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 25, 26 and 27, 2017

American University, Constitution Hall
4400 Massachusetts Avenue, NW
Washington, DC 20016

Board Members	**Board Secretariat and NIST Staff**
Chris Boyer, AT&T, Chair, ISPAB John Centafont, NSA Laura Delaney, DHS Greg Garcia, Health Care Coordinating Council Patricia Hatter, working with cybersecurity start up Gail Stone, Social Security Administration Ed Roback, (by phone) Marc Groman, Privacy Consulting Annie Anton, Georgia Institute of Technology **Remote Participation** Eric Mill, Presenter **Absent with Regrets**	Matt Scholl, NIST, DFO Robin Drake, Exeter Government Services, LLC Warren Salisbury, Exeter Government Services, LLC

Wednesday, October 25, 2017

Welcome and Remarks (from the Chair)

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

The Chair opened the meeting at 9:03 a.m., Eastern Time. The Board will be discussing IT modernization during the course of this meeting.

Recent activity for Mr. Boyer included leading the National Security Telecommunications Advisory Committee (NSTAC) report working group. The report is an expedited version, as it was completed in three to four months as opposed to the usual 18 months. The report recommends progressing in incremental steps. It also introduces the new concept of the

cybersecurity moonshot. The report attempts to address the underlying lack of trust in the internet. The White House may ask for follow-on projects to develop scope based on the report.

Mr. Garcia is now with the Healthcare Coordinating Council. He is working in a program management capacity with the Department of Health and Human Services (HHS) and others. There is a government coordinating, and state sector coordinating, council meeting on November 2, 2017.

Ms. Delaney indicated her recent activity at DHS has focused on cybersecurity events and natural disasters. There are two new binding operational directives (BOD) from the White House: one on assessing current enterprise services, the other directing removal of Kaspersky products from federal IT systems. She is also focusing on the state of communications following the recent disasters in Houston and elsewhere.

Ms. Hatter is now working for a cybersecurity start-up. She was previously with McAfee.

Mr. Groman comes to the Board as a former senior privacy advisor with the Obama administration and is currently working with a number of privacy start-ups. He is new to the board.

Welcome and Remarks (from NIST)

Dr. James St. Pierre, Deputy Director, Information Technology Lab, NIST

The Chair welcomed Dr. James St. Pierre of the National Institute of Standards and Technology (NIST) to the meeting to update the Board on NIST Information Technology Laboratory (ITL) activities. Executive Order 13800 and congressional actions HR 1224 (the Cybersecurity Framework, Assessment and Auditing Act of 2017), HR 2481 (the Protect Our Ability to Counter Hacking Act (PATCH) Act of 2017), and S.770 (the Main Street Cybersecurity Act of 2017) have taken place since the Board last met. The Executive Order focused on strengthening security federal networks, critical infrastructure, and developing cybersecurity workforce for the nation.

NIST issued guidance on the core of the cybersecurity framework for federal agencies. It provides an initial path on integrating new guidance. In August, NIST issued an initial public review of Publication 800-53. The privacy information is longer in the annex but has been integrated into the body of the document.

In September, NIST issued a discussion draft for Publication 800-37 that ties in more of the cybersecurity framework, the privacy framework and some concepts from Publication 800-160. NIST is also in the process of updating the cybersecurity framework and has submitted a draft for public comment.

The executive order directs the U.S Department of Commerce (Commerce) and the Department of Homeland Security (DHS) to lead an open and transparent process to identify broad action by stakeholders to improve communication resilience in the internet. Commerce and NIST are

working with the National Telecommunications and Information Administration (NTIA). The requirements are for a preliminary report to be ready for public comment in 240 days and the final delivered to the President in one year. In July, there was a workshop on enhancing resilience of the internet communication ecosystem at the National Cybersecurity Center of Excellence (NCCoE).

NISTIR 8192 is the report to the President on cybersecurity workforce. Commerce and DHS were directed to assess the sufficiency of efforts to educate and train the workforce in cybersecurity. The preliminary report is due to the President within 120 days. In August, a workshop was held at the Illinois Institute of Technology to get more input. A report was released in August as well. It is currently in the clearance process and with the Secretaries of Congress and Homeland Security.

The Cybersecurity Framework Assessment and Auditing Act (HR 1224) amends the NIST framework assessment for improving US cybersecurity. NIST's role in this legislation is to provide guidance to incorporate the cybersecurity framework into agency security practices. NIST is to chair a federal working group and establish a public private working group to coordinate the bill, metrics, and tools to measure the effectiveness of the Cybersecurity Framework. Finally, it seeks to initiate an agency cybersecurity audit role for NIST. As of the meeting date, the Department of Commerce has not taken a position on NIST auditing activities. Mr. Josh Moses is scheduled to speak to the Board on the agency risk reporting aspects of the executive order.

The PATCH Act of 2017, HR 2481, protects the country's ability to counter hacking attempts by establishing a vulnerability equity review board. The bill is concerned with agreement on the process for vulnerability disclosure to the public and the government. It deals with how the public can more easily submit vulnerabilities to the government, and how the government can have a more public process on its decisions on what to communicate up front and what it discovers later. The bill also establishes the number of people who should be on the board and how it adds people to the vetting process. From a corporate perspective, the big issue is that any vulnerabilities that are disclosed before they’re made available to the public, come with some opportunity for the business community to benefit.

The Main Street Cybersecurity Act (S.770) requires resources to help reduce small business cyber security risks. NIST's role is to provide and update tools, methodology guidelines and other resources, so small business can use them on a voluntary basis. NIST does quite a bit of this already. Putting legislation behind NIST's activity enhances it further. NIST considers its purpose when thinking about new work and determines what fits within NIST's purpose. What NIST is trying to do is cultivate trust in information technology and metrology. NIST is a measurement agency, and its statisticians and mathematicians work with its physical scientists on the metrology vision of science through measurement standards and testing. Cybersecurity clearly fits with trust and IT. It touches IT in many areas including performance testing standards

and other areas.

NIST has five priority areas: cybersecurity, internet of things (IoT), reliable computing, future computing technologies and applications, and artificial intelligence. The research areas cover fundamental, applied, research standards and technology transfer**.** Work is already being done in data science, with a view toward potential expansion. There is a long history of doing statistical analysis; certainty quantification for physical measurements, and in computations. It becomes important in the internet of things, and it's important to understand the complication of computational uncertainty and the error budget across complex logarithm simulations.

B-R-E-A-K

Update on Legislative Activities

Rafi Martina, Sen. Warner Staff

Samuel Love, Sen. Gardner Staff

The Chair welcomed Rafi Martina of Senator Warner's staff and Samuel Love of Senator Gardner's staff to the meeting to update the Board on the status of legislative activities. The members of the Board introduced themselves to the speakers.

The internet of things is a big topic for Senator Warner's staff. An internet-of-things course designed for kids is in the works. Senator Gardner is also concerned with IoT. His staff was looking at a label possibility for consumers, but have changed position recently. They are examining procurement as a means for the government to lead in what devices it buys. The need to raise security in devices is clear.

The senators are also interested in certification as a means to increase and level security. There is international interest in certifications. China, the UK, and Japan have expressed interest. Senator Warner's staff have been more optimistic about a certification approach. There is no single approach that will work for all.

Hygiene principles and certifications are not mutually exclusive. It would be helpful to have a document giving principles for IoT. Discussion needs to happen in this area. The NTIA is currently working on a document.

