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

March 20-21, 2024
JW Marriott Washington DC,
The Senate Room (Lobby Level)
1331 Pennsylvania Ave, Washington, DC 20004

Board Members	**Board Secretariat and NIST Staff**
Steven Lipner, SAFECode, Chair, ISPAB	Matthew Scholl, NIST
Dr. Brett Baker, NARA	Jeff Brewer, NIST
Michael Duffy, CISA Cybersecurity Division, DHS	Kevin Stine, NIST
Giulia Fanti, Carnegie Mellon University	Rodney Petersen, NIST
Jessica Fitzgerald-McKay, NSA	Diana Proud-Madruga, Electrosoft//Exeter
Alex Gantman, Qualcomm	Government Services LLC
Brian Gattoni, Federal Reserve Board	
Cristin Flynn Goodwin, Advancing Cyber	
Marc Groman, Groman Consulting	
Essye Miller, Executive Business Management (EBM)	
Katie Moussouris, Luta Security	
Phil Venables, Google Cloud	

Wednesday, March 20, 2024

Welcome and Opening Remarks

Steve Lipner, Chair, ISPAB, Executive Director, SAFECode

- The Chair opened the meeting at 10:00 a.m. ET and welcomed everyone to the meeting.
  - Invited each board member to briefly share a few words.

Board Member Introductions and Updates

Mr. Gattoni,

- Lots of action on AI and generative AI.
- Working with quite a few of our international partner banks in reviewing several sets of standards, including NIST standards and ISO standards, for their applicability against the payments and financial market infrastructure cyber guidance from 2016.

Ms. Flynn Goodwin

- Working with smaller and medium sized companies discussing struggles. Whether it be misguidance, or consuming large compliance regimes, or models, or looking at technology, I'm getting so many questions about where to start or how to start tackling issues.

Mr. Gantman

- Working with Steve in the National Academies study on assurance and nimbleness for complex software systems.
- Keeping track of regulations and discussions on software liability. Since last time, I had a chance to co-teach a class on the history of cybercrime, which brought home just how much of it has moved away from exploitation to just fraud.

Mr. Venables
- Massively focused on everything to do with AI, from how to help organizations implement it effectively through how to protect foundation models and dealing with hundreds of different bits of regulation and legislation around the world on AI, risk, trust, safety, and security.
- Big area of focus in the past six months, which I'll talk about later, is the White House PCAST report on cyber physical resilience.

Mr. Duffy
- Here from the Cybersecurity Infrastructure Security Agency (CISA).
- CISA is deeply interested in everything from AI to secure by design and default.
- Interested to hear from presenters and be part of the board moving forward.

ITL Update

Kevin Stine, Director, Information Technology Laboratory (ITL), NIST

Purpose
- Stays the same as always: Cultivating trust in metrology.
  - This is the business focus and lens through which they look at their work.

Key Position Changes
- I (Kevin Stine)
  - Moved up to serve as the Director of the Information Technology Lab
- Rodney Peterson
  - With his Cybersecurity Education and Workforce Development hat on, has agreed to serve as the interim Chief for the Applied Cybersecurity Division.
  - We are working to get a vacancy out to fill that role permanently.
- Kamie Roberts
  - Is back at NIST after a long-standing detail to a program within OSTP as the National Program Office Director.
  - She is now the Program Manager for all the NIST activities that we were directed to take on in response to the AI executive order.

FY24 Budget
- NIST recently received our full year appropriation for FY24.
  - For most of NIST research, measurement science, and measurement services, the appropriated funding for those internal programs is the same as FY23. This includes cybersecurity and privacy.
  - What's the effect of the FY24 enacted budget on the cybersecurity and privacy programs?
    - Even though our scientific and our technical research and services (STRS) account does show a top line increase, this amount includes a pretty substantial increase in external community projects, congressionally directed spending – commonly referred to as earmarks.
    - Need to manage some reductions for our internal spending this fiscal year.

