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

September 28, 2021

Virtual Meeting Platform: WebEx

Attending Board Members	**Board Secretariat and NIST Staff**
Steve Lipner, SAFECode, Chair, ISPAB	Matthew Scholl, NIST, ISPAB Secretariat
Dr. Brett Baker, NRC	Jeff Brewer, NIST, ISPAB DFO
Giulia Fanti, Carnegie Mellon University	Jim St. Pierre, NIST
Jessica Fitzgerald-McKay, NSA	Kevin Stine, NIST
Brian Gattoni, DHS	
Marc Groman, Privacy Consulting	
Arabella Hallawell, NETSCOUT Systems	
Douglas Maughan, NSF	
Katie Moussouris, Luta Security	

ISPAB Overview

In January 1988, the Congress enacted the Computer Security Act of 1987 (Public Law 100-235). A provision of that law called for the establishment of the Computer System Security and Privacy Advisory Board (CSSPAB) within the Department of Commerce. In accordance with the Federal Advisory Committee Act, as amended, 5 U.S.C., App., the Board was chartered in May 1988. In December 2002, Public Law 107-347, The E-Government Act of 2002, Title III, the Federal Information Security Management Act of 2002, Section 21 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-4) amended the charter statutory authority of the Board and renamed it the Information Security and Privacy Advisory Board (ISPAB).

ISPAB Scope and Objectives

- Identify emerging managerial, technical, administrative, and physical safeguard issues relative to information security and privacy,
- Advise the National Institute of Standards and Technology (NIST), the Secretary of Homeland Security (DHS), and the Director of the Office of Management and Budget (OMB) on information security and privacy issues pertaining to Federal Government information systems, including thorough review of proposed standards and guidelines developed by NIST.
- Annually report its findings to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the National Security Agency, and the appropriate committees of the Congress.

The Board's authority does not extend to private sector systems or federal systems which process classified information.

Tuesday, September 28, 2021

Welcome and Opening Remarks

Steve Lipner, Chair, ISPAB, Executive Director, SAFECode

ISPAB Chair Steve Lipner, Executive Director of SAFECode opened the meeting at 1 p.m. (eastern time), noting that the objective of this meeting was to focus on the status and the activities of the Executive Order 14028, *Improving the Nation's Cybersecurity* (May 12, 2021) and other Presidential directives. Mr. Lipner also noted that the agenda allowed for considerable time for Board discussion with the hope that the Board can provide some feedback and encouraged members to engage in the discussions.

Welcome and ITL Update

James St. Pierre, Acting Director, ITL, NIST

Mr. St. Pierre, ITL Acting Director began by thanking the Board for their time, guidance, and their advice, stating it was incredibly valuable to NIST. Mr. St. Pierre welcomed the two new ISPAB members, Giulia Fanti and Katie Moussouris and provided an update that Dr. Charles Romine, currently the Acting Chief of Staff for NIST will hopefully be back as the ITL Director by the next meeting. Mr. St. Pierre informed the Board that there was a nominee to fill the currently vacant NIST Director position. Laurie Locascio was nominated, with October 2021 as possible date for Senate confirmation hearings.

Mr. St. Pierre stated that the Board would hear discussions on the Executive Order, Industrial Control Systems work and Zero Trust Architecture. Mr St. Pierre also informed the Board that NIST was leading the Administration efforts by running the newly created National Artificial Intelligence Advisory Committee, run by NIST's Elham Tabassi, and the Secretary of Commerce will be making the final selections to the Committee. This has generated allot of interest and many nominations. The nomination period ends on October 25, 2021.

Matt Scholl, Chief of the Computer Security Division in ITL said that the purpose for holding this additional half-day ISPAB meeting was in response to the Board's desire to have a short in-progress review/update of the Executive Order activities and some of the executive branch activities that were under way, and to track these activities prior to the Board's next scheduled meeting in December 2021.

Published this week (September 23, 2021), DHS and NIST coordinated in releasing *Preliminary Cybersecurity Performance Goals for Critical Infrastructure Control Systems* as a follow up to the July 2021 *National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems*. The Board will hear from DHS and NIST, providing an update, with main points of interest from DHS and its outputs.