The Proposed HR 1224 bill was an attempt, given the federal government's interest in protecting its own networks, to try to set some kind of minimum cybersecurity hygiene requirements for IT devices. From Senator Gardner's perspective, the Mirai botnet attack was also concerning. He and Senator Warner discussed ways to try to improve IoT cybersecurity. Initially, Senator Gardner wanted to approach it from a label perspective and possibly utilize Underwriter Laboratories (UL) or another entity to provide a consumer indicator for what the expected level of security was with the device.

After numerous conversations with industry and others, the senators became convinced labelling

was not the right solution for device security. They needed a different method to get at security in a pragmatic and sensible way that still reflects the work industry is doing. They also look to address some of the issues that bad actors have been engaged in. This bill was an attempt to look at the procurement angle in order to arrive at some basic cyber-hygiene ideas within IT.

The general focus is on having requirements on the procurement side, which helps the devices to be more secure and possibly create a market incentive for people who want to do business with the government to build that security in to their products. These effects are positive, but the first order effect of creating a higher level of security in the products the government buys, is an important enough objective. Government buying power is significant enough that it could have the indirect effect of inducing vendors to create products with increased security in order to win government business.

The EU is looking at doing a certification regime for IT devices. The senators met recently with the Japanese government. The Japanese government is looking at doing the same thing. It seems the next in line is the UK. There seem to be many ways in which people are going about security. Underwriter's Laboratories (UL) is one, and there is the NIST Information Technology Lab (ITL). It's a disparate effort right now. In the US, the desire is to get out front of the discussions and try to create some commonality to the approach. Multiple standards would be impossible to live with. There must be commonality internationally.

The senators are increasingly convinced after talking to industry and experts that there is no single static or dynamic analysis technique that works across every range of device that exists. Testing devices in their operative environments is really important. Testing the device without testing in its operating environment creates a false sense of security. It's also just a snapshot in time, and that conveys a false sense of security. Coming out of the box a device has a certain level of security, but if the vendor doesn't commit to some level of patching, and if patches are not implemented at the same level of security, then security is diminished.

Everyone agrees the IoT needs to be focused on a cybersecurity research and development topic. The bill provides an alternative to a certification model. It provides industry with a way to showcase the secure work it is doing. It provides the federal government the means to ensure we have more secure devices and to do it without an inflexible and highly problematic certification regime that's backed by federal regulation. The bill attempts to arrive at a solution without an overbearing regulatory framework. Devices could be purchased if they meet a consensus certification or standard that NIST checkmarks as providing equivalent level of security.

AT&T has written comments to NIST on this issue. However, it would be helpful to have a NIST framework-like document related to the internet of things that establishes some basic principles using voluntary compliance, in the way the framework does. The focus there was on developing a baseline of standards that's commensurate with the risk of the device. NTIA is in the midst of an effort on IoT device upgrade building. They're working on different pieces of it instead of doing it all at once. It's an ongoing effort. It's not static or intended to be final, but

will continue on. Working incrementally makes sense.

The NIST framework is being proposed as an International Organization for Standardization (ISO) standard now. Companies may start certifying against it. It's being done through the market, and people are seeing the value in it. The government is not saying it's required. It's emerged as a standard and people are now moving in that direction on their own. The Food and Drug Administration (FDA) is doing some really fantastic work related to medical connected devices. NIST and the Department of Transportation (DOT) are making important progress. The framework should successfully coexist with the import industry and sector-specific regulatory approaches.

There are a lot of dispersed efforts going on across industry. We are at the same stage now on IoT as we were in 2011 and 2012 on enterprise security. What the framework did is it pulled everything together in to a risk management framework that people could understand. It's geared to people not heavily involved in standards bodies. It needs to be taken, organized, industry convened, and then devise a way to push it forward.

Something that was really sobering to us was that early progress on continuous diagnostic monitoring (CDM) discovered the average agency had 40 percent more shadow IT than their records indicated. The shadow IT problem combined with the rise of, and increasing reliance on, IT is something that is frightening.

The state of cybersecurity across the federal government is poor at best but there's more to it. There's a tension between the pace of business and innovation. It may be beneficial to slow down a bit. The opposite scenario is to wait too long, as happened with other cybersecurity issues that we're now convening on while we're all being hacked and data is flowing to our adversaries. It's important to not only convene, but to act while convening. It is a really unique opportunity to try and get the internet of things right, where perhaps we didn't get other things right.

It means balancing innovation and the desire for innovation. It makes sure that America stays at the forefront with providing for deliberate thoughtful approaches that integrate security concerns from the beginning. There is agreement on what the end objective is, the question is how to get there.

Everybody agrees the bar needs to be raised, but the other side of it is there can't be a complete dependence upon devices. Solutions that involve other layers of the network need to be examined in order to try to manage those devices. A great deal of device traffic comes from overseas. Unless everybody coalesces around a single standard, which seems highly unlikely, AND it gets approved which is even more unlikely, any standard will only go so far. That's half the battle. The other half is getting tools that can manage these devices in a secure way.

People are living in the cloud, the cloud providers are doing the same. Cisco is proposing to build a Manufacturers Usage Description (MUD) standard ability and capability into home routers. There's a lot of different ways to get there and there's an emerging market of

capabilities. It's going to take time for all that to sort itself out.

Conversations at Homeland Security about ways forward for the bill are still going on. There are no updates right now. There's an education process that needs to take place. Emergency management, public safety, and physical security people all have an increasing dependence and inter-dependence on cybersecurity. Many of the tools and technology being used now are connected in some way. That linkage is lost on a lot of people when some of their budget money gets taken away. It goes to cybersecurity which in turn is going to support agencies.

This bill provides a better opportunity to be a convener, a better opportunity for everybody to get in the same place on cybersecurity. There were no ideas from industry similar to what is in this bill. The bill fills that void. This bill is the bill that industry can get behind and see it as a sensible, flexible solution. It provides industry with the ability to come together with NIST and create industry driven standards. There are folks who are not going to participate in that process, but who also might not be the best stewards of security in their devices.

There's going to be some measure of certification programs that will eventually just happen, whether it's UL or a Consumer Report type of certification**,** or what all the other international governments are looking at. The big thing the government could help with is the market domain. It all ties in to this big issue of awareness, education, and getting people to take this issue seriously. That's part of the big challenge, because if that market is going to grow, there must be people out there willing to pay for the extra capability.

Consumers don't have the ability to effectively express their demand because there are no clear metrics of relative security among devices that they can use to pick a device because it meets a higher level of security. It is a challenge, because in order for a lot of these innovations to come out, innovators have to see a market. The question is how to increase people's understanding of the IT environment so that it helps make the case for building security into these things from a business perspective.

EO 13800 Agency Risk Reports

Joshua Moses, OMB

The Chair welcomed Joshua Moses of the Office of Management and Budget (OMB) to update the Board on Executive Order 13800 Agency Risk Reports. Mr. Moses discussed the broader framework that has been in the making for the last three years. It comes with a critical infrastructure role and is also emphasized in the executive order. They've been tracking implementation of the framework in a series of different ways for the last few years including the FISMA metrics available on http://dhs.gov/fisma.

Since 2016, the number of metrics being tracked has increased from 66 to about 80 in the wake of the Office of Personnel Management (OPM) breach and some of the other incidents that have taken place. The cybersecurity sprint of three summers ago focused on PIV implementation and

enhancing multifactor authentication. It was a matter of identifying where agencies stood with respect to the GSA Identify and Protect security functions.

Over the last two years OMB has spent time trying to align the framework to the budget. If one looks at *OMB Circular A-11*, there's an information security business case that ties to framework functions, and FISMA metrics collected by OMB. It is actually getting a sense of tying performance to budget and some measure of risk in a performance-based budgeting approach.

