patch-ability cannot be the sole answer to the problem with connected devices. The long game has to be considered, and how do we create a market for security? Transparency is key to allowing security in the market to actually happen.

Examining the models of other industries may be helpful in cases where there is danger to consumers. The Chinese manufacturer whose devices were involved in the attack on Dyn did issue a recall. The issue occurs in the case where companies have gone out of business. Who then issues a recall in that case? It becomes very complex. There is also the issue that the harm is not necessarily being done to the consumer. The harm may be caused by a completely separate third party (as in a distributed denial of service (DDOS) attack).

IT security may be left up to boards of directors. The nuances of cybersecurity may be lost on board members whose expertise is not in security. Management may not want to talk about cybersecurity. It may take a change to make it a necessary part of conversation with management. It becomes a means to have that conversation. People are now starting to pay attention to cybersecurity. There are better ways to talk about it now.

Has the impact of patching in different environments been considered? Pushing out patches may cause unexpected consequences. Down time for devices being patched needs to be considered. It is ok for some devices, but not others. The goal of the process is trying to create transparency of practices. The consumer should know devices will be offline for maintenance. If consumers know when devices are patched, they can be better prepared for consequences, and have a greater understanding of what may be happening on their network.

There are many good actors who recognize the needs in cybersecurity, such as Mudge and others. The question becomes, if people are to be responsible for reasonable security, what about the other element? It only takes a few devices acting maliciously to have a disproportionate effect.

Is there thinking about particular domains in the green paper? The paper takes a very broad view. The internet of things may be more of a trend than specific technologies. Privacy concerns for

industrial IoT are very different than for the consumer internet of things. They share some areas, but are still different.

The board is supportive of the NTIA efforts. **(Chair)**

National Cybersecurity Incident Response Plan (PPD 41)

Bridgette Walsh, DHS National Protection and Programs Directorate (NPPD)

Dr. Neil Jenkins, DHS

Ms. Walsh will be discussing Presidential Policy Directive (PPD) 41 that was released in July. The public engagement period is now going on. PPD 41 laid the framework for the National Cyber Incident Response Plan (NCRP). The President and the administration have worked on PPD 41 for a year. It establishes how the federal government will respond in a cybersecurity incident with intelligence support, and describes how the federal government will organize itself. The plan came from many private sector requests for this type of information. The National Cybersecurity Incident Response Plan is the outcome of those requests. The goal is to get it to the White House prior to the inauguration in January so that the current Secretary is able to sign the plan.

The plan designates the Department of Justice to act in response with partners such as the FBI and others. The asset response covers the bulk of the plan. It is led by DHS and the National Cybersecurity and Communications Integration Center (NCICC), the cyber-center for the federal government and others. The coordination element must exist across the government. Unity of effort is needed. We need to do a better job of coordinating between and among federal elements. Sharing responsibility has now been put in writing in PPD 41. It is a collective mission and responsibility to respond to issues and incidents that happen.

The NCRP is open for public comment until next Monday. It gives definitions for cyber incidents and significant cyber incidents. Incidents happen many times a day. The plan attempts to separate what is significant from those daily incidents. Offices have been directed to use the schema so that everyone is defining and rating things the same way. We encourage industry to use the schema at the ISAC and ISAOs that will be starting up shortly. The hope is to develop a common language. The schema was used this past week during the DDOS attack. The actual assessments from the attack may or may not be made public. The schema has been in use for a while.

It is uncertain if the schema mapping works well across different infrastructures. The health care sector asked DHS to work with them to define what constitutes a significant incident. Every sector should attempt to do this. It is a good activity for sector ISACs. There has been no negative feedback throughout the process on the schema itself. It is good even for sectors to gain specific understanding for impacts to those sectors. It represents progress across the board.

The government schema may assist in making sense of information. It is a major shift as the schema was only made public in late July. Everyone at the policy level recognizes how sectors and companies choose to use it will be determined in time. Some companies have the picture because they have been responding to incidents for a long time. There are others that are not as far along. The public comment period has provided topics of consideration for cyber incident plans to state and local governments and other entities. It hoped that sectors will be engaged in these types of

activities.

Sectors that have been hit more publicly have been forced to make advances in this area. Information sharing in this setting advances entire sectors. Formerly, there was in-sector information sharing, but not to official entities. The financial sector has been a leader in sharing information for the good of the entire nation. The financial ISAC now has eight thousand members.

Triggers to activate the schema are a critical issue. It is hard to differentiate between a daily DDOS attack and an incident that attacks an entire sector. The trigger event should be reached rarely because it reduces the response effectiveness. The cascading DDOS attacks on financial institutions may fall into that category. Getting the trigger right has to be part of the plan. The NCRP and the schema will be an important part of Cyber Storm 6 to be held next year.

Decision making in machine-to-machine sharing will still require human participation. There are concerns about preventing incidents in the upcoming election. Is there a policy that covers coordination among agencies? It is not certain. It is something that involves the states. There have been conversations with state officials offering cooperation and resources. It is classified as a national security event, and is treated as such. We offer the same services we offer for any other major event.

The NCRP is broken up into several sections including shared responsibilities, resources, risk based response, national planning frameworks, resources for state and local governments, and others. It defines mission areas, and response and recovery, and aligns with the national mission system. The cyber side connects to more physical terminology. It becomes understandable, at least at a basic level, to all. There is a new section on capabilities. The plan is not intended to be a directive-type document for the private sector. It is for the federal government. It should impart ideas for what tasks need to be done.

While it is a U.S. plan, there are international elements. Even if the incident is in the U.S., there is still an international response. FEMA assisted with the development of the plan. The physical side and the cyber side report to the same person, the President. It allows for greater connection and overlap. If events and consequences overlap, there could be two UCGs. They can unify or coordinate as circumstances require. It is a national plan, not a government plan. The communication sector has had a lot of discussion. There are ongoing calls to share information. Calls last week worked well during the attack. It seems a good process.

The need for a plan has been ongoing. Having a plan for the next administration is important **(Chair).**

It is the goal to replace the interim version from 2010 with an official plan. We are working very hard to accomplish the goal of having a signed plan by the end of the year. Great work is being done, and it deserves to be published. The goal is to have publicly adjudicated and approved the 2016 version on an interim basis. A version of the report is online.

L-U-N-C-H

Information Sharing Analysis Organization Processes

Michael Echols, CEO of the International Association of Certified ISAOs
Matthew Shabat, DHS

The International Association of Certified ISAOs held a series of sessions to understand priorities, and in-person public forums at the University of Texas, San Antonio (UTSA) in spring, 2016. There were also public webinars to establish working groups to establish focus areas. The NIST 100 series publications establish guidance for ISAOs. Other publications establish relationships with the federal government.

Publication 100-3 contains operational guidelines. Others provide information on privacy and security. There is an analysis component that is discussed in the 500 series. Publication 600-2 focuses on the role of government. Others focus on SLTT. The 700 series focuses on global information sharing. The first set was released on September 30, 2016.

There was a session to introduce the public to the documents. From the DHS perspective, there has been a lot of interest in the last six weeks from state, local, and international partners. A European partner was interested in setting up an ISAO for critical infrastructure, particularly for ports. They identified a hundred different ISAOs that they had interest in creating.

A state national guard was interested in working with utilities in an ISAO to set up sharing relationships. We have heard of franchisor/franchisee relationships being set up. There have been instances of breaches at the franchisee level that affected the franchisor; hotels and restaurants being examples. There is a lot of discussion of sharing between ISAOs and government or individual companies and government. The concept of an ISAO is designed to help a particular community establish capability in an area of interest.