    - Received a reduction in appropriated funds for our main facilities account for internal spending that includes facility modernization and deferred maintenance activities.
- **Mr. Groman** – asked when they talk about privacy and cyber, does that include the AI work under the EO? Is that work separate from privacy and cyber?
    - **Mr**. **Stine –** replied that AI is a separate budget/programmatic area. Cybersecurity and privacy and AI falls in the same bucket. AI will see an increase in FY24 to provide funding for the AI Safety Institute.
- **Mr. Groman** – mentioned that the question becomes, "where is privacy and cybersecurity related when it comes to AI?"
    - **Mr. Stine –** replied that he thinks that is a technical, programmatic point of intersection they are working on today, but the resources are viewed as they come into separate accounts.

FY25 Budget

- The proposed budget requested reflects:
    - An increase in spending for internal research and for urgent facility needs at NIST; this includes cybersecurity and privacy.
    - A substantial increase in funding for AI, specifically to address the long-term goals of the executive order and to continue to support the US AI Safety Institute.
    - An increase for quantum technologies including post quantum crypto and the potential scale up of quantum systems and activities.
- **Mr. Gantman** – asked if the state of the facilities could beat a point where it's the trigger for workforce attrition?
    - **Mr. Stine –** replied that it certainly makes it hard to recruit. Specifically, within ITL our facility and equipment needs are along the lines of a traditional office space. Other parts and labs of NIST are true laboratory environments and there is a much greater concern around our ability to continue to attract new talent and keep existing experts.
- **Mr. Lipner** – mentioned that historically, the computer security divisions have received a lot of funding from other agencies. He asked if that is still an important part of their program and workforce these days?
    - **Mr. Stine** – replied that they've been fortunate over the last several years that their appropriated budget at NIST, specifically for cybersecurity and privacy, has gone up as has the number of requests for them to take on more. Whether through legislation or executive action, they do sometimes receive other agency funding to support their work, in collaboration with other agencies with mutual interest. Sometimes that does involve provisional funding, but they try to not be dependent on the existence of other agency funds.

National Vulnerability Database (NVD)

- There has been media coverage recently about the NVD and the pause in enrichment of reported vulnerabilities. We are receiving many inquiries on the topic.
    - NVD is a priority for NIST and a key piece of the nation's cybersecurity infrastructure.
    - It's heavily used not just by researchers around the world, but by operational teams around the world as well.
    - Growing backlog of vulnerabilities that are submitted to NVD that require analysis, and the enrichment piece of associating a vulnerability with the platforms that are affected and with the vulnerability severity score.

- The combination of the growing backlog of submitted vulnerabilities and the budget constraints has shifted focus to prioritizing the analysis of the most critical vulnerabilities.
  - Looking at longer term solutions to help address this challenge.
- Working both within NIST and with the Department of Commerce to be able to provide more information publicly on where things are today and the actions that we intend to take.
- Looking for feedback from the community.

- **Mr. Gantman** – asked if they have a sense, in terms of months or years, of how large the backlog is?
  - **Mr. Scholl** – answered that under normal conditions they process 200 to 400 per week, but they've had a slight scale down.
    - Looking at new governance models, knowing that growth in the future is something that they need to address, but they also received a 10-fold dump (2000-4000 CVEs) from kernel.org within a couple of days.
      - They are working through that right now.
      - Will get back to looking at the new governance structure after addressing this.
    - Haven't really done the 'this many hours per analyst per number' yet.
- **Mr. Duffy** – asked if they expect the output or results that NVD is producing to change, or would it be mainly who's involved in the process?"
  - **Mr**. Stine – replied that it's more who's involved in the process at this point.
    - Want to continue to make sure that they can provide good, trusted vulnerability data that is enriched.
      - Comes back to cultivating trust which is infused in all that they do.
    - Need to view short term options as well as some longer-term options to make sure that they can keep up with the pace of the vulnerabilities that are coming in, understand today's resourcing constraints, and how to best address those in the future in managing that environment.
- **Ms. Flynn Goodwin** – asked if analysis of different companies' vulnerabilities by submitter location is helpful? The ability to map that information and see percentages of vulnerabilities that are coming in from different regions or different countries could be interesting. It doesn't change the technical realities of what you need to do with the data, but it could be interesting to be able to model and work with the additional information. I'm curious if that can find its way into your vulnerability metrics categories at some point?
  - **Mr. Scholl** – Replied that they get the CVEs upstream from either CNAs who are making their own CVEs or an authorized CVE Publisher. That type of data would have to come from working with the CVE board to see if that would be a field that they could add or capture as part of that submission. We don't have that as a CVSS score but, if it was a CVE field, it could be put in (to CVSS) as optional for the locality scoring capabilities, but maybe not in the base score. It's an interesting idea, but we don't capture that data. That would be something that the CVE board might have to investigate to see if that's something that they want to add or not.
- **Mr. Gantman** – asked "When you're talking about who gets involved, are you looking at deputizing CNAs to provide this data? For example, there's the CNA that issues the CVE but there are other CNAs that are impacted by that CVE who are in a good position to vet the rating