For the first time in 2017, it could be determined what agencies were spending against the framework, down into the category/subcategory level. It provides greater clarity in the information shared with chief financial officers (CFOs) and chief information officers (CIOs) to make sure there's an understanding of the expectations from OMB and DHS in terms of tracking performance.

All that work directly dovetailed with the executive order and what the President requested. There are four core areas it focuses on: securing federal networks; protecting critical infrastructure; strengthening deterrents and collaboration with State Department and other entities; strengthening international coalitions; and building a stronger cybersecurity workforce. NIST is taking a lead role with DHS in workforce building effort.

In the federal networks area, there are a couple of core activities. One was the agency risk assessments submitted to OMB by August 9th. Metrics collection took place in mid-July in order to capture information from across the federal government. Reports were received from 96 agencies. The data had greater clarity than any time previously. It is attributable to the directions given in the executive order. The accompanying OMB memoranda is *OMB M 2017-5.* It describes implementation to bring in reform based on that risk assessment.

Seventy-two FISMA metrics were used to get a baseline measure of how agencies are managing risk, including at-risk, or high-risk, agencies against the cybersecurity framework. A series of narrative questions were provided to agencies to set the context for planning to manage risk across their enterprises. It places the emphasis on risk in all its forms. We see a lot of risk emphasis echoed in the *IT Modernization Report*. It should be circulated here in a week and then the hope is to arrive at a foundational understanding of what capabilities can be brought to bear to detect intrusions once they occur. Those are the metrics that we largely rely on in FISMA.

The focus was tied to the budget to determine where resources are limited, and where gaps exist. A plan will be formulated based on following the existing guidance and frameworks that we already have to manage risk across agencies, and the federal government. All that information became a report that OMB worked on in close collaboration with DHS. People from NIST and other agencies will secure the gaps discovered across government. It isn't a surprise to anyone that many foundational issues came to light.

With the work from the *IT Modernization Report*, there's a discussion of whether there is a consolidated or a common operating perspective across the enterprise. The short answer is "no"

in federated organization. A lot of the work centers on detecting intrusions and how to help enhance communication across the organization. Those are some of the approaches that are captured in this report. The report is not yet public and whether it will be made public will be at White House discretion**.**

Accountability is also an important piece. *OMB 1725* relied on some of the work from *Circular A- 130* where a senior accountable official is to be responsible for implementing the executive order for individual agencies. It requires someone with overview of not only enterprise risk management, but the necessary budget resources to address those risks. It may or may not be the CIO or even the CISO. How can there be accountability across the organization? The answer is through metrics tracking, making sure that information hits the right desk at the right time, and also getting to some measure of return on investment, where every dollar spent on cybersecurity reduces risk.

The method for doing that is tying into some measure of performance and some measure of threat; meaning there must be some measure of true risk in the environment. Most agencies didn't have a handle on where the threat was coming from. Nearly a third of the incidents reported to Homeland Security last year did not have an associated attack vector specified in the reporting. It goes to that OMB enhancement to provide tools for people to understand and get to some root cause, thereby reducing the time to detect, and triage incidents. The work in the next couple months is to circulate that information. The methods for holding officials accountable come through management directing, engagement through the deputy director for management, the President's management council, and the budget. The *IT Modernization Report* is having feedback incorporated now. The critical elements are the authority-to-operate, the move to cloud and other areas.

L-U-N-C-H

Securing High Value Assets

Martin Stanley, DHS, Office of Cybersecurity Communications

The Chair welcomed Martin Stanley of DHS to the meeting to update the Board on the Securing High Value Asset program. The program started in 2015 as a result of the cybersecurity sprint. The risk management framework is intended to be applied as a part of normal business, to look at the most important assets. Historically, there's been a one-size-fits-all method to handle compliance, and a greater focus on less critical systems and services.

The program is an effort to make sure that focus remains on the most critical components to delivering the federal mission, and to protect those capabilities. This idea has been reinforced in a number of OMB memos, most recently in *M-17-09 Management of Federal High Value Assets*, and a binding operational directive issued by the DHS secretary in 2016. Updates to those documents will be coming out. HVAs are considered to be enablers of mission essential functions or public-facing critical services.

There are many ways assets are considered to be important. Mr. Stanley's office has been trying to connect this idea back to NIST and FISMA. Working with partners at NIST, DHS has been trying to pull things back to the NIST Risk Management Framework prioritization. The Federal Information Processing Standard (FIPS) rating is a key piece of that process. In some of the updates to the new administration's executive order on cybersecurity, there are a lot of tie-ins to arrive at one coherent set of guidelines based on the right priorities. Defining what a high value asset is, is an ongoing conversation. The definition process is difficult. The definition has to do with threat and consequence. Those concerns apply to any enterprise that's looking to secure its most critical assets.

There are multiple factors in determining what a high value asset is. First, determine if it is being threatened. Then, look at the consequences involved. DHS is in the process of re-evaluating the services it provides to federal agencies to secure high value assets. They're similar services to those DHS provides to any party that requests assistance. However, these services have been tailored and focused on the special needs of federal agencies that are trying to protect these systems.

It is an entire process that takes place. DHS works with systems that are identified and prioritized by the administration on an annual basis. Once a year systems are selected to be looked at and focused on during that current year. DHS uses a traditional risk and vulnerability assessment that is based on some common scenarios that adversaries are using to target federal systems.

There are six scenarios in the evaluation. There is a phishing exercise, and an attempt to penetrate external-facing systems. There is also a Blue Team type assessment of security architecture, where there are structured interviews. It's qualitative and it's quantitative. Many of the conversations are indicative of how well the organization is managing these systems. Interviewers may ask for someone to demonstrate where all the entry, exit points, and all the interconnections are for a particular system. If that doesn't happen in 30 minutes, it generally indicates there may be other issues going on in that organization.

In the process, they found a lot of stuff that was already known. There are issues with systems that don't have effective authentication systems. There is a full gamut of findings.

There seems to be a lack of understanding of how to segment systems in a way that deters access by intruders. There are systems at different levels of trust, communicating freely with each other. It's more of the wherewithal and the strategy about how to segment the environment, or how to separate critical controls and critical functions. There's a need for people who know how to do segment appropriately, and a need for guidance for people who are practitioners just trying to do the right thing.

There has been success identifying specific deficiencies in specific systems, and to provide recommendations to protect or further strengthen those systems. These systems require constant review and attention to ensure they're being protected. The idea that people at particular agencies

or enterprises may look at a system once it's designed, and then walk away, or never do any re-assessment, is not a practice that can persist. Accountability is key. When we go into an organization, there must be somebody who is the single point of contact, who is empowered to get cooperation from the organization.

There have been incredibly interesting conversations about how a system that's really critical to an organization serves the various stakeholders. Those stakeholders often are not all on the same page. It's really good to bring a third party in, to go through this process, and get everyone on the same page.

If there's a system that has another large enterprise, other agency, or someone else who has a big stake in a particular system, they should be more involved in the authorization determinations for the system to make sure their risk in being a customer or a client or a stakeholder in that system is being managed by the people that are operating the system. It's something we're going to see more and more, and be a bigger and bigger challenge for security practitioners. The organizational and mission involvement must be there when setting the risk parameters and the risk profile.

There's a comparable approach in the Cybersecurity Framework. One of the really interesting things that has happened as a result of the lessons learned is using those common findings to work with NIST to build the 800-53 HVA Control Overlay, based on the control overlay concept that's outlined in the NIST 800-53 publication.