National Security Memo on Preliminary ICS Performance Goals

Peter Colombo, DHS, Keith Stouffer, NIST, Vicky Pillitteri, NIST

Mr. Lipner introduced Peter Colombo from the Department of Homeland Security (DHS) and Keith Stouffer and Vicky Pillitteri of the National Institute of Standards and Technology (NIST).

Mr. Stouffer thanked the Board for the opportunity to address them and provided a brief overview and updates on some of the deliverables in the *National Security Memo on Critical Infrastructure and the Infrastructure Control Systems Performance Goals* which was signed on July 28th of this year. The presentation included Mr. Stouffer and Ms. Pillitteri, who are the NIST technical leads, along with Peter Colombo with CISA, who is the overall lead of the project.

- This National Security Memo (NSM) No. 5, issued July 22, 2021 requires the development of cross-sector control system performance goals and sector-specific critical infrastructure cybersecurity performance goals
    - September 22, 2021: Preliminary control systems cross-sector goals due by September 22, 2021 (goal met):
    - Final cross-sector & sector-specific goals due by July 28, 2022
- This NSM emphasizes the initiative should be "a voluntary, collaborative effort between Federal Government and the critical infrastructure community to significantly improve the cybersecurity of critical systems."
- CISA and NIST led the development of the draft cross-sector goals with input from interagency and industry control systems groups and delivered them to the White House on September 22, 2021.
    - Control Systems Interagency Working Group (CSIWG)
    - Control Systems Working Group (CSWG)
    - Distribution through the Industrial Control Systems Joint Working Group (ICSJWG)

Mr. Colombo added that the discussion revolves around a very policy rich environment, especially the control system space and that the genesis of this requirement is NSM number five. There are really two tranches of deliverables that were specified within this NSM. The preliminary control systems cross sector goals were due out on September 22, 2021. Mr. Colombo stated they were very relieved to have met that initial goal but would draw the Board's attention to the term preliminary, because the longer-term deliverables are due by July 22, 2022. Mr. Colombo explained the intent of the Performance Goals are to provide baseline and enhanced recommendations on best practices that are consistent across sectors, intended to draw attention to existing standards rather than replace them, and intended for a broad, cross-sector audience of owners/operators. The Performance Goals were not intended to be a CISA directed compliance regime or intended to supersede or countermand any existing regulatory guidance or standards.

Mr. Colombo detailed that the core draft was focused on outreach efforts and laid out plans to go forward with an ever-widening stakeholder engagement to ensure both interagency and industry have had the appropriate level of input on the long-term deliverables. Mr Colombo stated there is also an added secondary deliverable for sector specific goals, noting there are sixteen distinct, specific sets of rules that are ideally derived from those higher-level cross sector goals in terms of ongoing interagency management collaboration. It was highlighted that they were not able to incorporate all the feedback because of the limited timeline of a September 2021 rollout but it was clear that any recommendations or input made will be adjudicated and nothing would be left on the cutting room floor or unaddressed. The document was widely socialized and posted on the DHS website on September 22, 2021 and is starting to get public comments trickling back in. It was noted by Vicky Pillitteri in drafting the document that implementing all recommendations does not necessarily mean you are secure by default. This is not representing a subtotal of everything you can do to eliminate all risk. This would be a baseline of what you should be doing. There were nine Preliminary Performance Goals provided:

- Risk Management & Cybersecurity Governance
- Architecture & Design
- Configuration & Change Management
- Physical Security
- System & Data Integrity, Availability & Confidentiality
- Continuous Monitoring & Vulnerability Management
- Training and Awareness

- Incident Response & Recovery
- Supply Chain Risk Management

Mr. Stouffer provided a breakdown of the nine goals, stating that each performance goal includes a description of the goal, rationale for the goal, specific objects that support deployment and operation of secure control systems (baseline objectives and enhanced objectives), as well as objectives to strive for in the future. An example was of a Preliminary Performance Goal was provided:

1. **Risk Management and Cybersecurity Governance**

   GOAL*: Identify and document cybersecurity risks to control systems using established recommended practices (e.g., NIST Cybersecurity Framework, NIST Risk Management Framework, International Society of Automation/International Electrotechnical Commission (ISA/IEC) 62443, NIST Special Publication (SP) 800-53, NIST SP 800-30, NIST SP 800-82) and provide dedicated resources to address cybersecurity risk and resiliency through planning, policies, funding, and trained personnel.*

   RATIONALE: *A formal risk management process provides standard terminology, documents risks, identifies roles and responsibilities, and is used by management to understand and manage risks, estimate impacts, and define responses to incidents.*

   Baseline Objectives
   • *Identify, document, and prioritize known risks to control systems*
   Sample Evidence of Implementation: Organization has completed and documented a risk register and risk assessment using an established recommended practice on all control systems; the organization has a plan for updating them on a regular (e.g., annual, semiannual) basis.

Next steps were discussed on how to meet cross-sector goals by continuing to work with CSIWG/CSWG to refine cross-sector control systems goals, as well as working through Sector Risk Management Agencies (SRMA) and sector coordinating bodies. CISA is currently conducting internal planning to best execute the sequence of activities for developing the Sector-Specific Goals. Mr. Stouffer mentioned that some goals may have as few as two to three objectives and some of the goals may have up to six or eight. As for the cross-sector goals, you've got everything from a major regional utility, to a local municipal water supply that may have two or three staff members (or less) handling such security and challenges, but the commitment here is make goals that are applicable across that entire spectrum. Objectives are written at a high level.

Ms. Vicky Pillitteri of NIST added that the plan going forward is to leverage existing working groups and dive into the work on the sector specific goals, engaging with SRMAs as the SMEs in their sectors to utilize existing relationships and understand the sector and working a project plan to approach that engagement and what is expected to execute. We have all these different sectors working on these goals, but we want to make sure that they're relatable and that we don't have multiple unique products and then sub iterations from subsectors that don't bear resemblance. It's so critical that we get engagement from all the relevant stakeholders within these sectors across federal agencies, from the private sector, and just general stakeholders throughout this process. The goal of this is transparency, communication, and real partnership across all. Ultimately, we were looking at how we ran the cyber security framework process and are using that as the model to continue. Obviously slightly different scope and scale, but that's kind of the golden standard that we're ending up from the NIST perspective, with ongoing development and

research of our technical guidance and resources that will support owners and operators with implementing good security practices. Earlier this year we released an infographic on tips and tactics for control system cybersecurity. NIST is conducting research necessary to issue a revision to SP 800-82 and going through our literature, review, and identifying areas that need further collaboration both across NIST and with our external partners, and hopefully having something out early in 2022

Ms. Pillitteri asked the Board how NIST and CISA can expand stakeholder outreach and coordination to best support the critical infrastructure control systems and ensure that we get buy in from all relevant stakeholders. Mr. Stouffer responded that ultimately, we want to make sure that these are actionable performance goals that really do make a difference.

Discussion:

- Mr Lipner asked, faced with a new policy, framework, or structure, how does it make its way to the systems that are operating, how does this all flow, and how do we get to a set of high-level objectives that are going to make a difference?
    - Mr Stouffer said that what will make a difference is going be the stakeholder engagement that occurs throughout the next steps, and to specifically point out the rationale statement, explaining that organizations are tired of hearing that they need to do something without the reason why. Mr Stouffer also stated that their intention, as the goals become more finalized, is to map them to various other frameworks that organizations are familiar with, such as the CSF, and provide a reference to any implementation guidance that may help an organization with that objective. NIST is conducting research to update SP 800-82, Revision 3.
    - Mr. Colombo reiterated that outreach to the organization and partnerships were key, along with plans to take the preliminary write ups and lay them against real world data and examples that an organization can use to raise their entire security posture.
    - Ms. Pillitteri stated there was an opportunity to dive deeper and provide more specified targeted guidance, to improve the usability, accessibility, and the use of existing resources and good practices. There is an opportunity to share the wealth of knowledge that we have and make it accessible to all and look forward to working with all stakeholders to make sure that what is produced as the final does reflect its current state and where we need to go.
- Ms. Hallawell commented that there seems to be an organization cultural difference between the IT world where they have a robust security organization, and the ICS community, where a manager, for example handles the physical security. Ms. Hallawell asked if they were adding specific lanes such as physical access and physical security, or is it taking key tenets from the CSF and making it more implementable, for ICS systems?
    - Mr. Stouffer answered that the big difference between control systems or ICS and IT systems, is that control systems physically interact with the environment. So you can't just blindly apply IT countermeasures to the control system environment. Much of our guidance is how to interact with IT countermeasures specifically within a control systems environment and to provide compensating controls, other ways of meeting the intent of certain security controls.
- Ms. Moussouris asked who are the other stakeholders engaged so far on these various topics as they apply to elevating the state of ICS security, and is there a concept of assessing current maturity levels among the intended audience to gauge how deep the gaps are and exactly where they are? As opposed to waiting until you do a compliance assessment later to determine compliant versus noncompliant.

  - Mr. Colombo stated that what's on paper now and working across the existing bodies right now may not be enough because it is mainly touching the owner operators and there may be a risk of missing vendors and integrators. So a big part of our conversation with SRMAs, is do we need to set up an ad hoc structure to engage other stakeholders?
  - Keith Stouffer spoke to the maturity aspect stating that the maturity amongst the critical infrastructures themselves is going to be very different depending upon the infrastructure. Some of the difficulty will be reaching small and medium size organizations. So again, socialize these performance goals and get their thoughts.
- Ms Fitzgerald-McKay asked if there were plans to differentiate between some of the different recommendations? As an example, prioritize into things that you must do whereas if you have more technical expertise you can move on to more complex implications.
  - Ms. Pillitteri stated that was something to consider moving forward whether it's quasi maturity concept in the performance goals that are cross sector, or whether it's developed for sector specific performance goals, and having the opportunity for a crawl, walk, run model does help with the accessibility and potentially the usability of any of the resources.
  - Mr. Colombo said one thing we can do as these are presented to various sectors is to provide references such as NISTs Tips and Tactics or the recently released infographic with five different things you can start with now, that are relatively easy, that are inexpensive to do, that will increase your security posture, and once you have done these steps, additional steps are provided to consider.
- The Board Chair commented that it would be beneficial if you are able to take the objectives or best practices, and pilot with an organization to get some experience with how these things can affect an organization.
  - Mr. Stouffer stated that this was something to consider and provided an example of how this process was done at NIST with the manufacturing sector to develop a manufacturing profile with the cybersecurity framework (CSF).
- Ms. Moussouris made two suggestions to the panel: 1) To prioritize the list of "must use" versus the "would be nice to have", and 2) to prioritize which goals are critical, providing somewhat of a roadmap, and providing the prerequisites, people, process, and techniques needed to implement these baseline objectives.

NIST Executive Order 14028 Update
Kevin Stine, NIST, Matthew Scholl, NIST

- Mr. Kevin Stine opened the presentation by providing a comment on the previous panel discussion, saying he didn't want to understate the value of the relationship with the Manufacturing Extension Partnership, the MEP Program which has a network across the country with direct access to small and medium size manufacturers that could be a testbed to get close to the challenges that those organizations face from a control systems perspective and be a source of great information to help provide more information on the operational challenges they experience so that we can make sure the things we produce are relevant. Additionally, the potential to work with industry closely through the NCCoE to build out example solutions of some of these capabilities and working with those that are providing the products and services.
- Mr. Stine provided an update on Executive Order 14028 implementation at NIST and tied it to a new initiative that was announced on the heels of the White House Cyber Summit. Most of

NIST's technical leadership responsibilities are found in Section 4 of the EO, focusing on enhancing the software supply chain security. Mr. Stine stated there are longstanding programs in supply chain risk management as well as the software quality and security, so this EO provides a good opportunity to leverage existing work, not just NIST, but also in industry, identify gap areas, in standards, guidance, and practices.