Michael Echols, CEO of the International Association of Certified ISAOs

Mr. Echols has been working to help organizations understand information sharing benefits everyone. Everyone has the right to protect themselves as they choose within the law. The most progress has been made through education. Different mindsets have been the biggest inhibitor to progress in this area.

Everyone has a different definition of cybersecurity. It is an opportunity to advance understanding and raise awareness. ISAOs are really platforms. The meetings focused on areas in cybersecurity that the ISAO can address. People have not recognized the opportunity in ISAOs. They did not recognize the opportunity in the Cybersecurity Information Sharing Act (CISA) for ISAOs. The concept of due care is gaining understanding and acceptance. Companies are looking for something to be part of, and create the ability to show due care. The private sector can drive the government to do better. In this thinking, everyone will improve.

What is a certified ISAO? Certification is not necessary for ISAOs to exist. It depends on where the community wants to be. Certification verifies the group is a legitimate business entity. The whole purpose is to allow a community of interest to come together and share information in the way they choose. The value is based on what the group is gathered together to accomplish. There are some rules that govern the group, but what is being shared could be a range of things.

DHS will partner with all information sharing organizations in a sector. It will not turn away an

organization wanting to share information. DHS vets organizations for fit or potential benefit from the information. Organizations can focus on information or analytics. DHS shares with domestic and international entities. DHS also has automated indicator sharing. As soon as information was received it was sent out. In the future, there will be ISAOs of experts who look for certain types of indicators. ISAOs would receive indicators of interest to that group. The ISAO would do the analysis, and return information to DHS. Some groups may want information instantly, whether vetted or not; and some want perfectly reliable information. It is a challenge to handle both.

How is law enforcement plugged into this activity? ISAOs can act in the same way as neighborhood watch programs. Law enforcement is often not familiar with cybersecurity. In the future, ISAOs will develop relationships and knowledge with local law enforcement. There is an opportunity here, but we have to see the larger picture. Classified information is also an issue. Some ISAOs may have classified members. The second piece is law enforcement information, how will that be handled in terms of sharing.

How does this fit with other information sharing efforts? The goal is to align it with other efforts from the beginning. We want to receive information from public and private sector entities. With automated indicator sharing, many are sharing automated functions on behalf of their membership base.

The hope is the ISAOs will focus on all the information being moved, and provide analysis based on communities of interest. They may only look at indicators from sectors of interest. ISAOs can fill in the gaps where ISACs don't go. It can become an issue of information overload. How is that handled? There are no requirements today. Once the data comes in, and the requirements of what to do get developed, the systems to make things easier can be created.

Communities of interest may keep information within their communities. How is that dealt with? Things do not happen in isolation. Companies will start to see the opportunity to have their own ISAO that covers their supply chain. This is what is about to happen. Large companies can have thousands of organizations in their supply chain. It becomes complex very quickly. Any entity in a supply chain can be a vector in an attack. It's not a small undertaking for an ISAO.

The ISAO has expanded on the success of the ISAC. It is important because information is more robust to share across sectors. Part of the next series of information sharing documents create a pull between waiting for there to be more ISAOs, and making information available sooner. There is some sector-specific activity now but the path forward is encouraging.

Some agencies and others don't want to deal with this issue at all. There is a credit union ISAO. The board is made up of CIOs of credit unions. They are getting terrorism information, but not cybersecurity. It is not only a centralizing influence, but also means working with government. Centralizing information lowers risk for everyone. More people will participate in sharing over time. Progress is being made, and more groups are in testing with indicators. Indicators are coming by email and disk. It is a recent uptick in activity.

Legislative Update Panel

Stephen Vina, Deputy Chief Council, Senate Homeland Security Government Affairs Committee

Liam McKenna, House Oversight and Government Reform

Greg Garcia, ISPAB, Moderator

Please provide an assessment of what types of progress has been made from the perspective of Capitol Hill for the community as a whole. Include predictions for 2017, etc.

Liam McKenna, House Oversight and Government Reform

The focus areas for the House Oversight and Government Reform Committee are privacy, acquisition, and emerging technology. It includes the 113th Congressional update to FISMA, the omnibus bill that included the Cybersecurity Act, and information sharing. Going forward, there is a lot for the Executive Branch to look forward to. There is the December 18, 2016 deadline for the Cybersecurity Act. The December first deadline for the Commission on Enhancing Cybersecurity is also coming up. These are important activities.

The IT Modernization Act is also a focus. There is awareness of the issue of aging information technology and the need to fix it. There is good support for the bill. It was one of the President's goals. There are still millions of lines of COBOL code running in the federal government.

Stephen Vina, Deputy Chief Council, Senate Homeland Security Government Affairs Committee

Mr. Vina works for Senator Harper, the ranking Democrat from Delaware. Developing a cybersecurity workforce will be an ongoing theme for the next number of years. The challenge is bringing people up faster and paying them more. Recent bills have clarified the authorities between DHS and other agencies. It has helped to foster a continuous monitoring standard. The 114th Congress codified NCICC. For the 115th Congress, it was the information sharing bill. There is important work on improving cyber hygiene across the federal government. The current Congress focused a lot on the OPM and IRS breaches. There have been letters on ransomware and other issues. December 19, 2016 is the 1-year deadline for agencies to have implemented EINSTEIN.

Senator Harper sent a letter to the nation's governors to encourage them to take advantage of the cybersecurity tools available from DHS for their elections. The reorganization of the National Protection Programs Directorate (NPPD) is a big topic. The hope is something will happen this year. If not, it will come to the next Congress. The bill changes the name to reflect what they do more concretely, and changes the mission as well. We are working with all parties to arrive at a situation approved by everyone involved.

There were four separate bills in Congress related to cybersecurity in 2016. Most passed the house, and are in committee. There must be a mark-up process. Some touch on SLTT capabilities and needs, helping states to secure their systems, as well as other areas.

There is a lot to be done. Congresses have thought in terms of accomplishing certain goals such as FISMA, information sharing, and others. There may not be a clear objective for the 115th Congress. Oversight is key for information sharing. It is also important to talk about metrics.

The 2015 Symantec report compared threat feeds. It found most (95%) were unique. With real time threat information sharing, the Symantec report made the point that within 24 hours a quarter of threats spread from the originating machine to machine one. Forty percent spread within an hour. It makes it clear why sharing days or weeks later is not useful. We want to see if there is more sharing and by whom. It will not solve advanced persistent threats. Signatures will not be detected because they change every time they deploy.

Heuristics and behavior-based detection are key objectives. In the last day or two, the first automated semi-truck on the road started delivering beer. Are recent events part of the discussion? There is emerging technology, but not an area of interest. Mr. Vina is not speaking from the viewpoint of Senator Chaffitz. We need to be careful of over-regulation.

Mirai (malware used in the recent DDOS attack), used consumer devices to affect the global web. It has changed the understanding of the threat. For Census 2020, the census chair has stated the intention to conduct rigorous oversight. Mobile devices were tried for the last census, but did not work well. The system has since reverted to paper. Subsequent tests for mobile have gone well, but it's not ready for prime time as yet. Decisions need to be made. The technology must be ready in 2018. The Australia census issue is informing concerns now. We must make sure the testing is robust for the 2020 census.

The commission report to the next President should have a number of important areas such as a commitment to cybersecurity threats and the budget to support it. There are some big issues in cybersecurity. We look for a way forward on encryption, data breach notification, and the internet of things will need to have a place in the report. Correct attribution following incidents and the correct response is important.