and the enrichment data. Could they sign off on it before NIST accepts it without significant review?

- **Mr**. **Stine** – replied that options like that are certainly on the table for consideration. There are different roles and tiers of roles that can be performed. Hoping to engage the industry more broadly, possibly through a consortium, to flesh out ideas like this.
- **Mr. Scholl** – commented that he will talk about this tomorrow. If we remember in 2016, what ended up happening was the creation of the CNAs to assist with issuing CVEs.
  - They looked at that model, what they could learn from it, and how that could be extended.
  - They are still working with getting the federal registers and consortium created, cleared, and passed. They intend to look at something very similar to that.

- **Mr**. **Gantman** – asked if they are looking at integrating the KEV into NVD?
  - **Mr. Scholl** – replied that the KEVs and the CVEs already cross reference each other. When they have to prioritize, KEVs get priority for us to look at and verifying the CVEs are good, looking at the remediation information that's provided, and providing scoring.
- **Mr. Gantman** – asked if it makes sense for them to be two independent systems that are referencing each other as opposed to just metadata in the NVD?
  - **Mr**. **Scholl** – replied that's an interesting question and he doesn't know the answer to that. NIST doesn't have KEV information, CISA does. NIST is just collecting the problems with the technology and then they link to each other where those things intersect.

Cybersecurity Framework 2.0

- CSF 2.0 was released on February 26, 2024. Many changes came because of the tremendous community input that we received.
  - Name/Title
    - For years, the official name had been Framework for Improving Critical Infrastructure Cybersecurity, and it had a very laser sharp focus primarily on critical infrastructure owners and operators.
    - Over the last 10+ years, they observed that new organizations outside the defined critical infrastructures are using it.
      - Made the official name change to the NIST Cybersecurity Framework 2.0.
  - New Function
    - Original 5 functions: Identify, protect, detect, respond, and recover.
    - Added a sixth function "govern".
    - Govern was already in the framework before, but it was buried in some of the other functions. Felt strongly that cybersecurity continues to be more and more an organizational governance area.
    - There's a lot of new content and new cybersecurity outcomes from a governance perspective that were very critical and that are now embedded in that governance function.
  - Supply Chain Risk Management
    - Was in the framework but sprinkled throughout.
    - Is still sprinkled throughout but there's also a significant increase in the categories and subcategories around supply chain risk management in the governance function, from both a first party and a third-party risk perspective.

- Purpose of CSF 2.0
  - This is a platform, it's a suite of resources, to help organizations take better advantage of the CSF and put it into practice. That includes things like QuickStart Guides, implementation guidance, and implementation examples.
  - We have more in the queue of QuickStart Guides that we're developing now, based on a lot of the community feedback we've received.
- Mappings
  - The CSF and other NIST resources follow the hub and spoke model.
  - Relationships exist between the CSF and NIST privacy and AI work.
    - Want to have those mappings in place across the NIST resources to help organizations take better advantage of those resources.
  - There's a lot of value in having a rich set of mapping data that is both human and machine readable so that your GRC tools that organizations are using can ingest the mapping data and help with your organization governance risk and compliance activities.