The control overlay concept is really for unique or specialized applications of NIST 800-53 security controls. They're generally applied in addition to, or in combination with, other control frameworks. It starts with a moderate or high baseline, and adds additional controls. It's designed to work with high and moderate level impact systems. There actually have been HVAs that were categorized as low impact systems. Once this overlay works its way through the internal clearance process, the plan is to publish it and provide it to agencies.

The overlay addresses the things the team has observed. It doesn't necessarily address everything. It's been the case many times where an adversary gains a foothold through some mechanism, and they're able to move laterally into the environment to get to what they really want to get to. The document reinforces the application of specific controls, segmentation, and flow controls. Access can be restricted between components at the right places, but it also should to be able to monitor what's going on between and through those communication gates.

Reducing attack circles is very, very important. Permissions and roles with respect to these systems or other areas where care is needed to ensure the right users with the right privileges are able to do the right things. Interconnections are a big area of concern. So much counterparty risk is being accepted, and not necessarily well-understood. We want to make sure that we've provided some specifics on how to do a better job of understanding risk. Then at least a risk that is being accepted is well-understood, and can be mitigated against.

Another common issue is not having a central view of what's going on in the environment. There are trusted internet connections where activity is visible in and out from agencies. Within organizations, there may be folks that operate systems who are coordinating with the network team. There needs to be full situational awareness to be able to determine some types of incidents aren't going on. The document contains some specific guidance on how to ensure that's happening.

There are a lot of things in the *IT Modernization Plan* that will be focused on looking at different architectures. Today, in the environment that we work in, what we have to apply, and what we're trying to ensure, must be in place. There is a chart of all the controls. A lot of time was spent on how each control is applied.

There's a pretty good list of HVAs now. Mr. Stanley's group is meeting with those at the agencies that know about the critical missions and helping them. There are agencies that operate high value assets where a risk meeting occurs every single day where they review a certain set of activities: reviewing recent vulnerabilities that have come out, planning to deal with vulnerabilities and notify all parties internally.

There should be a quicker response generally. It's not a question of organizations not taking this seriously. Organizations don't know how to take it seriously. More fundamental questions need to be asked. A data analysis has been done. They've noted there's a threshold of overall program budget where, when an agency is below a certain threshold, it doesn't score well on any of the evaluation measures.

Voluntary Voting System Guideline Briefing (VVSG)

Mary Brady, NIST

Josh Franklin, NIST

The Chair welcomed Mary Brady and Josh Franklin of NIST to the meeting to brief the Board on Voluntary Voting System Guidelines (VVSG). Work on this project was previously done by NIST staff. Work was completed in connection with the Help America Vote Act and submitted to the Election Assistance Commission (EAC). Public working groups were established. Work happened in a number of areas. There was discussion of the VVSG, including the scope. Use cases were developed and work was done on the structure that was difficult to understand. Work was then done to map high level principles and requirements to test assertions. The principles are out for review with the EAC and working groups for feedback.

The work started with 18 principles and 53 guidelines. They were discussed within and between the public working groups, and in the course of the work they found there were some overlaps of the text. Duplicates were removed and categories merged. Throughout this process, the guidelines went from 221 pages to 38 pages. Those pages only covered human factors. The page number reduced to 20, and then to 10. It currently sits at five pages.

One of the great things, as well as one of the challenging things about voting is that the states are responsible for running elections. Some of the states run elections from the top down, and they have some decent resources coming from the state level to help them out. Some of them run from the bottom up. There are some very wealthy counties that can afford quite a bit of expertise.

The number of jurisdictions throughout the US and the territories, is estimated from 6,600 all the way up to about 10,000. It's an incredible challenge to reach into all of them to try to figure out if they understand the threats, particularly from nation-state actors and how to help them secure individual voting systems. A couple of items that make voting difficult is the whole notion of ballot secrecy and the idea that almost everybody gets to vote. There is a large spectrum of capabilities at the polling place that that must be usable and accessible. There's been a large focus on accessibility this time around.

There are requirements on voter privacy, indicating that the ballot is marked, verified and cast as intended, that the ballots were both safe, usable, and accessible. Some of the security that comes into play: if ballots are auditable, the notion of ballot secrecy and limited access control, physical security, innate protection, system integrity, and detection of monitoring. The principles and guidelines were delivered. Each of the working groups are examining requirements for various stages.

Some systems are included in the VVSG, and some are not. Things like local and online voter registration and electronic poll books. If there is a vote center, or multiple vote centers, some of those actually talk back to the voter registration database. There must be a network that talks back to the voter registration database.

According to the Office of the Director of National Intelligence, there were several attacks that were attributed to Moscow involving data exfiltration from voter registration systems. There's a lot of focus on voter registration systems and phishing against election officials and voting system vendors, doxing of political campaigns, and attacks on the backend systems.

Standards were high in terms of traditional attacks. An attacker would have to be physically proximate to a polling station to attempt an attack. They were worried about accidental events, natural disasters, events affecting public confidence and trust. There have been attacks from nation-state actors. Elected officials with state systems on their desk can be vulnerable. There are a lot phishing emails.

A great amount of attention is given to voter registration systems and to election reporting systems. There are methods for tallying up totals and getting official counts. There are also web based systems that produce unofficial election results. They're not inside the VVSG. They've been subject to mild service attacks in the past, and it was thought they would likely be attacked this time around too, but there wasn't much.

The systems themselves are embedded legacy Linux OS distributions with older or proprietary physical data on them. They're required to stand the test of time, so many of the systems out

there are more than 10 years old. Most people could not imagine using a laptop or a desktop that's more than 10 years old. Some of the operating systems these programs run on are no longer supported.

The jurisdictions that can pay may receive anywhere from one to five updates so they're all patched. This is slowly changing. Some of the issues with patching include states being required to go through lengthy re-certification processes following updates.

What are some of the security innovations since 2009? Within the industry there is secure boot and stronger process isolation, exploit mitigation technologies, stronger network protocols, and some security framework work. Within voting systems, the notion of software independence was introduced around 2007. It's a key component of the VVSG principles and guidelines today.

It is the notion that there cannot be an error in a voting system that goes undetected in the long run. Using today's technology points to people largely using paper to vote. There's this notion of risk limiting audits. There's work going on in verifiable cryptographic protocols, as well as some studies on usability and verifiable cryptographic protocols. Paper ballots provide tamper detection and innate audit capability. However, paper can be modified or swapped. There are also chain of custody questions. There has to be verification. Routine audits need to be performed.

Best practices are often context dependent. The VVSG is a voluntary voting system standard. The EAC has an election reporting checklist, and DHS came out with voter registration guidance. Shortly thereafter, the EAC published its own voter registration checklist that went hand in hand with guidance. There are some best practices for voter registration, election night reporting, and supporting systems for various optical scan ballot marking capabilities. They don't exist for electronic poll books, campaign voter, backend offices, and election management systems.

What are some of the important issues? With respect to technology, there's a need for accessible and auditable voting systems. There's a need for external scrutiny of voting systems. Manufacturers will state their systems are secure. We hear a lot of secretaries of state and election officials say if they're not connected to the network, they're secure. The security community is going to come at it from a little different perspective, meaning a hacker or someone who wants to do harm to the voting system isn't necessarily going to play by the rules. It's good to have other eyes-on and other types of scrutiny.

Software updates are needed for voting systems, so work must be done with the Election Assistance Commission and the testing and certification framework to find a way. A lot of system updates are needed. The security class of the supporting infrastructure is an unknown. With respect to election management, meaningful post-election audits have to be increased when managing elections.