There are additional areas that need to be in the report: finding the right role for the government response, and developing a clear understanding is important; developing an encryption model for quantum computers; and increasing awareness of the tools available to state and local governments. DHS must have resources to make that assistance available. It becomes a combination of funding, people, resources. Many times assistance from DHS is free.

It will be helpful next year to understand what areas to focus on. Emerging technology, privacy, and others are in the mix. We recognize the need for better visibility in federal networks. These are things we should be able to do. We are getting better data and updates. Continuous monitoring type programs will assist in getting more data and better updates.

We have been trying to link ISPAB as a Board to current topics. We may want to examine how the ISPAB timeline works with agency budgets in order to anticipate actions, and time responses accordingly. **(Chair)**

Board Consideration: Timing ISPAB actions with agency budget considerations and planning.

B-R-E-A-K

Ransomware Threat Information Briefing

William Wright Symantec Corporation
Iliana Peters, Health and Human Services, Office of Civil Rights Senior Advisor for HIPAA Compliance and Reporting

Symantec publishes the annual security threat report. Ransomware, and the evolutionary path of ransomware, is another topic in the news. Ransomware has been around awhile. Misleading apps were an example of ransomware that first appeared in 2005. Misleading apps were replaced by the fake antivirus in 2010. It was successful, but people were becoming more aware.

Locker ransomware became the next type to become prevalent. It looks official, like it's from law enforcement. It threatened legal action, and people paid. It worked for a while, but people caught on. Today, crypto-ransomware is prevalent. It encrypts files, and people must pay to get files back. It dropped off because criminals couldn't figure out how to get paid. Bitcoin is now used almost exclusively in crypto-ransomware attacks. There has been a thirty five percent increase this year.

It is still profitable for attackers make ransomware attacks. There is easy access to encryption and cryptocurrencies. There are effective infection vectors. Keys are now unique for each infection. Bitcoin is difficult for law enforcement to track. Criminals have adopted advanced attack techniques. They are using the same techniques as state sponsored actors.

Currently, there is ransomware as a service. It is inexpensive, and even has a 24-hour helpline. The creator takes a percentage of every time it's used. The number of new malware families has increased in the last few years. The average ransom amount has doubled in the last year alone but that number does not include the true costs: incident response, data loss, loss of life and others.

Ransomware infection most commonly occurs by email with a script file. Office and social engineering, malicious macros, and infected web sites are other methods. Victims are everywhere in the world, but the U.S. has the largest share. Consumers make up most of the victims, but organizations are also targeted. Advanced techniques include infiltration, reconnaissance, lateral movement, and stealth. Ransomware now occurs on smart devices. IoT smart watches and TVs are being held for ransom now.

There is now an evolution to corrupting backups. It presupposes backups are continuously connected. Continuous connection helps but is not necessary. What is the current advice from the FBI on responding to a ransomware demand? Don't pay. The criminals count on willingness to pay. It is not guaranteed stolen data will be returned, even if the ransom is paid. Paying the criminals enables them to continue perpetrating attacks.

Ironically, there seems to be honor among thieves. Many act do professionally and return data when ransoms are paid. They care about their reputation. There are also instances of hitting and moving on. The risk of sending a key is low, so why not be a "legitimate" criminal. Healthcare is not as big business for ransomware as may be thought.

Iliana Peters, Health and Human Services, Office of Civil Rights Senior Advisor for HIPAA Compliance and Reporting

The Office of Civil Rights functions as the regulators for HIPAA. The office recently published guidance for ransomware and HIPAA rules. It tracks statistics and publishes them on the website. There are monthly newsletters including threats in the health care sector. The Office of Civil Rights worked with NIST to do a crosswalk to the HIPAA rule. It uses the NIST framework and HIPAA security rules. They also published a document on cloud computing. Cloud vendors are generally covered by HIPAA.

The guidance, developed by DHS and HHS, walks through a number of areas. It defines ransomware for the purpose of HIPAA. When a hacker deploys ransomware, they also tend to deploy other types of malware at the same time. It may be present in systems long after the ransomware attack is resolved. Most ransomware deletes files and recreates them in the container. It is often true returned data is not generally the original data.

The Department of Justice has jurisdiction over the criminal provision of HIPAA, and criminal individuals who use or steal personal health information (PHI) for personal gain. We also explain how the requirements of the HIPPA security rule prepare to detect and report malicious malware. It explains about ransomware, what to do and whether to coordinate with law enforcement. It gives a definition of "breach". Breach notification is required of HIPAA entities. Any use or disclosure of personal health information (PHI) not covered by the rules is considered a breach.

Ransomware does constitute a breach under the law. The media must be notified if the PHI of more than 500 individuals are involved. There has been a rise in hacking incidents. Presently, ransomware represents 14 percent of IT incidents. It is meant to be an incentive to do risk analysis.

Generally, health care entities are in the business of treating people. They don't see IT as a primary responsibility. They would rather invest in new treatments, etc. It is only now a priority to protect data to the degree HIPAA requires. All health entities need to do a better job at data security.

Are patient information networks are connected to the whole hospital network, or is the patient information separate? Some patient networks are connected, some are separate. Outside entities often handle billing in its entirety, as an example. Breaches are presumed, and reporting is required unless there is proof there is a low probability data was compromised. In that case, there is no requirement to notify.

Smaller financial institutions are migrating to service providers. Is this happening in the healthcare sector? Can ransomware work in the cloud? It can happen. The financial sector has a good history with working with its smaller members. The financial sector is significantly advanced compared to the healthcare sector. They have adopted the approach of helping everyone improve.

In terms of service providers, business associates may or may not be compliant with HIPAA security rules. A security incident in terms of the HIPAA security rule, is something that doesn't rise to the level of a breach. A failed malware attack constitutes an incident, and should be reported. A ransomware attack is an incident whether or not it is able to capture data.

Ransomware guidance is available at
http://hhs.gov/sites/default/files/Ransomwarefactsheet.pdf
Other information on breach notification and reporting is available as well.

The root cause of a majority of breaches are caused by lack of basic security measures. The MedStar attack was ransomware. We can't make further comment at this time. Compliance with the HIPAA rule is required. There is authority to issue fines for non-compliance incidents. Entities can settle for a portion of the required civil fine, with a correction action plan. They are monitored for a couple of years following incidents to ensure compliance.

Can an entity be compliant and still be open to an attack? It is possible. The education industry is also vulnerable. There is a data integrity project at NCCoE. We have received advice from companies on how to keep data safe.

Public Participation

No public participants registered in advance, or were present to speak at the meeting.

Review of Wednesday Actions

The board postponed review of actions until Thursday.

Meeting Recessed

The meeting recessed at 4:22 p.m., Eastern Time.

Thursday, October 27, 2016

The meeting opened at 9:03 a.m., Eastern Time.

Recent Cybersecurity GAO Reports and Findings

Greg Wilshusen, Director, Information Security Issues, GAO

At the request of the House Energy and Commerce Committee, GAO released a report in August, 2016 on the role of the CISO and how it relates to statutory requirements. It also identified key challenges to fulfilling CISO responsibilities. They interviewed CISOs, and surveyed 24 agency CISOs. There are a number of responsibilities and requirements defined for agencies. Many of these have been delegated to CISOs. They found more than half of the agencies surveyed have not defined a role for a CISO even though agency policy stipulates there must be a CISO. GAO made recommendations to agencies based on the individual findings for the agency.