- **Mr. Groman** – asked two questions: Does it more seamlessly integrate other risk frameworks and what do we need to do to get to a place where we're integrating the analysis based on overlapping data? The second piece is the accountability piece. Who is accountable? The CIO? The C-suite? The board?
  - **Mr. Stine –** replied that, regarding the accountability piece, they included some of that discussion in the governance function: what are the things that organizations should be thinking about with respect to cybersecurity? Then understand the impact of governance decisions on identify, protect, detect, respond, and recover.
    - Not fully there yet, but it does point to some other NIST resources and other industry resources that do have that enterprise risk view.
  - The NIST portfolio of frameworks have "grown up" on their own in silos.
    - Have tried to tie those things together in meaningful ways and tried to be purposeful in how those different resources are related to allow for a more seamless integration between CSF and other things.
  - Naomi and the privacy team have announced they're going to be launching an update to the privacy framework.
    - There are changes in the CSF that will allow for greater integration on the privacy side.
  - Doing the same thing on the Secure Software Development Framework (SSDF) and even the AI risk management framework.
  - They are open to other suggestions or ideas, but they have a lot of the pieces in place that are purposeful efforts to mature the CSF alongside all the others allowing for much tighter connections and more seamless use.
- **Mr. Duffy** – asked how much they are seeing this as NIST going back to the frameworks and working within NIST or is it something that other parts of the government or externally can take to the next phase? Is NIST also thinking about where the other players could be supportive?
  - **Mr. Stine –** replied that some of that is coming together in the context of CSF through the National Cybersecurity Strategy, where you've got different requirements that are leveraging the CSF. They're staying very engaged in those types of interagency and across government and industry activities. We want to bring those resources and if there's good ideas, and folks that are inspired to take that and run with it, maybe with some of our advice and consultation, there's a lot of value there.

Artificial Intelligence (AI)

- Work will continue to focus on cultivating trust and design and development using the governance of AI.
- Producing guidance and tools,
- Continuing to enrich and help organizations take advantage of the AI risk management framework.
- From a broader standards perspective, they are engaged both domestically and internationally.
    - The President issued the AI Executive Order 14110 on safe, secure, and trustworthy AI. That set forth a very ambitious AI agenda aimed to deliver standards and guidance in a significant number of critical areas related to AI.
    - Making good progress on this.
- Most of NIST's deliverables in the executive order are due around day 270 so around July 26, 2024, they:
    - Issued a request for information shortly after the EO was issued. That was a wide ranging RFI intended to gather input and feedback from the community to inform many of the deliverables that we were tasked to develop.
    - Issued draft guidelines for evaluating differential privacy guarantees that has gone out for public comment. They have received great feedback from the community and are continuing to adjudicate that. Will have that publication ready by its due date.
    - Hosted an SSDF workshop focused on how to apply the SSDF. They are learning through the engagements and anticipate having a draft of that AI SSDF publication out for public comment soon.

AI Safety Institute

- In early February, Commerce Secretary Raimondo launched the AI Safety Institute (USAISI).
    - She announced key members of that executive leadership team to lead the institute that is established at NIST.
    - The Executive Director that was named is Elizabeth Kelly.
        - If you're interested, maybe this platform is a good opportunity to hear from them in the area of progress made between February and the next meeting.
- The AI Consortium has received tremendous feedback from the community. Established more than 200 formal collaborations in support of the consortium that will support both the activities of the AI Safety Institute and our broader implementation of the AI Executive Order responsibilities.
- **Mr. Venables** – mentioned that there are many different government groups on AI: the NSA AI Security Center, there's work at DHS, there's a responsible AI officer at every agency, and there's work going on in OSTP. He asked if there's a council of these groups to make sure nothing is excessively overlapping and that nothing is falling between the cracks?
    - **Mr. Stine** – replied that some of those are probably going to be more focused on information sharing and ad hoc collaborations. There are interagency mechanisms to help with that. Industry is participating in a lot of those different mechanisms, which is a powerful way to help keep us all accountable and to make sure we're talking to each other. His goal is to make sure that NIST produces trusted foundational research and science, and sets of tools and guidance, developed in very open and transparent ways with the community, that can then be used as the foundation to support other AI activities across the government.