Overall, the community as a whole needs to understand voting system security, even those that

are in charge of very small jurisdictions. They need to understand how modern computers are attacked. DHS is already helping with some of their online educational materials. The election officials need this information written in their language. Even some of the early efforts from DHS, when they were trying to give information out to election officials, was not available in their language, so election officials didn't really understand what they were given. There are a number of topics where additional guidance is needed.

There have been a lot of discussions on not just cybersecurity, but physical security of the voting systems and contingency planning. In some ways, the election officials are already planning for what happens if the power goes out. We've seen this in several states, particularly those that have been hit by hurricanes during an election week.

In summary, a lot of work has already been done on the principles and guidelines in the VVSG. The draft is ready, but it's always little bit out of date. It's been voted on by the Technical Guidelines Development Committee (TGDC), and it's been passed on for further comment and resolution. It's been developed through an open and transparent process. The requirements will be developed that way as well.

Update on Draft SP 800-53

Victoria Pillitteri, NIST

Naomi Lefkovitz, NIST

The Chair welcomed Victoria Pillitteri and Naomi Lefkovitz of NIST to the meeting to provide an overview of recent updates to the NIST Publication 800-53. The initial draft was released in August for comment. Adjudication of those comments is in progress. The final public draft will be released in December, 2017. Publication will occur in April, 2018.

There are a number of updates to the publication. The control structure was changed to be more outcome based. The structure is more aligned with the NIST Cybersecurity Framework. The biggest change in the area of privacy is the privacy appendix was moved to the body of the document. The control selection process was separated from the controls themselves. The language of the controls was restructured. There are new state-of-practice controls based on threat intelligence and attack data. It also includes controls to strengthen cybersecurity, privacy guidance and accountability.

There is now a Risk Management Framework (RMF) interagency working group. OMB convened the group and NIST led it. The goals were to review the 800-53 baselines of "low", "moderate", and "high". Many concerns were expressed on the number of controls. The number of controls is not the key to security. The working group was started as a result of these concerns. The group received 175 comments on the controls. The net result of all the work was that controls were added to each control level.

A public workshop was held in September, 2016 on the privacy controls appendix. There was a core drafting team with weekly and monthly meetings. There were initial public draft comments. The working group received over 3000 public comments. The redline version of controls and baselines highlights significant technical updates and changes. Most comments were from private individuals representing themselves.

There is a new structure of X-1 controls. Reaction to the new structure was strong both for, and against. Thus far, comments have been separated into groups. The working group is tackling groups of 400 comments every few weeks. The final draft goes through an internal review for concurrence. Most comments on integration were positive.

The next steps include the comments continuing through the adjudication process. Updates to the 800-53A, Rev 5 are beginning. For the future, the Rev 6: 800-53 automation project should go online next summer. Comments can be posted online any time. The 800-37 Rev2 workshop was held at the end of September. The 800-37 fully describes the relationship between security and privacy controls. It attempts to clarify the relationship between security and privacy where protecting personally identifiable information is concerned. Privacy and security controls can overlap, where privacy oversight can speak to security outcomes.

The working group is going to a more online approach for working on changes to 800-53 and getting those changes out to stakeholders. There is limited staff to handle FISMA-related work. It seemed more efficient to have the capability to make changes online and receive input more quickly. The larger document of controls will be available about a year from now. Some new controls have been suggested and those suggestions are being evaluated. The group is working to provide clarity on the relationship between 800-53 to 800-53A. The controls are only part of the battle. Implementation considerations, along with policy and procedures play into the picture. In the future it may be that the 53 and 53A will be released together. The anticipation is the final public draft will be ready to publish in December, 2018.

NIST and the joint task force partners' privacy team continue to adjudicate comments. They are having ongoing subject matter expert stakeholder meetings to inform comment resolutions. Ms. Lefkovitz is working closely with the Office of Information and Regulatory Affairs (OIRA).

Looking beyond Revision 5, the update of 800-53A Revision 5 focuses on responding to the requests that have come from stakeholders. An initial public draft will be produced as soon as it is possible. It is somewhat more of a challenge than it has been historically because all the controls have been restructured. This includes the assessment criteria. The assessment language has to be restructured to parallel the control. Moving onto Revision 6 in the future, there has been a lot of feedback about other methods to include the public, in order to move to more incremental, smaller changes that are more consumable by everyone. It means that process can happen more regularly. It is happening through the 800-53 Automation Project to be released in the summer or fall. It will be an online repository of all of the current controls. It will allow stakeholders to submit comments on the controls at any time; not just during the call for public

comments.

Public Comments

Mike Nelson, Cloudflare

The Chair welcomed Mr. Mike Nelson of Cloudflare to present comments. Mr. Nelson noted there has been a radical change in the information technology industry in the past few months. In the past there was a great deal of inspiration and hope in the IT industry. However, recently there has been a great deal of suspicion toward the industry for a variety of reasons, and a real belief that information technology is failing to do its job. World events and recent breaches have played into this feeling. There is anxiety about protectionism and real fear about being locked into a limited range of technology where individuals must give up large amounts of information with little value being given in return. Security of those systems also seems to be lacking.

In short, a different message needs to be communicated by the industry. Mr. Nelson advocates using the cloud to secure connected devices as opposed to attempting to regulate the devices themselves exclusively. Attempting to regulate billions of devices will be too difficult and expensive to achieve with reliable results. The framework of how technology works together lags behind people's understanding of that technology. Abuses and breaches get amplified greatly. There is no countering message to this scenario currently.

NIST can help create a new vision of what things can be like when the right solution is achieved. It is true some of the recent incidents are self-inflicted wounds. Some of those wounds are due to poor management and other things that are not technology issues. The environment is also complex. NIST has the unique role of being an independent third party. Standards and technology are easy compared to the other issues involved. The perception is that the technology is broken because management is broken, which is not in fact the case. When implemented properly, technology works well.

Policy makers generally are unprepared to address these types of issues. It seems like industry cannot get out of its own way. Industry is really good about promoting how great technology is, but not at discussing risk. There is a tendency to look at each area in isolation, instead of taking a common view to search for solutions.

NIST's role is to cultivate trust and transparency. NIST's work on cloud security has been good. Publishing a briefer simple version of that work would be enormously helpful. A lot of good support work was done in the nineties. Some of that may be helpful today.

Review of Wednesday Items

Board discussion items were held for Thursday.

Meeting Recessed

The meeting was recessed at 4:19 p.m., Eastern Time.

Thursday, October 26, 2017

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

National Science Foundation Report on Cybersecurity

Dr. Peter Weinberger, Google

The Chair welcomed Dr. Peter Weinberger to the meeting to update the Board on the *National Science Foundation Report on Cybersecurity*. Work on the report started in 2011. The original concept centered on determining if the classified community had different foundational cybersecurity requirements from the unclassified community. There are two issues regarding the history of creating the report. Money issues caused lengthy gaps in activity, drawing out the process by quite a bit; and the report has a classified annex.

There have been improvements in the state of things overall, but in absolute terms, have we gained or are we still falling behind against the threat? The route to adoption of a good security idea is tricky. If a big corporation happens to adopt something, then many users benefit. Even with training, errors in judgement still occur. Well understood solutions are not being adopted, password rules being an example. Are there password rules in an organization? It is a research question. What characterizes those organizations that have changed policies versus those that haven't? It generally goes to what kind of risk decisions are made. Equifax's behavior exemplifies bad risk decisions. Some good ideas get adopted, some don't.