- This EO lays out an ambitious agenda, certainly not a one and done approach. NIST wants the practices and guidance developed to be practicable and actionable, maintained and improved so they can lead to more sustained and enhanced security over time.

ITL Executive Order 14028 Action Items Update:

- Hosted a public workshop in June soliciting input from stakeholders (public, private, academic producers, consumers, and suppliers) to help identify resources that can support the development and implementation for NIST's responsibilities under Section 4.
- In June, NIST issued a definition of critical software, recommending a phased approach to implementation so that the government could learn from the early implementation and refine the approach and methodology. This definition would then inform policies and actions that will drive procurement decisions across the United States Government and NIST wants to make sure that the definition and surrounding guidance would be clear and viable, leading to improved security and not lead to policies or implementations that would have an adverse effect on either security or on the government's ability to procure software. This guidance focus includes mappings to the Cyber Security Framework (CSF), to SP 800-53 controls, and other relevant government resources such as CISA and GSA, with the intent of maximizing the use of existing resources focusing on explicitly called out topics like least privilege, network segmentation, and proper configuration.
- OMB issued policy memorandum M21-30, Protecting Critical Software Through Enhanced Security Measures, which codified a phased approach and provided additional details.
- NIST published guidelines that recommended minimum standards for vendor or developer verification of code, collaborating with NSA.
- NIST was directed to initiate two labeling programs, on the cybersecurity capabilities of IOT devices, and consumer software development practices and identify key elements of labeling programs in terms of minimum requirements. NIST will not establish their own labeling program. There are existing labeling programs in government and industry. NIST is focused on producing the minimum requirement, the fundamental characteristics, and attributes for labeling program in these two domains.
- In August, NIST published a White Paper asking the community for suggestions on the potential baseline security criteria for IoT devices as well as suggestions and feedback on the challenges to the practical approaches to consumer software labeling and held a panel discussion to consider feedback received.
- NIST is working multiple workstreams but ensuring they are mutually supportive and learn lessons from each other and stay internally coordinated so that the critical software definition feeds the security measures and is informative to the software verification guidelines for minimal standards.

Discussion:

- Ms. Hallawell asked if NIST has received any feedback since the papers were published? Mr. Stine stated that comments received to date ranged from positive to suggesting the need to take the guidance further.
- Mr. Groman asked, if the notion was to have a consumer facing label such as a nutrition label, that would advise consumers of the potential level of security in a product? Mr. Stine noted that often software is purchased as a service as opposed to something that is purchased in a package and has a label. NIST at this stage, is agnostic on what form that label, designation, marker, or information could be because of the way that software is developed and provisioned today. Mr. Scholl added that a recent NIST workshop noted many of the challenges that Mr. Groman voiced, and highlighted several topics, from the human, sociological, and psychological aspects of a meaningful label to the different potential stakeholders/consumers and what would be communicated. Mr. Scholl acknowledged this was a challenge, and that the Executive Order stipulates this as a pilot program, and the goal was not to have NIST run it, but it would be a tech transfer to industry in February 2022 and noted that while operating under an Executive Order, NIST is limited as to what can be required. Mr Groman commented that the competitive issues at play are astronomical. Mr. Stine acknowledged the complexity, and other challenge is, that whatever is produced to inform the consumer needs be meaningful, understandable, and is verifiable in a post-production environment.
- NIST is working on IOT, product labeling, and securing critical software in the U.S. Government, and guidance for minimum standards for verifying software, which is very product focused. Another workstream in the EO requires NIST to issue guidance around software process orientation rather than product, and NIST will leverage the Secure Software Development Framework, designed around outcomes and software processes, looking to see if the outcomes in the SSDF cover all the outcomes for the EO, are the references complete, and are there artifacts that can be produced to provide evidence that an organization is applying a process.
- Ms. Hallawell asked if the intent of the workshop and process is to help developers with a better process to defend against vulnerabilities and build code so it can't be exploited?
    - Mr. Scholl answered the question with yes, the Software Verification White Paper is focused on the developers, but it is also for organizations with helpful suggestions such as fuzz testing, regression testing, code bench reviews to make sure nothing is deliberately added.
- Ms. Moussouris asked what the plan for updating the frequency of the labels when things change, and what triggering events might necessitate a change that is out of normal cycle for updating a label?
    - Mr. Scholl responded that at this time, they do not have answers, but hope to have answers as the pilot program rolls out.
- Mr. Scholl reiterated that NIST will not be running or overseeing a test and conformance program, and anticipates lengthy discussions around vendor self-declarations, noting the guidance that NIST might be suggesting needs to be heavily based upon what the natural outputs of the development process would generate anyway.