Eighteen of 24 CISOs surveyed said they tension existed between the role of the CISO and system security. Thirteen out of 24 felt coordination with component counterparts was a challenge in the organization. The report noted oversight by contractors was often limited. Security controls were not reviewed by contractors. Assessments were generally not comprehensive. It has been a challenge for GAO in assessments and within agencies.

There is a movement to move more information processing capabilities out to the cloud. GAO is trying to determine how many cloud implementations in the government have not implemented EINSTEIN. OMB used to report the number of full time equivalents (FTEs) involved in security activities. The number used to be broken out between federal and contractor FTEs, but it is no longer defined that way.

Are there challenges between the agency level CISO and the component level CISO? Some authority for the position comes from budget. Different risk profiles call for different centers of control. The recommendation to OMB was to clarify the role of CISO in terms of roles and responsibilities. In the Federal Information Technology Acquisition Reform Act (FITARA), CIOs are required to have a greater role in IT acquisition and other areas. The effect is still to be determined. It does come back to budget. Agency operational divisions can be very different. Where requirements for consistency exist, there is accountability. It has become true that CISOs are moving up in organizational structures.

It has been a theme in ISPAB discussions that the CISO role needs to be elevated to the top level of the organization. OMB is the only organization that can change the culture where security is relegated to lower levels. If infrastructure security is moved outside IT, then it becomes harder to maintain the necessary focus. If there is lack of trust internally, it needs to be changed. Security must be a high priority for CIOs for change to occur.

Oversight of indirect reports or information sharing and security procedures were found to be challenging for a significant number of CISOs. Hiring and retaining qualified staff and resources were also cited as challenges in the report.

Civilian agency spending on information technology was found to be about 8 percent on average. Actual spending ranged from two percent to eleven or twelve percent. FDA was cited as the agency spending the least on security. Since the findings filed by GAO, FDA has made significant progress in taking care of vulnerabilities. New leadership has helped in implementing necessary changes.

There may be a staggered release of limited use reports in the future. The GAO report can be used to motivate change in agency practices and spending. Now, it becomes the role of the Federal CISO to create change. Mr. Wilshusen has not seen the roles and responsibilities of the Federal CISO as yet. He anticipates working with the Federal CISO office regularly in the future. There has been a much greater focus on cybersecurity coming out of the Federal CISO office. They have made a number of actions to raise the importance of cybersecurity within OMB.

Agencies need to focus on training recommendations. Training is a key aspect in making sure staff understand roles and responsibilities. Everyone receives security awareness training, but there is more to making sure staff is fully trained. Tailoring training helps people meet specific roles and responsibilities.

Agencies have not moved further along in intrusion detection because there is a lack of ISPs who can support EINSTEIN 3a. Agencies looking for internet service providers in 2015 did not have many choices. There are more service providers available now. Agencies must understand the benefits and limits of service providers, when considering how to implement intrusion protection.

Cyber audits are ongoing and planned in advance. Links to most are available. Questions are welcomed at any time. All audits are requested by chairs or committees, or are mandated by legislation. GAO will be reporting on OPM in April, 2017. There is a government-wide review of cyber risk management. There is assistance available for agencies to assess risk. GAO will examine how well this guidance is being used.

There will be a number of things being examined in the FedRAMP review. All agencies will participate, and companies that provide cloud services to the government. They will examine the user and provider viewpoints.

GAO will also look at the federal cybersecurity workforce. All agencies will participate, as well as companies that provide cloud services to the government. The audit will identify gaps, and needed skillsets. GAO will also examine emerging technologies in the longer term. There is a lot of work across agencies to assess financial system security.

Work was started on removing social security numbers from Medicare. The effort started in 2007, and is still going. GAO is looking into getting the work completed in the nearer term. When is DoD included in the audit cycle? Defense is included depending on the scope of the audit and what the mandate from Congress is. GAO has reviewed the setup of Cyber Command. They have looked at insider threats, and use of utilities. The audit may come from a request or government wide review.

CNAP Update and Plans for Transition of Effort

Trevor Rudolph, OMB Office of Cybersecurity

Mr. Rudolph will provide a brief update of CNAP, how it will carry forward to the next administration, and how the Board can assist. It was released by the President in February, 2016. The Office of Cybersecurity found the federal government had three issues: fragmented management, legacy equipment, and workforce issues.

Progress has been made on the issue of fragmented management. It deals with protection of high value assets (HVAs) and centralized IT services for small agencies. It is the first time the government has inventoried all its unclassified assets, and placed values on those assets. There will be guidance from OMB to extend the program for the longer term. We have decided to target certain initiatives to make sure there is foundational policy to ensure existence in the future. There will be more specific direction to identify, protect, and remediate issues. It is something that will evolve over time.

We are looking at centralized services for smaller agencies. If we centralize email, networking, and other services, we will be able to save on cost, and receive other benefits. There are critics of the centralization approach. It creates a greater risk of drawing attacks on a larger target. The idea of centralizing risk can be dealt with. There is not a perfect answer yet, but continuing in the status quo is unacceptable. The problem has not been people or technology, but budget. The message to the next administration will be that centralization is the correct path. There must be a coordinated and budgeted effort to proceed and make it work.

OMB plans to release guidance on IT modernization. It will provide guidance to agencies on prioritizing what needs to be replaced, followed by oversight. There has been guidance on workforce. Is it enough to coordinate existing efforts, or to go bigger? OMB came very close to its goal of hiring 6,500 cybersecurity experts this year. OMB would like to augment the scholarship program. It allows managers to make conditional offers to students. At a recent job fair, DHS handed out three hundred offers on the spot. Something dramatic must happen to effect real change. Recruiting may need to start earlier to increase effectiveness. There needs to be an emphasis on the mission to protect, as opposed to developing the next big thing. Agencies have the opportunity to work with the NICE program. A cyber academy has been talked about during the current administration, but the time has not been right. Perhaps 2020 will be the right time.

How does funding work for assets that are deemed high value after the initial assessment? DHS is implementing teams to provide agencies with assistance. The expectation is that agencies will make their own valuations. The CNAP is progressing, but needs the help of Congress in the next fiscal year. There is Congressional interest in the revolving fund (ITMF), but there is also interest in capital funds for agencies. There is support for modernization on the Hill, and a good level of bi-partisan support for this issue. The mechanism has to be authorized, then the decision must be made on funding.

(Chair) How can the Board weigh in on priorities for the next administration? If the board can assist with advancing the proposal, it will assist. The Board can send a letter to the Hill, and to the cyber commission. The Board can think about language that emphasizes modernization, and moving forward rapidly. Proofs of concept on new or emerging technologies may help create ability to plan further in the future.

Legacy issues can be solved with centralized services. Assistance is currently offered to agencies at no charge. We may need to look at the Federal CISO role in terms of a centralized system. The Federal CISO would have expanded authority. It is too early to tell how it has been received at the White House. Others will ultimately make that decision.

It may be time to update FISMA. If shared services are going to be addressed, the section on agency responsibility must change. Does it make sense to have a separation between national security and non-national security systems? A FISMA update is due soon. Some services may be given to external providers. We want to avoid developing the next generation's legacy systems. The commission is working through developing specific recommendations for this area.

BREAK

IoTSecurity and Recent IoTDDOS Malware

Andrew Kennedy, Senior Program Manager, BITS Financial Services Roundtable
Dr. Manos Antonakakis, Georgia Tech School of Electrical and Computer Engineering (via conference call)

The presentation today comes from a joint work with additional researchers, sponsored by NIST, DARPA, and Comcast. What is considered to be the internet of things? Definitions have been proposed by government, industry and academia. For this purpose, we do consider consumer devices and home automation devices that use the network to reach out to the rest of the internet to be part of the internet of things.