With malware, the question is, who are the bad guys, and what do they deal with? If things are getting better on this side, they have to innovate to get around security improvements. Are zero days actually finite? We don't really know. There are people who believe secure systems are achievable, in contrast to the opposing thought that everything has bugs. A system is secure when it doesn't offer many surprises. There is a long list of things that should not go wrong.

There needs to be more research in security science. There is some hope of a physics-like science in security, but there is no evidence such a science exists. Research time lines are always longer than desired. Interdisciplinary research is hard, and researchers know research is hard. Working on improvements and evaluating research are also hard.

Companies that do bug bounties take security seriously. It is a problem that security is not a core component of education in computer science or programming. It is more than the obligatory course for majors. Teaching robustness against the unexpected needs to be emphasized more. The end result is many people are not doing the right thing. There must be reactions to the bad guys. Research must help with new ideas.

Briefing on the NIST IoT Cybersecurity Program

Kat Megas, NIST

The Chair welcomed Kat Megas of NIST to the meeting to update the Board on NIST IoT

Cybersecurity activity. Ms. Megas leads the IoT cybersecurity program at NIST. They consider the internet of things to include all connected devices. The NIST program started a year ago. It covers a spectrum of cybersecurity work at NIST. The program mission at NIST is to cultivate trust in IoT and foster an environment that enables innovation on a global scale. They develop and apply standards, guidelines, and related tools to improve the cybersecurity of connected devices and the environments in which they are deployed.

Their ongoing program efforts include the IoT task group of the Inter-agency International Cybersecurity Standardization (IICS) working group. They coordinate on major issues in international cybersecurity standardization. The working group has 54 federal employee participants representing 13 agencies. The IICS working group will meet in December and determine next steps for the current draft report. Gartner just released an update to its 2017 estimates. It estimates we are on track to outpace current projections for 2017 by 30 percent in terms of the number of connected devices. For their definition, all connected devices are being considered. The difference between industry and consumers in terms of connected devices is also shrinking.

The Cybersecurity for IoT Colloquium focused on where perceived threats and risks are. The federal government, the University of Maryland at College Park, and private industry were represented. The importance of global standards in industry lag, and consensus-built standards were highlighted at the colloquium. There was much discussion on incentives. Everyone wants to improve, and people want to do the right thing. Companies should be rewarded for doing the right thing.

The list of activities at NIST and the National Cybersecurity Center of Excellence (NCCoE) in this area includes: byte-rate encryption, wireless infusion pump work, and a new project that's potentially being stood up in the NCCoE on IoT-based distributed denial of service (DDoS) attacks. Privacy for IoT devices is being looked at. Something will be published very soon. Webcast and presentations will be available online. Starting in January, there will be a series of events in hopes of starting thinking and garnering feedback from industry.

The cybersecurity framework is also generally applicable to the internet of things. There is a public website at NIST where people can go to look up more on areas of interest. NIST's work on de-identification and anonymization of data and the use of unique IDs is important in terms of privacy. In lightweight encryption, work in passive powered four-bit microcontroller-size devices with almost no memory is also going on.

Publications or planned publications are expected on these areas of research. A new catalog on IoT standards is expected to be out next year. It will go through the NIST internal report process and then public comment. In summary, the threat landscape is varied and broadening, and there's no authoritative set of security and privacy guidance at this time. The IoT space is wide, there are some common risks and threats across the internet of things, but there are also some very market-specific or application-specific risks and threats that need to be considered, which is why

there will be no one-size-fits-all answers. There was also much consideration of incentives and privacy issues, particularly regarding informed consent in IoT.

Ms. Megas's team began with looking at federal agencies as they are at least partially responsible for agency security under the Federal Information Security Management Act (FISMA). It seemed a natural way to begin. They discovered many use cases that apply to the federal government also apply to health care in the private sector. Connected vehicles are also being considered as the government operates fleets of vehicles. They are in the process of putting out guidance to assist federal agencies with securing devices. It is intended to be an introductory document.

The next steps include a summary of feedback from the colloquium. The first session of a series of town halls begins in January, 2018.

B-R-E-A-K

EO 13800 Modernization Report

Eric Mill, GSA

The Chair welcomed Eric Mill of GSA to the meeting via WebEx to update the Board on the Executive Order 13800 Modernization Report. Mr. Mill is a senior advisor in the Technology Transformation Services Office at GSA. He is a co-author of the *IT Modernization Report*. He provided a summary of efforts on the modernization report to date.

The report focuses on network modernization and consolidation, as well as shared services. Shared services are intended to consider commercial cloud, cloud email, collaboration tools and other shared services such as security operation centers as a service. Policies are expected to change to aid in transitioning to cloud use.

The report says two things: reduce focus on network level protections, meaning there has been too much emphasis on locking down networks and focus on perimeter protection. The emphasis should instead be on reducing federal technology services through better technical services and data level protection, and visibility beyond the network level. The report talks about updating policy accordingly.

Physical chokepoints for network traffic have been difficult because there is a limited number of trusted internet connections in the government, and scalability is a problem. Trusted connections are often managed separately, or are physically separated from the systems the technology is designed to protect.

Improving visibility includes activities like more sophisticated logging infrastructure, collecting logs in one place and reviewing them regularly, and virtualization of security tools. There is a focus on getting agencies to focus on their HVAs as directed by OMB and DHS in their High

Value Asset program. It emphasizes that modernization efforts will begin with those high value assets. It changes the focus from low value assets to high value assets.

Appendix A to the report contains a section on best practices and foundational risk case capabilities. Appendix B provides a framework of an example of virtualizing security tools. It is meant to demonstrate how a federal enterprise can be more agile and flexible.

The report was published for public comment. They received slightly under 100 comments from industry groups, as well as from Microsoft, Google, and Amazon. Comments were taken by email and at GitHub. All input received is publically visible on the internet. Responses from companies and industries and a variety of sectors were received and read by the team. As of the meeting date, the report is not yet final and changes are still being made.

L-U-N-C-H

Update on NIST Activity

Matthew Scholl, NIST

Megan Doscher, NTIA (replacing Kevin Stine as presenter for this briefing)

The Chair welcomed Matthew Scholl and Megan Doscher of NIST to update the Board on NIST activities. Ms. Doscher replaces Kevin Stine. There have been discussions on the American Technologies Council, the *IT Modernization Report*, and Mr. Mill's related updates. The focus is to highlight how these areas are intended to work together. They will inform updates to NIST Publications 800-53, 800-39, and 800-37. NIST is supporting that work with promoting the use of an "authorization to use" (ATU), which is different from an "authorization to operate" (ATO).

The ATU is intended to assist the ability for people to co-sign an authorization to engage in shared services. The government does not want to have a full ATO for each agency to use one shared service. Each signer of an ATU should acknowledge it understands its role in a shared service, and what risks come with that acceptance. The intent is to push people to limit use of the high value designation to truly high value assets and promote the use of Federal Risk and Authorization Management Program (FEDRAMP) approved clouds as much as possible.

The definition of "high value" is not clearly understood in all cases. Independent asset evaluation is going on in agencies. The privacy team should be in any decision that impacts people in order to understand the data. Every agency must conduct a privacy impact analysis (PIA).

Misunderstandings occur because the agency signs off on the ATU. Many clients assume at that point they have no further responsibilities for their use of the system, but that is not the case. The client still has responsibilities. A PIA is always required. Systems also require analysis to determine what types of data will be contained in them. Data sensitivity needs to be determined, and that takes privacy input. Impacts to individuals must be understood in the light of security controls.