Staff Recognition

- NIST Fellow
  - Mary Theofanos
- Commerce Gold Medals
  - Dylan Yaga for improving law enforcement, DHS, and U.S. Border Patrol operations by identifying over 1,000 errors in biometric data exchange standards.
  - Greg Cooksey, Paul Patrone, Anthony Kearsley, and Matthew DiSalvo for the invention of serial cytometry, a revolutionary technology for cancer diagnostics and therapeutic evaluation.
  - John Jones II, Karen Reczek, Allison Getz, Donna Sirk, Barbara Guttman, Marcela Najarro, Alan Zheng, Will Guthrie, and John Butler for extraordinary national leadership in improving the scientific quality of forensic practices through standards development.
  - Peter Bajcsy and Carl Simon, Jr. for developing a suite of tools used to characterize a first-of-its-kind tissue-engineered product for treatment of macular degeneration.
- Commerce Silver Medals
  - Kristen Greene, Shanee Dawkins, Yee-Yin Choong, Mary Theofanos, Scott Ledgerwood, Kerrianne Buchanan, Susanne Furman, Kevin Mangold, and Adam Pintar for giving a vital voice to U.S. first responders' communication technology needs in law enforcement, firefighting, and emergency services.
  - Monique Hunter, Scott Jackson, Jason Kralj, Stephanie Servetas, and Blaza Toman for the development of a first-of-its-kind biologically stable water quality standard that modernizes recreational water surveillance.
- NIST Bronze Medals
  - Ann Virts, Ya-Shian Li-Baboud, and David Schmitt for developing innovative metrics, test methods, artifacts, and datasets that measure the performance and safety of exoskeleton wearable robots.
  - Julie Haney for leading and developing NIST's Usable Cybersecurity Program, transforming how government agencies view the human element in cybersecurity.
  - Martin Stevens, Ralph Jimenez, Charles H. Camp, Jr., and Thomas Gerrits for refuting published claims about quantum-enhanced microscopy by careful measurements of molecular absorption of photon pairs.
  - Michael Indovina, Robert Snelick, John Garguilo, Andrew McCaffrey, and Sheryl Taylor for the creation of innovative software to help fight communicable diseases by ensuring that clinicians have accurate vaccine recommendations.
  - Michael Nelson, Blaza Toman, David Newton, Johanna Camara, Lane Sander, Amanda Koepke, and Katrice Lippa for development and deployment of a statistical tool for experiment design and rigorous assessment of measurement uncertainty for chemical analysis.
    Nader Moayeri for collecting a set of BLE RSSI data and evaluating the performance of various proximity detection methods to blunt the spread of infectious diseases.
- Director's Award for Excellence in Administration
  - Melissa Banner et al for development of the Administrative Management Portal to centralize precise training and resources for the NIST administrative management community.
- George Uriano Award

    - Timothy McBride, Sanjay Rekhi, et al for positioning NIST and DOC to successfully implement core CHIPS for America Act programs to revitalize US leadership in semiconductor manufacturing.
- Judson C. French Award
    - Blaza Toman et al for development of the first glycan SRM for accurate quantification of N-linked glycans in monoclonal antibody therapeutics.
- Ron Brown Excellence in Innovation Award
    - Greg Cooksey, Paul Patrone, Anthony Kearsley, and Matthew DiSalvo for pioneering real-time, cell-by-cell analysis for early cancer diagnosis, the evaluation of novel therapeutics, and accurate clinical decisions.

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

Mandatory FACA Ethics Briefing

Andrik Massaro, DOC Ethics Office

Introduction

- OGE 450 Release
    - He knows this was requested of the board members in a rushed fashion. There was a miscommunication with the programmatic end and he hopes that can be resolved by the end of the day Thursday.

Special Government Employees (SGE) & Other Advisory Committee Members

- Any executive branch employee or contractor may serve as a member of an advisory committee.
- Three main types that go on FACA boards:
    - Special Government Employees
        - Serve on advisory committees and are appointed to exercise their own individual best judgment on behalf of the government.
        - They will discuss and deliberate in a manner that is free from conflicts of interest.
        - Have a less restrictive set of responsibilities competed to a typical employee.
    - Representatives
        - Not a government employee.
        - There to provide points of view from non-governmental entities or other interest groups.
        - Expected that these individual representatives will have some kind of bias as opposed to an SGE or a regular government employee.
    - Regular Government Employees
        - Individuals who are already federal employees who are simply assigned to serve on the committee.