Laptops and mobile devices are not considered as internet of things for this presentation. What are the problems with Iot? It involves trusted devices in networks. It increases the attack profile of networks. There is less than good understanding of how network protocols and cryptography should be used. It opens holes to user security and privacy. It is hard to track the growth of IoT devices in the context of a large network. It is important to measure the growth. It helps the community to anticipate events. How can growth be measured? The network can be set up in such a way that networking events can be clearly attributed to devices. Devices run for long periods of time. It is critical for measuring their behavior in real networks by collecting IoT network indicators that can be uniquely attributed to certain classes of IoT devices.

IoT devices tend to communicate with many domains and locations on the internet. What protocols are used? Using devices in the IoT lab, the by-volume communication patterns from the IoT devices can be seen. It is interesting to note, devices speak more UDP (DNS) than transmission control protocol (TCP). There are large numbers of internet control message protocol (ICMP) and internet group management protocol (IGMP) traffic too. Many custom protocols exist on top of user design protocol (UDP).

A paper will be published from Dr. Manos's lab with more details than is presented in the table with http and https indicators showing known attacks and problems. Will the known security issues ever be fixed (such as through patching)? Home automation growth has increased dramatically in the last three years. The remaining types of devices have seen steady growth in the last five years.

There are a half a billion DNS lookups per day. These look ups will never go away. It becomes

important to have a way to control these devices. It is a matter of time before the government will issue massive recalls on internet of things devices for security issues. We should consider voluntary certification of IoT devices. Do we need an UL certification mark for IoT devices? There is a desperate need for an IoT security label that would act as an early warning.

How can we ensure devices are shipped with the default password off? How can we ensure that devices are able to accommodate individual passwords? Going to www. Findyourthings.info from the local network can determine if there is a trust violation. ISPs have no knowledge of devices behind routers at home. There is a discussion that could be had about routers, and what could be done at that level. Carriers alone are not the solution to the problem. Manufacturers continue to create devices without security. The problem should not be on the consumer or third party. The ISP community does try to assist its users.

Andrew Kennedy, Senior Program Manager, BITS Financial Services Roundtable

Mr. Kennedy is speaking today about the financial services industry and about distributed denial of service attacks (DDOS). The roundtable works with cybersecurity, fraud, and publishes best practices. Today's discussion will cover DDOS, and the economics of cybersecurity.

There are two fundamental concepts with DDOS that need to be acknowledged: patching our way out of a DDOS attack is not possibly, and devices need to talk to devices. DDOS attacks have a wider effect than may have been planned. There are effects across the board. A holistic model is needed, and the time to act is now.

In the financial attacks in 2012-13, a nation-state was alleged to be behind it. The attacks were notable because they disrupted services. There have been attacks since, but they are being managed (ensuring continuation of services). There were multiple phases to those attacks over several months: the adversary was adaptive, and forced changes to tactics. The attack averaged 65GB/sec., a tenth of what is seen today. Core systems were not affected. It is a significant amount of data. Existing structures worked for information sharing. BITS worked in communicating with the sector. The financial sector supports all its members in the belief that action protects all members. Attacks diminish the reputation of the entire sector. The threat space is never ending.

Economically, it is easy on the attacker, and hard for defenders. Weak passwords, ubiquitous broadband, and malware sophistication make it easier for bad guys. Attackers use every tool available to them. The increase in broadband is a blessing and a curse. The tool used in the recent attack was published. Human behavior still causes problems. Cyber actors often work from safe jurisdictions.

Government has a role, but there is a fragmented approach that is not easy to solve. There is a lot of good activity, but there is no whole government approach. There are fifteen regulators in the financial sector alone. Large efforts are being focused on compliance instead of defense or response. There is a limited pool of talent everyone draws from. The trend to multi-factor authentication is good, but it is still complex, and some simpler way may be needed. Risks need to be determined that are applicable to government and sectors.

Domains are being set up with rules to be a member (.bank or .insurance). The NIST framework

and government exercises are good. The international drive to norms is an important long term effort. Some attacks are due to poor hygiene. How can we work collectively to make it difficult for attackers? Is there capacity to withstand multiple DDOS attacks? We will need to know. People notice how we respond. Are we working toward solutions that will solve the problem? It is hoped we are.

There are many lessons being learned from government experience. We need to know how to get back to normalcy following an attack. There was a recent senior exercise involving CEOs and the White House. There will be some good findings that come out of it. The main thing is to continue doing these exercises. It is a muscle that needs to be worked.

There is talk of security by design. What about architecturally? What can be done about architecture? It is tough to talk about architecture without a leap forward. There is value in authentication. Can anything be done at a device level? Devices do what they are intended to do. Authentication usually involves a person, but is it possible to authenticate a use? It is worth exploring. It is a separate discussion. Some of this happening at the enterprise level. It will translate to consumers eventually.

The trends in botnet take downs are pretty good. Zeus and Citadel were taken down. There is still a legal process involved. The justice system was not set up for cybersecurity. Any botnet is a bad botnet, even if it is not presently acting. Locations of botnet devices need to be determined.

It is important to remember that customers buy solutions. Manufacturers tend to think of features and time to market before security. Consumers do respect a UL label. If the same existed for cybersecurity, it would matter at the point of purchase. There must be something that can be done while these changes are made, like educating consumers to buy better products. It also helps if stores stock the right merchandise. It may be more to getting people to buy the right things. Information on reliability in terms of security can be provided to consumers. Factory default passwords must be changed, and not usable until they are changed. Devices should be patchable by default.

L-U-N-C-H

NIST Update

Matthew Scholl; Kevin Stine; Donna Dodson, NIST

Donna Dodson, NIST

It was just last year the creation of the Applied Cybersecurity Division (ACD) was announced. Previously there was one division, the Computer Security Division (CSD). People were not sure how the program would develop at the time. It has been a nearly seamless transition. The divisions are well connected, and it is a mark of success. We are working hard collectively to institutionalize the culture of working together. It is an important outcome from the inception of the new division. There is an explosion of interest and curiosity about cybersecurity. Being open to new opportunities for collaboration is the lifeblood of NIST. We must now prioritize what is being done, and who we are working with. Analytics and programmatic areas would be of concern if resources were available. Key management and public key infrastructure are very important.

Work in quantum resistant cryptography is happening now. We are considering how to readjust resources in light of these things.

The National Cybersecurity Center of Excellence (NCCoE) is now very strong. The facility opened in January, 2016. There are now 23 labs with active projects in 17. There is an academic affiliates council as well. Much work has been done with secure email. NIST will be presenting at Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG). Another publication that will be coming out in the next few months deals with the medical device infusion device project. All major medical device manufacturers have agreed to work with NIST in this effort.

We are excited to work with the financial service, energy, retail, and hospitality sectors. A number of leaders have expressed interest in working with NIST. It means the center is doing what it was meant to do. We want to look at the center strategically to see what is possible for the future.

Matt Scholl, NIST

Mr. Scholl provided a NIST cybersecurity update. NIST exists to cultivate trust in metrology. NIST will be making a formal call for collaboration in quantum resistant cryptography. We will be moving aggressively on a timeline of four to six years. Light weight cryptography is also an area of interest. There may be need for light weight cryptography. It will not be able to resist long period attacks, but will protect for a short period of time. NIST has finished two workshops. We are looking at cryptography use cases for light weight cases, and whether advanced encryption standards (AES) are useful in this context.