NIST is very interested in security engineering issues, to provide tools, techniques, guidance and practices to reduce vulnerabilities in software and improve the state of software. They are looking at tools and tool chains, anything to facilitate building a better product. There will be more information in 2018.

The National Vulnerability Database (NVD) is a huge data set that some researchers have mined. Researchers have mined the data to get an understanding of possible trends in vulnerabilities and taking different looks at the data. They have returned to companies looking for additional information.

NIST is very concerned about the quantum computing future. Representatives from NIST went to the European crypto-authorities workshop in July. The UK, Germany, France, Netherlands, and Korea will also participate in various functions. NIST has received 34 post quantum submissions to date. They anticipate between 50-70 official submissions. Official responses received in November will be made public. There is a two-day workshop in April, 2018. NIST continues to track key safety. There are still 3-key triple Digital Encryption Standards (DES) in inventory. Many gas pumps use this type of cryptographic key. Migration away from this key should come soon. Secure engineering, software security, cryptography, federal agencies, and assisting agencies and DHS on HVAs are also areas where work is happening.

Mr. Boyer proposed publishing a process document so there is understanding of what happens behind the scenes with different types of publications. Mr. Scholl will undertake the initial draft. The FIPS process and the NIST special publications process are different.

NIST is also looking at big data analytics. Can there be big data sets for testing purposes to determine validity of outcomes? Security of big data and security for big data are concerns.

EO 13800 DDoS Report Update

Tim Polk, NIST

Megan Doscher, NTIA (replacing Evelyn Remaley, NTIA as presenter for this briefing)

The Chair welcomed Tim Polk of NIST, and Megan Doscher of NTIA to the meeting to update the Board on the Executive Order 13800 DDoS Report. The executive order directs the Secretary of Commerce and the Secretary of DHS to produce a report on how to increase resiliency against automated distributed threats. A public draft is due January 5th, with the final report to the President due in May.

NIST held a workshop in July. There were 150 seats and all were filled. NISTIR 8192 was published with six themes: global nature of the problem, availability of effective tools, importance of securing products throughout the lifecycle, education and awareness, and others.

Home users can't be expected to be very technical, but some decisions made by users really matter. The market tends to reward being first to market over device security. Cybersecurity

insurance may be a benefit in the future, but it is too soon to expect consumer benefit currently. Cyber insurance is not uniformly defined as yet.

The consensus is that no one sector could fix the problem on its own, even if it wanted to. Improvement will be a challenge. New, insecure devices are being deployed very rapidly. NSTAC report will be approved in November. The draft report is going public on Jan 5, 2018. A comment period on the new draft will follow for 30-days. Assimilation of comments received will follow. A workshop will be held in late February as part of finalization process. An internal agency review follows the workshop. The final report is due May 11, 2018. It will follow in the style of the cybersecurity commission report to the President submitted in 2016.

Thursday Board Recap

The National Science Foundation Report called out the need to do something different with the cyber moonshot concept. The goal with the moonshot is to put down a marker and make significant progress against that marker. "Roof Shots" are incremental steps toward a moonshot goal. It needs to be figured out. There must be a better way to measure success. We have trend lines.

Speaker for future meeting: Have Vint Cert provide thoughts to the Board. The early internet assumption was that everyone with access was a trusted entity. It was not built with security in mind.

Topic for future meeting: "Secure Time" is also a topic. Leap second impact.

Topic for future meeting: The GPS "Y2K" is coming up in 2019. The Board will want to weigh in on this topic. Have DoD come to brief the board.

Meeting Recessed

The meeting recessed at 2:49 p.m., Eastern Time.

Friday, October 27, 2017

The Chair opened the meeting at 9:02 a.m., Eastern Time.

Briefing on Inspector General (IG) Metrics and Assessments

Dr. Brett Baker, NRC (National Regulatory Commission)

Peter Sheridan, Federal Reserve Board

Tammy Whitcomb, US Postal Service

Khalid Hasan, Federal Reserve

The Chair welcomed Dr. Brett Baker of the NRC and Chair of the Federal Audit Executive Council, Peter Sheridan and Khalid Hasan of the Federal Reserve, and Tammy Whitcomb of the U.S. Postal Service to the meeting to update the Board on Inspector General Metrics and assessments. The Board members introduced themselves to the speakers.

Oversight.gov is a one-stop shop set up by the council for inspectors general to post their audit work publicly. Work typically is available within a few days of being posted. The upload process is simple, and contact information for all inspectors general offices is on the site. It launched officially on October 1, 2017. Most, but not all inspectors general post work publicly on the site. The site is searchable and allows research into topical information on work being done by other IGs. Information is close to real time and shows metrics on savings, and what the IG community is doing.

Another site is http://www.ignet.gov. It describes the IG community with more general information about the community. It is more business oriented and about who they are and what they do.

There is a recent report on web application security. Nine IGs participated in the report and 22 assisted with surveys. Seven recommendations were contained in the report to OMB. NASA reported on web applications that they were concerned with. The IT committee undertook doing the report on behalf of the contributors.

FISMA calls for an annual independent evaluation of information security program and practices. It is an assessment of the effectiveness of the information security policies, procedures, and practices of the agencies. They found thousands of vulnerabilities, inaccurate inventories and poor security policies. Their report is posted on the web.

Mr. Sheridan and Mr. Hasan work with the FISMA requirements for the annual agency audit. Agencies must be in compliance with NIST guidance, and the CIO must report annually. OMB designated DHS to provide oversight of the process. The reporting deadline for agencies is October 31st. IGs now monitor effectiveness as well as compliance. Compliance tended to be defined by the agency using more subjective methods, while the effectiveness of those methods is now measured more quantitatively.

There has been a lot of attention focused on the maturity model. There is thought to developing a companion document for the model. How does continuous monitoring play into it? Most agencies are not at that level of maturity. Formerly, there was a three year assessment with nothing in between. Now there is continuous tracking on a daily basis. Systems that fall below a floor threshold are not in compliance and lose authority to operate.

The first three levels of the maturity model cover basic operations and capabilities: Ad-hoc, Defined, and Consistently Implemented. The last two levels are more advanced. Indicators include risk management, and taking an enterprise risk management approach. There are about 60 questions in the matrix. Within assessment areas there are questions with ratings that determine the maturity level. Most agencies are at level 2 as of 2016. Agencies and IG assessment showed discrepancies in level of maturity. Agencies tended to overstate maturity.

IGs rely on NIST OMB directives. There are no new requirements for the agencies. Many IG reviews feed into the final report. It can take 6-9 months for one maturity review. Many individual system reviews come in to play as well. IGs are necessary for the government to function properly. Many agencies do not have data governance. They will also examine whether government data retention policies are being followed.

They will be releasing an evaluation guide in the future. The Board can assist with defining priorities.

DHS Binding Operational Directive on Software Use in USG

Michael Duffy, DHS

The Chair welcomed Michael Duffy of DHS to update the Board on the DHS Binding Operational Directive on Software use in the US Government. Mr. Duffy will provide an update on the specific binding operational directive (BOD) 1701, which mandates removal of Kaspersky products from federal government systems. Binding operational directives give DHS the authority to identify priority areas for federal agencies to focus on and direct actions to implement very critical items over time.

To date, BODs have been used to implement critical actions across the .gov domain. They have fallen into four areas. There were hundreds of critical vulnerabilities in 2015. All were mitigated in the stipulated 30-day period. Across the .gov domain, the number of bad things is declining. BOD 1701, removal of Kaspersky products from federal IT systems, gave a series of required steps to agencies. There is a 30-day milestone for agencies to identify Kaspersky products on their systems. The directive used the *Circular A-130* definition of "system".