Special Government Employees (SGEs)

- Their service is a temporary government service which cannot exceed 130 days during any 365-day period, regardless of compensation.
- Subject to less restrictive conflicts of interest requirements and ethics rules than typical federal employees but are subject to more restrictive requirements than non-employees who are not covered by the conflict-of-interest laws.
- If an SGE unexpectedly serves for more than 130 days, they still are an SGE for that year. However, we generally advise an SGE not to do this as, during the next 365-day period, the appointing official should reevaluate whether the SGE should still be designated as an SGE.

  - Generally, any part of a day on which you perform any work for the Government for which you are compensated should be counted as a day, regardless of the amount of time worked that day or the nature of the services.
  - Any part of a day in which you substantively serve the Government counts.
  - However, uncompensated activities limited to strictly administrative matters, uncompensated brief communications, and uncompensated brief periods of reading or other preparation performed at a setting away from a government workplace, need not be counted.
- When are you acting as an SGE and when are you not?
  - The key delineation is when you're doing substantive work for the board, you are acting as an SGE in this capacity. If you're an SGE for a different board, or for a different agency, it's essentially the same rule.
  - It's when you're acting substantively for that position. If at the end of the day we gavel out and you go participate in some kind of other function, you would not be participating as an SGE, but this entire day would count towards the 130 days, regardless of how long you spent here.
  - It's critically important you keep track of your days, if you're nowhere near the 130 days, it's less important, but I would still generally recommend keeping track of your days and your time worked.
  - **Mr. Lipner** – stated that the board meets 6 days a year, and then there's some email.
  - **Mr. Massaro** – commented that if there's substantive work, that would generally count [as a day]. He doesn't know what kind of preparation is put into these meetings, but he's getting the impression that no one will be anywhere near those 130 days.

Common Questions

- Do the ethics rules apply to you if you receive no pay from the Government?
  - Yes, they do. The definition of an SGE includes those who serve "without compensation." Doesn't matter if it's compensated or uncompensated. Ethics regulations apply to you. Please understand that different ethics rules apply to people in different positions, whether you're an SGE, regular employee or representative.
- Do the ethics rules apply on days when you perform no Government services?
  - Yes, they do. They apply equally on days you serve the Government and on days you do not. With certain restrictions, some ethics requirements only apply to when you are working on behalf of the government.
  - Some of these restrictions can be nuanced and can be difficult to glean from just a simple reading of either the criminal statutes or the federal regulations. If any of you have questions, we encourage you to reach out to the Ethics, Law, and Programs Office, its ethics division idoc.gov.

Ethics Program Requirements

- SGEs are required to complete ethics program requirements prior to participating in deliberative meetings. A meeting where there is a presentation and you asked questions is not a deliberative meeting. The only deliberative meeting based on an understanding of the agenda from our office is that final hour in which you are considering recommendations.
- Annually this includes:
  - Filing a new entrant financial disclosure report.
    - For most SGEs, this will be the Confidential Financial Disclosure Report (OGE 450) filed electronically through FDonline (Intelliworx)
    - This report must be filed and certified before SGEs participate in deliberative meetings.
  - Receiving live ethics training before participating in deliberative meetings.

- **Mr. Venables** – mentioned that he has an OGE 450 prepared for submission to two other federal government programs he's involved with. The Intelliworx tool is atrocious. He asked if he could submit that full OGE document? It's all signed off and accepted by two other government agencies.
  - **Mr. Massaro** – replied that would be sufficient. He added the caveat that other agencies may have different restrictions and may want you to file with their system.