NIST is working with internet engineering task force (IETF) with transport layer security (TLS) updates and elliptic curve cryptography. The latest updates downplay key functions at end points. It allows key management to happen at end points. It is good for point-to-point security, but it poses other challenges. It will take some time to develop roles and standards. It involves end-to-end encryption. There are other issues being raised with cryptography. IETF will have a preferred method for strong security. We're looking at this as a default preferred method for security. It is still a topic of hot discussion. It still has to be determined if options will be allowed or not.

We are continuing to work in software assurance, looking at reducing flaws in software. Are better instruction and tools needed to create better methods? We are looking at NCSI, high performance computing. In September, there was a securing high performance computing workshop. NASA, NSA, the national labs, and others came to NIST. It is very different from classic computing. We brought the two communities together to start the discussion on security for high performance computing.

The next step is machine learning and artificial intelligence. What algorithms can be generated for cyber security? It is a research question now. This is what will be happening in the Computer Security Division for the next few years.

What will be the deliverables? We will be putting together competitions with coding challenges, to develop tool chains. We want to know how well tools help developers create better software. NIST provides an evaluation capability, but it does not compete with tool creators.

Kevin Stine, NIST

Mr. Stine will discuss the Cybersecurity Framework and federal agencies. The NIST Framework is now associated with the Baldridge Framework. It is out for public comment.

Tomorrow, Rodney Petersen will update the NICE program for the Board. This weekend is the seventh NICE conference in Kansas City. A cybersecurity job map for the nation will be announced. As was mentioned yesterday, we have learned a lot from NSTICC in the last few years. There has been an increase in publications based on what was learned in that effort. Publications have come out in the last few months, with more expected in the next few months. There are other publications in process to be published as well. Publication 800-63 (3) is in process. There is much discussion on the direction of that document.

NSTICC has progressed from a pilot program and we have learned much from it. There has been a decrease in the number of pilots, but there have been grant awards. NIST hosted a workshop on privacy controls with the Department of Transportation in September to talk about privacy.

The Privacy NIST IR is in the final stages of approval. The Small Business Cybersecurity NIST IR will also be coming out in the near future. There is also a NIST cybersecurity small manufacturer's effort underway. It has been well received so far. We have a partnership with the engineering lab at NIST to develop the cybersecurity framework in a manufacturing environment.

Baldridge Cybersecurity Assessment Program for Industry

Robert Fangmeyer, NIST Baldridge Excellence Program Director

The Baldridge Performance Excellence Program started in the 1980s to improve quality driven productivity in the U.S. The goal was to develop an accepted standard in conjunction with industry to recognize organizations, and promote use and best practices of awardees. Organizations that incorporated this program showed superior performance. Today, we offer a more comprehensive tool including non-prescriptive leadership and management guidance organization wide.

This program is recognized both nationally and globally as a standard of excellence. The program has been around for about thirty years. Companies with the Baldridge recognition have out-traded the market by 6:1. Independent economists evaluated the overall impact of the program, and found the return was estimated at 820:1. It may be the best known rate of return for a federal program. This program has also been integrated into a number of other organizational processes such as the ISO 9000 series.

Matt Barrett, NIST Cyber Framework Program Lead

Risk management has been integrated into the cybersecurity framework. External participation is needed for the ecosystem to function. The framework has four implementation tiers. The changes help organizations improve over time. It is noteworthy that the cybersecurity framework is not necessary to do well with the Baldridge self-assessment, but it does help. The Baldridge Cybersecurity Excellence Builder (BCEB) combines with the framework for organizations to improve.

The BCEB is organized the same as other excellence builders. Completing the first section informs

the following sections. The second section deals with processes. The tool is a combination of leadership and workforce, and how they align to work with larger strategy for the organization.

In the Baldridge process, understanding performance in the context of results is key. Measuring the right things and understanding what the results say is very important. The categories enable a system approach and view. Processes evaluate the organization's approach and how developed it is. The results show what has been implemented. The draft Baldridge Cyber Security Excellence Builder is available to review on the NIST site. Comments are welcomed and encouraged.

The level of maturity for an organization is evaluated on four different dimensions (approach, deployment, learning, and integration). Trends are examined over time and comparisons performed. Scoring is broken down into reactive, early, mature, and role models.

It has been well received by DHS, and there is interest from the ISACs. A new Baldridge award cannot be created unless it is approved by Congress. Cybersecurity is a component of all the sectors that currently make the award. There has been a cybersecurity element in all the award types since 2001.

B-R-E-A-K

EO 13636 Cybersecurity Framework and the US Government

Matt Barrett, NIST Cyber Framework Program Lead

Kelley Dempsey, NIST

FISMA directed NIST to write guidance for risk management activities. There is now a suite of publications on conducting risk management activities. FISMA differentiates between national security and non-national security systems. The rule is there must be procedures, but they do not need to be the same for both. There has been some confusion on the laws and publications available for federal organizations. There is some perceived complexity due to the number of documents. It makes it more difficult to determine what is relevant. The objective was to bridge the gap between the technical language of the framework and users of FISMA guidance.

The role of the framework was described in broader terms in additional memorandums. The memos were big drivers for uptake of the cybersecurity framework within the Federal government. The framework is not a stand-alone item. The guidance is intended to show how all the pieces work together. The team is beginning its work on the third internal draft of the framework, and work is proceeding. We will be adding an exhaustive mapping of Publication 800-53 Rev 4 controls to the framework. It will be published as supplemental guidance. It falls more in the category of informational, rather than normative. The expected release date will be winter, 2017. The framework is intended to be modular and complementary to the federal risk management plan. It is intended to augment the current process rather than pile on more work.

The relationship between the two seems not to be well understood at present. A communication gap may be causing the lack of understanding. The confusion comes from federal government and senior executives. They are handed ATO packages heavy in documentation which they cannot consume.

Can the board assist in creating understanding? The understanding of the risk management framework is there, but tailoring is required. There are publications available that speak to a senior management perspective. It covers accountability and risk executive functions.

It may also be a language problem. There are many terms in the documents people may not know. Further efforts to raise awareness are needed. People may be confused because it seems like a one or the other choice. From a senior management perspective, there is Special Publication 800-39 to assist with understanding. It maybe this publication is overlooked. There need to be champions in organizations who understand and advocate for it.

Board Review and Discussion

Chris Boyer, Chair, ISPAB; Assistant Vice President, Global Public Policy, AT&T

Letters to OMB and Congress:

1. The Chair is interested in a letter from the Board to lay out priorities for the next administration. A draft was started today. Cybersecurity is a national security. The priorities are that important.
2. Fully staff and support cloud for privacy in US government programs.
3. IT Modernization – support CNAP as a vital tool to jumpstart modernizing infrastructure
4. Centralized IT services of certain agencies (smaller agencies)
5. Clarifying roles and responsibilities of Federal CISO. To OMB and Congress (?) to make the position permanent.
6. Budget for cybersecurity at the national level. Inherent limitations in the current system. Long term view and investment. We are asking OMB to be the budget champion across the federal government.
7. Empower CISO role by elevating importance.
8. NTIA, Commerce, NIST role in the internet of things.
9. Letter on bug bounties

These programs require long term plans. OMB should serve as a champion for this budget. The risk management framework should be promoted as a great achievement. Because cybersecurity is a national security issue these recommendations should have a high level of priority.

Security in software should be improved. The issue with open source libraries is a huge problem. There is also an uphill climb for CIO authority.

Mr. Boyer will develop language for these topics. The meeting tomorrow will start at nine am.

Meeting Recessed

The meeting recessed at 4:00 p.m., Eastern Time.