OMB Zero Trust Architecture Strategy
Eric Mill, Office of the CIO, OMB

Matt Scholl introduced Eric Mill from the Office of the CIO, Office of Management and Budget. The following topics were covered during Mr. Mill's presentation:

- OMB recently released A Strategy for Implementing Zero Trust Architecture Across the Federal Government. Zero Trust can mean different things. OMB viewed their goals as providing enough clarity, guardrails, and clear priorities to agencies to make decisive steps over the next few years toward progress.
- A Strategy for Implementing Zero Trust Architecture Across the Federal Government was released for a short public comment period. Over 100 comments were received. Mr. Mill stated they were aware that the draft was missing some things in certain places, so the public comments received would help fill that in.
- Some key point related to the draft:
    - The draft is aligned with CISA's maturity models focused on identity, devices, networks, applications of workloads, and data.
    - Identity is a huge priority, building on the work of NIST and OMB, trying to get to a baseline of phishing resistant, multi-factor authentication, around consolidated, federated single sign on within the government using modern standards, and consolidating identity services, and integrating with cloud services.
    - The draft is very authentication heavy. It may be expanded to cover machine identify and authorization. OMB feels that in the field of authentication, the industry has arrived on a practical bar for phishing resistance that can be implemented across the U.S. Government, and that the government already has a strong authentication tool in the form of PIV. Where PIV cannot be used, gaps can be filled in, moving away from OTP, SMS, and push notifications.
    - As for the network priority, it is encryption focused, moving away from trusted networks, removing as much implicit trust as possible, and encrypting data in transit, particularly in systems that agencies consider to be internal and not internet facing. HTTP and DNS were selected as marquee protocols to push federal agencies to encrypt traffic internally and to treat them as internet accessible traffic, whether they are or not.
    - As to application security, OMB is hard on empirical security over compliance and wants to make compliance work associated with security, proportionate to its value.
    - Mr. Mill discussed vulnerability testing, stating that OMB finds agencies are self-constrained on vulnerability testing on their application layer services in cloud environments and want to encourage agencies to understand that they are authorized to test those systems, and OMB's role is to remove any barriers.

Discussion

- Mr. Lipner asked Mr. Mill to return to address the Board on privileged access management (PAM) and provide an update on the Zero Trust Architecture Strategy. Mr. Mill added that PAM

shouldn't be a substitute for multi-factor authentication, but they do expect PAM to be addressed more in the final version as it was commonly asked about in their public comments .

- Ms. Moussouris mentioned the specific provision around application security testing, and available third-party testing, asking if that is an implication of bug bounties or something else?
    - Mr. Mills answered that it is meant to reference dedicated firms and there are no bug bounty mandates in this strategy.
- Mr Mill concluded stating the formal comment period has closed, however comments can be emailed to zerotrust@omb.eop.gov.

The Chair recessed the meeting for a 15-minute break.

Public Comment, Summary of Day 1, and Board Discussions

Jeff Brewer, Designated Federal Officer for ISPAB, received no official requests to address the Board from the public.

Board Discussions

Steve Lipner, Board Chair

Mr. Lipner addressed the Board regarding the presentations that were provided today and asked the Board what they felt was going well, and what was going poorly?