Restriction on Non-Federal Activities

- Special Government Employees may not:
  - be a registered lobbyist.
  - be a registered foreign agent, the definition of a foreign agent under the Foreign Agent Registration Act or FARA;
  - represent someone or receive compensation due to someone else's representational activities (such as a partner's) before a federal agency or Federal court; The basic gist is you're not allowed to represent someone else to the federal government.
    - **Ms. Flynn Goodwin** – asked how that works if you're an attorney?
      - **Mr. Massaro** – replied that it's very difficult. Essentially, you're not allowed to practice at all in federal court. There are certain circumstances when you could be in a state court in which the federal government is a party. Very rare, though. You are allowed to, in your personal capacity, make public comments. When you're an attorney and in-house counsel, filing on behalf of your employees or your company, in general, this restriction would be triggered. He will talk with his chief to get more clarification on this.
    - **Mr. Lipner** – commented that NIST and DHS CISA in particular, issue public RFIs, and organizations or people on this board respond to those. Are our board members forbidden from making that response or being part of the development of that response?
      - **Mr. Massaro –** replied that he's not sure about being part of the development of the response, but in the actual act of representation and responding with your name on that bottom line, that would be strictly prohibited.
      - **Ms. Flynn-Goodwin** – commented that this is an important point. He's essentially taking every expert who's advising the government out of the process of helping their companies file comments with the government on the issue they're seeking input on.
      - **Mr. Groman –** added that there is some nuance here and his focus has always been on making sure he doesn't represent his clients before the FTC for example, because they call him all the time.
      - **Mr. Massaro –** replied that it's the representational activities that invoke the federal prohibitions.
  - be paid for teaching or writing about programs, policies, and operations of Commerce.
  - be employed by a foreign government, unless your only Federal service is as a member of a Federal advisory committee; or
  - engage in political activities during days of Federal service.

Conflicts of Interest Statues

- As SGEs, you are subject to certain criminal conflict of interest statutes, including:
  - 18 U.S.C. § 201: Bribery - You may not seek, accept, or agree to receive anything of value in return for being influenced in the performance of your SGE official acts.
  - 18 U.S.C. § 219 – Lobbying – You may not serve as a representative of a foreign principal that requires registration under the Lobbying Disclosure Act or the Foreign Agent Registration Act

- 18 U.S.C. § 207 – Post-Government Employment Restrictions – Following your SGE service, you will be subject to certain representational restrictions, which will limit your ability to represent others, with the intent to influence the US Government (not likely to apply to your service).
  - All SGEs: The lifetime post-employment restriction on any particular matter involving specific parties (where you participated personally and substantially) applies to you.
  - Seek ethics guidance for more specific information on what representational restrictions may apply.
  - **Mr. Lipner** – stated that the slide says, "particular matter". He doesn't believe that the ISPAB has ever dealt with a "particular matter" in its lifetime.
    - **Mr. Massaro –** replied that he understands that it can be as narrow as a particular matter involving specific parties, or, and this is the one that's more likely to be triggered, a particular matter of general applicability. There are specific circumstances where it would fit under the definition of a particular matter and in which it would apply generally. Just understand that if someone is asking you to represent them on a matter in which you specifically participated in here or in any other position as an SGE, that's a complete no go. There's no temporal limit, it's a lifetime ban. As I said before, speak with ethics guidance for clarification on that.
- 18 U.S.C. § 209 – Supplementation of Salary – You may not receive salary or supplementation of salary from any source other than the United States for work as an SGE. Most of you have other sources of compensation so this restriction is only related to your work as an SGE. The way this typically comes up is people offering specific gifts which can be interpreted as sources of income.
- SGEs may be prohibited from compensation for teaching, speaking, or writing when the activity is related to their SGE service. General rule of thumb, if you're going to teach, speak, or write about specific circumstances or specific information that was a part of this FACA or any other work you did as an SGE, that is something that should be cleared through program counsel.
- **Mr. Venables –** commented that everything done in ISPAB is public. There's nothing confidential discussed here.
  - **Mr. Massaro** – replied that it's still a good idea, prudentially, to speak to your program counsel about teaching, speaking, and writing just because it invokes additional restrictions and to include the ethics division.
    - You're all experts in your field. If you were to go speak in your personal capacity as an expert, it might tangentially relate to something you've done on this board or as an SGE but that wouldn't be invoked by the restriction.
- Representing Others before Government - You may not communicate or appear, or accept compensation for such representation, on behalf of another back to the Government in connection with "particular matters involving specific parties" (e.g., contracts, grants)
  - In which you participated as an SGE through decision, approval, disapproval, recommendation, the rendering of advice, investigation or otherwise; or
  - Which is pending at DOC, if you have served more than 60 days in the immediately preceding 365 consecutive days. (Ref: 18 U.S.C. § 203 and 205)
- Financial Conflicts of Interest
  - You may not participate in any particular matter, which will have a direct and predictable effect on your financial interests or those imputed to you, unless you qualify for either a regulatory exemption or a written waiver. Written waivers are typically rare, but they're more likely to be granted for an SGE because you are experts, and your skills are rare, making it harder to find individuals who can step into your position.