Friday, October 28, 2016

The meeting opened at 9:04 a.m., Eastern Time.

Continuous Diagnostics and Mitigation V2.0 Update

Martin Stanley, DHS

Matt Hartman, DHS

DHS is responsible for issuing standards and guidance on continuous diagnostics and mitigation v2.0. Continuous Diagnostics and Mitigation (CDM) is also part of this partnership. Information security continuous monitoring (ISCM) is a great start. Publication 800-11 states how to use automated security tools. The NCCoE partnership has developed guidance for implementing ISCM and we have a functioning instance of CDM. There is a big push for ISCM (Publication 800-137).

DCM fits into the CDM structure for people, processes, technology, and tools. This allows us to know about vulnerabilities, what is on our networks, systems, and devices. The 2013 Blanket Purchase Order (BPA) available to state, local, territorial and tribal agencies (phase 1), provides a consistent, government-wide set of tools giving agencies the ability to understand what is on the network. These tools are being implemented across agencies. Subsequent phases have different focus areas allowing for a layering capability. As phases are implemented, tools come online. Additional capabilities will tie them together.

Protecting data became part of phase 4 as opposed to phase 1 or even phase 2 because vulnerabilities are critical and a more enterprise-wide focus was developed. Protecting data is a parallel effort and a high value initiative.

There is an education component for agencies to better understand what ISCM means and to have it implemented. There is also the challenge to do agency-wide tool deployment. Cyber Scope may be replaced for tool reporting. Data reported through Cyber Scope has inaccuracies. Reporting is skewed which leads to an ongoing effort to cover blind spots. System reporting required by FISMA is a conceptual grouping of people, processes, and tools. It's difficult to draw an exact boundary in the network. CDM drills down to the component level.

Requirements gathering is part of the work being done as well as collaboration. The requirements for BOUND will evolve, and may include things like DDOS mitigation. Phase 3 of CDM centers on event management, capturing NIST guidance and reinforcing best practices. This area is challenging for agencies since collecting and analyzing policies is difficult when policies are not in place. The goal is to use information that is generated and implement an authorization capability, which is different from the current system.

CNAP calls on DHS to implement a security engineering capability and to go out to agencies to further secure systems through engineering processes. Agencies receive assistance with acquisitions help such as developing a Statement of Work (SOW) and ensuring security is part of contracts.

The priority is to look at high value assets (HVA) and suggest improvements, focus on reviews,

root cause analysis, and influence progress in the right direction. Establishing collaboration early will not waste time. The team provides recommendations and does not take control of systems. They work with the CISO and CIO under FISMA authority.

How is EINSTEIN going? EINSTEIN is an external control, whereas the controls here are enterprise level controls. There are deficiencies within the budget. Mobile devices, for example, are not covered currently, but they should be covered in phase 4.

There is a dashboard in place to provide visibility and a construct to push down priorities from the administration for agencies to report their status to meet prioritized security objectives. Preparing agencies for ongoing authorization is an added benefit and provides a better way to manage risk. It is a challenge to answer specific questions on vulnerability.

The Heartbleed incident provided a good lesson. Reporting for Heartbleed was a manual process. It was effective, but heavy.. This is a comprehensive program for federal agencies. There are knowledge gaps where agencies need to know how to operate and how governance should look.

Is there a need for additional workforce? There is an effort to bring more people in to add to the current workforce. OPM is meeting with OMB and GSA to develop a cyber workforce strategy to attract, retain, and incent skilled personnel. A lot of security work is done by IT and general personnel. The belief is that organizations need to be willing to provide more training and awareness of requirements and risk. Program reviews should emphasize what's important. There is also a need to enforce that the bulk of implementing software controls should happen in the development process.

DHS Study on Secure Mobility and Mobile Threats

Chris Brown, MITRE

Mr. Brown will discuss development of the mobile threat catalogue. DHS is partnering with NIST, Montgomery County, and the State of Maryland. It demonstrates commercially available technologies that provide protection to organization-issued and personally owned mobile platforms.

The goal was to work with different sectors such as energy and health to help with cybersecurity needs. We learn and try to demonstrate solutions in the lab. Organizations can adopt pieces or the whole guide, if desired. There are several sponsors and partners that help accomplish projects. National partners who work across a wide variety of technologies donated software, hardware, and expertise to get things done.

The result of the work was to put out a practice guide that documents the results. The goals are to secure data on a mobile device, allow users to work within and out of the corporate network, allow for granular control over the enterprise network boundary, and minimize any impact on functions. There are different threat categories including: hardware, firmware, mobile OS, application, and device.

Originally, Publication SP 1800-4 was out for comment earlier this year. Most respondents highlighted the need for a more robust threat model. Additional risks and mitigations were added.

Information was then collected. We incorporated 1800-4 public comment information and performed a baseline review of the threat landscape, mobile security literature, best practices, and other sources.

The DHS study on mobile security was an opportunity for collaboration between NIST and DHS. Created in conjunction with the DHS mobile security working group, feedback was incorporated from the GSA RFI on mobile threats and devices and DHS in one-on-one meetings with industry. The starting point of putting together the threat catalogue began after data collection from the DHS study on mobile security occurred.

The purpose is to provide organizations information to perform risk assessments, build threat models, enumerate attack surfaces, and assist in standards mapping activities. This report will be combined with the DHS report provided to Congress. The catalog attempts to address network interfaces specifically. This is an area where threats can be present. For each threat in the catalog, there is a breakdown by category, and a reference to the source of the threat. Exploits were referenced. Countermeasures are listed that enterprises can use to mitigate. It is worth noting that a lot of issues are user errors.

The goal is to present information in the best manner. Therefore, a web interface was created that is easy to navigate. A spreadsheet has also been deployed, but the web interface will serve as the master. In order to contribute, a new issue can be submitted on a new or existing threat which is then reviewed. Users can also directly edit the repository. When a user sees information on a threat, a hyperlink leads to more information. Member suggestions include a Wikipedia-like design where comments can be edited and changed. If the entire report is not read, countermeasures should be rolled up.

There is an associated interagency report that explains why and how to use the catalogue. It was based on the 800-63 interface. NIST IR 8144 provides context to the catalog. The public comment period ends on November 10, 2016. A possible enhancement maybe to provide interdependencies in threats, and when the order of mitigation is important. When it is complete, the publication will be submitted to DHS and then to Congress.

NIST Welcome

Dr. Kent Rochford, Associate Director for Laboratory Programs, NIST

NIST's role in security and privacy has grown over the years, and will continue to do so. It's good to know what we're doing well and important to know what we're not doing well. The attacks last week brought up interesting questions on research priorities and areas of impact. We need models people can relate to. The internet of things security discussion is defined sector by sector. Cross sector discussion is critical to our success. People do not understand the internet of things. We need to make a big impact by developing guidelines on how to apply security and consumer guidelines.

The ability to create the technology is way ahead of the ability to manage it. The NIST Framework may be instrumental in increasing understanding. A suggestion was made to take the existing framework, apply it to different environments and develop new use cases for how we can utilize it

in the IoT space to develop tier 1, tier 2, etc. and establish a baseline. Industry has more of an understanding, while the gap exists in consumer knowledge. The framework is something to build on. Maybe the Board has more resources to push through some of these efforts.

In some ways, this is happening through the development of framework profiles where cybersecurity priorities can be identified. There are two approaches: working with the regulator or authority, and putting the research out there. We constantly deal with how we're balancing executive and legislative interactions and performing our own research. NIST authorizations are fairly broad; the limits involve resources and people. NIST has legislative and executive mandates, and its work for the public. The challenge becomes where to put effort. We can give examples of how to do further research to industry. NIST is limited in the amount of research it can do.