Agencies had 60-days to provide a timeline for removing Kaspersky products. At 90-days, agencies are to begin removing Kaspersky products. Those are the three actions required by BOD 1701.

A new binding operational directive, BOD 1801, relates email security. It provides a baseline of security in the .gov domain that needs to be raised for email authentication (vetting potential phishing emails, etc.) The executive order acknowledges the federal civilian government operates on behalf of the American people, and they should be confident the .gov domain is secure.

Use of the BOD has promoted communication between federal departments and agencies across the .gov domain. If there is evidence of activity at a certain threshold that requires immediate attention, they are able to do so with a binding operational directive.

NIST Update – Part 2

Kevin Stine, NIST

The Chair welcomed Kevin Stine of NIST to the meeting to update the Board on additional NIST activities. Mr. Stine provided updates on program areas that have not been covered in Thursday's update with Mr. Scholl. The seventh framework workshop was held in June. They received good feedback. The read out document from the workshop was issued in July, 2017. It summarized what was heard from the community. The second draft of version 1.1 is due in fall, 2017 for public comments. There is a 30-day comment period. The first draft contained the majority of the changes. The second draft brings back the sections on measurements based on feedback received.

NIST issued a cybersecurity framework manufacturing profile in September. It has been well received. The National Initiative for Cybersecurity Education (NICE), has had a busy summer with activities related to the Cybersecurity Workforce report. They included an RFI and a workshop in Chicago. The report is in review with the Secretaries of Commerce and DHS.

Publication 800-181, the NICE Cybersecurity Workforce Framework was published in August. It received positive feedback and was well received. It re-purposes older publications on workforce categories. It recognizes multi-disciplinary roles in hiring, acquisition, etc. It provides definitions of roles and associated training required for those roles.

The annual NICE conference is 2 weeks from now in Dayton, OH. The Annual K-12 Conference in Nashville, TN is supported by NICE, but held by an outside organization. The pre-conference event is hosted by IBM for 6-9th grade girls. It was noted a "digital citizenship" theme would attract more young girls to cybersecurity as a career.

Three new projects have launched at the NCCoE. Some are out for public comment. Since the last board meeting, three 1800 series documents have been released for comment. Feedback is welcomed on all.

It is a great volume of activity. Guidance to industry on how information is used would clarify understanding. It's hard to identify SMEs, etc. It's hard to get comments submitted within

shortened time frames. Advance notice when brief comment periods if possible would be helpful. A walkthrough of the process when working with companies would also be helpful.

The Safeguarding Health Information Conference was held in September. There were seven hundred attendees online and in person. @NISTcyber launched this week. It helps to get word out on events, publications, etc. Mike Garcia has resigned from his position at NIST. Mr. Stine is now acting lead for trusted identities.

Board Work and Consensus Decisions

The Board discussed the following areas of interest concerning letters, topics of interest, and future meetings.

Future Meeting Topics:

1. NIST audit authority vs IG audits and IT training for IGs. Does the recommendation from July still stand? Have Kathy (?) come in to have follow-on discussion at the next meeting. Additional information could take the form of workshops for IGs.
2. Legislative issues on the Warner – Gardner bill. Perhaps have UL or others come in and brief the Board. Add to the agenda for the next meeting in 2018.
3. Plan the annual White House briefing for March, 2018.
4. National Science Foundation briefing on R&D strategies and how to measure. Discuss the "moonshot" concept.
5. GPS "Y2K" coming up in 2019. The Board will want to weigh in on this topic. Have DoD come to brief the board.
6. Threats: EMP threats, etc. What is the government doing in these areas?
7. Phishing: Mentioned in multiple presentations.
8. Privacy impact analyses PIA oversight, etc. Privacy council. (Mr. Groman).
9. Invite GOVCAR (?) to report to the Board.

Future Meeting Topics

1. Big data as used in the government, and implications for the federal government. How to deal with increasing data, privacy, storage, encryption, etc.
2. High performance computing security, etc. and strategy
3. Friday update: Annual update from a remote location (Commerce, etc.). IOT legislation will still be in process.
4. Invite Safe Code and Vera Code for future meeting.
5. Invite Matt Goodrich to discuss the relationship between PIA and FEDRAMP.
6. Invite Vint Cert to provide perspective to the Board.

Areas of Interest:

1. Publish a FIPS and SP publication process document so there is understanding of what happens behind the scenes. (Mr. Scholl will draft).
2. Mr. Boyer will provide the NSTAC report to the board.

3. Mr. Scholl will propose locations, dates for the next meetings in 2018. Possibly propose a 2-day meeting instead of the current two and a half days.

Adjournment

The meeting adjourned at 11:47 a.m., Eastern Time.

List of Attendees

Last Name	First Name	Affiliation	Role
Scholl	Matt	NIST	DFO / Presenter
Baker	Brett	NRC	Presenter
Brady	Mary	NIST	Presenter
Doscher	Megan	NTIA	Presenter
Duffy	Michael	DHS	Presenter
Franklin	Josh	NIST	Presenter
Hasan	Khalid	Federal Reserve Board	Presenter
Lefkovitz	Naomi	NIST	Presenter
Love	Samuel	Sen. Gardner Staff	Presenter
Martina	Rafi	Sen. Warner Staff	Presenter
Megas	Kat	NIST	Presenter
Mill	Eric	GSA	Presenter (Remote)
Moses	Joshua	OMB	Presenter
Pillitteri	Victoria	NIST	Presenter
Polk	Tim	NIST	Presenter
Remaley	Evelyn	NTIA	Presenter
Ross	Ron	NIST	Presenter
Sheridan	Peter	Federal Reserve Board	Presenter
St. Pierre	Jim	NIST	Presenter
Stanley	Martin	DHS	Presenter
Stine	Kevin	NIST	Presenter
Weinberger	Peter	Google	Presenter
Whitcomb	Tammy	U.S. Postal Service	Presenter
Chalpin	JP	Exeter Government Services	Staff
Drake	Robin	Exeter Government Services	Staff
Salisbury	Warren	Exeter Government Services	Staff

Last Name	First Name	Affiliation	Role
Boeckl	Kaitlin	NIST	Visitor
Baker	Brett	NRC OIG	Visitor
Crouch	Lara	Beacon Global Strategies LLC	Visitor
Evans	Allison	Lewis Burke Associates	Visitor
Hasan	Khalid	FRB OIG	Visitor
Heckmann	Chris	J.A.G	Visitor
Matsui	Shigekazu	NTT	Visitor
Moses	Joshua	OMB	Visitor
Nelson	Michael R.	Cloudflare	Visitor
Onyewuchi	Agatha	SSA	Visitor
Polk	Loretta	NCTA-The Internet & Television Association	Visitor
Ross	Kelly	Hettinger Strategy LLC	Visitor
Sokol	Annie	NIST	Visitor
Suh	Paul	USPS	Visitor
Tooley	Matt	NCTA	Visitor
Turner	Maurice	Senate	Visitor
Friedman	Sara	GCN	Visitor/Media
Geller	Eric	Politico	Visitor/Media
Higgins	Josh	Inside Cyber	Visitor/Media
Johnson	Derek	1105 Media	Visitor/Media
Marks	Joe	NextGov	Visitor/Media
Mazmanian	Adam	FCW	Visitor/Media
Miller	Jason	WFed	Visitor/Media
Uhill	Joe	The Hill	Visitor/Media
Waterman	Shaun	Cyberscoop	Visitor/Media
Weber	Rick	Inside Cybersecurity	Visitor/Media