- Mr Groman stated that given the authorities that currently exist in law and that the agencies and executive branch have that they are using their authority to fullest extent, but at the end of the day, their impact will have little to do with improving cybersecurity and that far more significant changes are required, and that would probably require being implemented through statutory changes and law. Mr Groman stated he doesn't want to undermine the authority, the efforts so far, take wind out of their sails, but far more drastic efforts need to be made if a significant impact is going to be made on the cybersecurity posture of the government.
- Ms. Moussouris noted that in the EO itself, although it appears to be a priority to improve cybersecurity, it seemed like there were some odd inclusions and some that were not well-defined yet, such as SBOMs. She stated her concern over the relative impact of these inclusions and views it as a lack of prioritization within the EO. Ms. Moussouris and suggests some form of prioritization exercise on the EO components to prioritize 1) what are the activities known to produce positive security outcomes, and 2) what are the activities that are the easiest to implement to maximize the impact of agencies' efforts. Ms. Moussouris also suggested that some form of follow-up on the results after some of the EO has been implemented to see if it had an impact on reducing the number of cybersecurity incidents for those that implemented the EO versus those that did not and noting what had the most positive impact after implementation.
- Mr. Lipner commented that in theory, an EO is well adhered to and should make a difference as to how an agency protects the government's information and position it as a leader that the private sector would listen to, as well as the impact to government procurements.

- Mr. Groman agreed that when policy decisions are made around security or technical controls, that the private sector in the procurement world does respond, but the impact of an executive order is limited in many circumstances.
- Mr. Maughan noted that implementation of an EO is not necessarily tied to an individual and their responsibility to implement, that perhaps it should be.
- Dr. Baker stated that an EO might put out good guidance, but the compliance piece, and the enforcement of the EO is where things fall off and noted that the responsibilities should be added to a CIO or CISO's performance plan. Mr Groman suggested that the accountability should rest at a leadership role such as the head of an agency, or head of the bureau.
- Mr. Gattoni added that from the budgetary side, that additional legislation is necessary to put the investment decisions into the hands of the agency heads that can make necessary changes.
- Ms. Moussouris suggested a way to provide accountability and measure improvements over time by developing a baseline and showing from one year to the next the need for additional resources if data shows that agencies are falling behind on implementation.
- Mr. Groman stated that measurement metrics has always been a challenge noting FISMA metrics as an example, that it is difficult to measure performance from year to year if your FISMA requirements are always changing. Dr. Baker added that more testing has been done in the FISMA space, hoping to make that more stable and stated that there should be some type of controls in place at an agency to make sure things are happening.
- Mr. Lipner asked if the ISPAB would want to say something about the compliance piece? Using the audit and compliance process to encourage the agency implementation actions? Mr Groman stated that having the Board send a letter regarding this subject isn't anything that people in government don't already know and doesn't recommend if it can't be constructive.
- Mr. Lipner asked if the Board should say anything about prioritization? Ms. Fanti asked, if a letter on this topic were submitted, what type of response could the Board expect? Mr. Scholl answered that it would be direct input into how OMB would shape policy around the Executive Order, and direct feedback on how NIST should make prioritization decisions in different areas called out in the EO. Mr Groman stated that it would be one thing for the Board to recommend prioritization, but it would be difficult from the outside to advise specifically what should be one, two, three in priority. Ms Moussouris suggested as a Board, recommendations that the line of demarcation would be to prioritize activities that have known positive security outcomes and that there are those in the EO that have never been implemented at a large scale and that agencies need to prioritize based on their current resources and prioritize activities that have been proven successful in the private sector, without specifying an order. Dr Baker advised that OMB has current guidance to what Ms. Moussouris is suggesting and linking it to the EO could be helpful.
- Mr. Lipner noted that he will draft a letter from the Board based on the prioritization discussion.
- Mr Groman said that OMB, the President of the United States, and Congress needs to make cybersecurity more of a priority against the hundreds of other priorities that they

are given and make the difficult decision about role of technology and data and the need to secure it versus the mission and other critical activities. Mr. Groman stated that the Board needs to raise this to a policy level, and risk assessment needs to be made at a higher level of authority.

Next ISPAB meeting set for December 08 – 09, 2021 (virtual)

Board Recessed at 4:14 PM