It has been suggested to get with the FTC since they are somewhat regulatory, and put together an initiative to look at how to develop IoT guidelines that include NIST, FTC, UL, the private sector, etc. The idea is to figure out how to make twenty plus organizations come together instead of solving it separately. Ideally, we want groups that represent the broadest application of IoT principles. It is important to get in front of the threat.

Chair (IOT topic): The Board can assist NIST with determining action. Commerce and FTC, Mudge, UL, and possibly others to talk about kicking off how to do consumer guidelines. Want groups that represent the broadest application of internet of things principles. Crazier things will happen, and then the hammer will come down. We have to get in front of it. Anything that gets done must be global.

National Initiative for Cybersecurity Education (NICE) Update

Rodney Petersen, Director, National Initiative for Cybersecurity Education

Danielle Santos, NICE Program Manager

Much has happened in the last year in the program. Since we last spoke to the Board, new literature for the program has been developed. We have scoped to include training education and workforce development. NICE also partners with DHS and others. The plan has three goals: future pipeline, nurturing the community, and skills development. The commission and other groups will be dealing with workforce development. We want to broaden work with the people doing the hiring. It is a new group we are working with.

NICE has been in existence since 2008, but has had new funding in the last few years. We are now fully staffed. We have connections with NCCoE, and the applied cybersecurity division at NIST. There is a new education lead, and a new industry lead. There is also a new lead for government. Work with other agencies is very important. There is a coordinating committee that meets monthly. The National Science Foundation (NSF), The Department of Education (ED), DHS and others meet with us monthly to share information and look at issues. The NIST open working group was launched in January with individuals from different sectors. We have been fortunate to be visible at the cabinet level and other committees. OPM and OMB have released strategies; we are working with them to implement those strategies.

The NICE framework is the key asset we are working for. It will be published as a NIST publication

next week. Training, certification companies, and universities are aligning to it. Increasingly other areas have cybersecurity aspects of their work. Cal State has developed challenges for students to develop skills in cybersecurity.

Next week, we will be making announcements at the NICE conference. We have partnered to develop a jobs heat map for cybersecurity. It goes to city and local levels for types of jobs and availability. Next week will be the seventh annual conference in Kansas City. Eight new centers of academic excellence will be announced as well.

People often want to be involved with NICE. There are two ways to do that. One is through the annual conferences. We also do piloting workshops. There is also a session on cyber education and business needs. People can also join the NICE working group. We are now at over 600 members. There are five subgroups covering education, competitions, and others. They produce fact sheets and white papers.

NICE also offers e-news letters on a quarterly basis. Guest authors come from DOL, academia, and industry. There are also releases on new initiatives in workforce development. Webinars are also upcoming. The webinars will also feature guest speakers. The subgroups will be speaking on different topics in 2017. The public can also provide feedback. The draft will be in public comment starting next week.

RAMPS is a grant program that is starting this year. It partners with K12, higher education and regional employers around the U.S. They will work with K12 schools and local employers. Challenges and opportunities: Getting good workforce data is a challenge, the new administration, working with government agencies is a challenge. RAMPS is new. It has created the ability to collaborate with DOL, and we hope the community pilot work will grow. At the state level, the governor of VA is chair of the National Governors Association. It is a huge advocate of cyber and makes it a priority.

Board: How can ISPAB assist NICE? It can do more with the intersection of privacy and security. It is an area the board can assist with, particularly in education and training. It can also assist with industry engagement. It is a two-way relationship, both have things to offer.

The EPK evolved into the workforce framework. The issue of curricula: The NSF and others are now receiving funding to identify gaps, and work on establishing a foundational cybersecurity curriculum. The debate on having cybersecurity courses versus cybersecurity content across the curriculum is ongoing.

Board Work and Consensus Recommendations

Chris Boyer, Chair, ISPAB; Assistant Vice President, Global Public Policy, AT&T

Follow-up and board discussion:

1. Letter to the next transition team on recommendations. Mr. Boyer has drafted, and some edits have been made. He walked through the letter. The internet of things item was split out to a separate bullet. Mr. Scholl will confirm the number of related letters and dates. Add language for federal support of state initiatives, proposed by Mr. Garcia. Mr. Scholl

will find out how to get communication to transition teams. Can possibly send now to the current addressees, and resend to the appropriate transition party. The letter will be sent around for edits from the Board by the end of next week (before the election). Mr. Scholl made a motion; Ms. Levin seconded. The motion was approved. The Board may meet with new committee chairs on the Hill next March.

2. Matt Scholl will look at availability and schedule at Raeburn for a future meeting and report back to the board.
3. There are two spots open on the board. Ms. Levin provided the name of a privacy person, also the CISO of Merck. Another privacy person would be a good addition to the Board, possibly contact Scott Aarenson. Mr. Scholl is working on a replacement for Danny Toler on the Board. There is still an academic spot open, to possibly replace Ms. Anton.
4. Dates and locations to be announced for the next meeting: most likely in late March, 2017.

Adjournment

The meeting adjourned at 12:35 p.m., Eastern Time.

ANNEX A

List of Participants

Last Name	First Name	Affiliation	Role
Scholl	Matt	NIST	DFO / Presenter
Antonakakis	Manos	Georgia Tech School of Electrical and Computer Engineering	Presenter
Barrett	Matt	NIST	Presenter
Brown	Chris	MITRE	Presenter
Dempsey	Kelley	NIST	Presenter
Dodson	Donna	NIST	Presenter
Echols	Michael	International Association of Certified ISAOs	Presenter
Fangmeyer	Robert	NIST	Presenter
Hall	Travis	NTIA	Presenter
Hartman	Matt	DHS	Presenter
Jenkins	Neil	DHS	Presenter
Kennedy	Andrew	BITS Financial Services Roundtable	Presenter
McKenna	Liam	House Oversight and Government Reform	Presenter
Peters	Iliana	Health and Human Services	Presenter
Petersen	Rodney	NIST	Presenter
Rochford	Kent	NIST	Presenter
Romine	Chuck	NIST	Presenter
Rudolph	Trevor	OMB Office of Cybersecurity	Presenter
Shabat	Matthew	DHS	Presenter
Stanley	Martin	DHS	Presenter
Stine	Kevin	NIST	Presenter
Vina	Stephen	Senate Homeland Security Government Affairs Committee	Presenter
Walsh	Bridgette	DHS	Presenter
Wilshusen	Greg	GAO	Presenter
Wright	William	Symantec Corporation	Presenter
Chalpin	J.P.	Exetergov	Staff
Drake	Robin	Exetergov	Staff
Hatzes	Laura	Exetergov	Staff
Bobrow	Adam	Foresight Resilience Strategies, LLC	Visitor
Hewitt	Michael	NIH	Visitor
Onyewuchi	Agatha	SSA	Visitor
Rzasa	Alex	SSA	Visitor
St. Pierre	Jim	NIST	Visitor
Trimble	Paula	Kimball and Associates	Visitor
Carberry	Sean	FCW	Visitor/Media
Higgins	Josh	Inside Cybersecurity	Visitor/Media
Marks	Joseph	Nextgov	Visitor/Media

Last Name	First Name	Affiliation	Role
Rockwell	Mark	Federal Computer Week	Visitor/Media
Somers	Meredith	Federal News Radio	Visitor/Media
Waterman	Shaun	Cyberscoop	Visitor/Media
Weber	Rick	Inside Cybersecurity	Visitor/Media