- It's not just your financial interests, it's the financial interests of those who are imputed to you. That includes your spouse, a minor child, general partner, an organization for which you serve as an officer, Director, Trustee, general partner, or employee. (Individual contractors do not count.)
- Also, a person or organization with which the employee is negotiating or has an arrangement concerning prospective employment. I just want to make clear on this point that there is a delineation between seeking employment and negotiating employment. Simply sending out a job application wouldn't invoke an imputed financial interest to you, but if there's an offer on the table that would be a specific circumstance in which the financial interest of your prospective employer is imputed to you. This applies for an SGE at all times. It means in your capacity as an SGE, you cannot take a part in a particular matter, which will have a direct and predictable effect on the financial interest of your employer.

- Particular matter means anything involving deliberations, decisions, or actions that are focused upon the interests of specific persons or entities or an identifiable class of persons or entities. The Government interprets this term broadly.
  - Not broad policy options or considerations directed toward the interest of a large and diverse group of people.
  - May involve specific parties (e.g., a contract, grant, or case in litigation)
  - May be of general applicability (focused on the interests of a discrete and identifiable class of persons, such as an industry)
- Direct and predictable effect means there must be a close causal link between your SGE work and the financial interest.
  - The impact must not be "speculative" or dependent on events that are independent of and unrelated to your SGE work.
  - It is not necessary to know the magnitude of the loss/gain.
- Financial Conflict of Interest Exception for FACA members working on "Particular Matters of General Applicability": SGEs benefit from a specific exception to the financial conflict rule, which permits SGEs serving on FACA committees to participate in particular matters of general applicability where the disqualifying financial interest arises only from the SGE's non-Federal employment or prospective employment.
- This exception is subject to several important limitations:
  - the matter cannot have a "special or distinct effect" on either the SGE or the SGE's non-Federal employer, other than as part of a class;
  - the exception does not cover interests arising from the ownership of stock or other financial interests in the employer or prospective employer, and;
  - the non-Federal employment must involve an actual employee/employer relationship as opposed to an independent contractor (such as certain consulting positions).
- **Mr. Scholl –** asked when this applies for an SGE? He knows it applies when we're doing deliberations in these meetings but what about a month from now, representing his company at an ISO standards body?
  - **Mr. Massaro –** replied that you would be prohibited from doing an official action that has a direct and predictable effect on the financial interests of either your or anyone that's imputed to you.
  - **Mr. Lipner** – clarified that if he's representing his organization at an ISO standards meeting, he can represent their position at that meeting without triggering a conflict?
  - **Mr. Massaro –** replied that would not trigger a financial conflict of interest. He recommends reaching out to him with concrete examples/details if in doubt so that he can provide more

specific guidance. There must be a close causal link between your SGE work and the financial interest. It can't be attenuated or speculative and the amount or degree of the financial interest isn't relevant. If there's any kind of direct and predictable effect on the financial interest, even if it's minor, this prohibition would be triggered.

Impartiality Conflict

- As an SGE you are prohibited from participating in particular matters involving specific parties (e.g., contract, application, claim), that will have a direct and predictable effect on the financial interests on a member of their household, or a person with whom they have a covered relationship, if they believed a reasonable person would question their impartiality.
- In essence, SGEs should not participate if it could raise the appearance of a loss of impartiality or where the SGE has concerns that their impartiality will be questioned (Ref 5 C.F.R. § 2635.502).
- This is a conjunctive standard, meaning if there's a conflict of interest arising from a covered relationship, the prohibition is only triggered if, in addition to the financial conflict, there is an appearance of impropriety.
- Covered relationships include:
  - Persons with whom you have or are seeking business or financial relationships (e.g., prospective employers or clients)
  - Household members
  - Close relatives
  - Employers and clients of your spouse, parents, or dependent children (and their prospective employers and clients)
  - Recent former non-federal employers and clients (which includes anyone who was an employer or client within the past year
  - Organizations (other than political parties) in which you are an active participant.
- SGEs are likely to have employment other than their U.S. Government position. It is important that SGEs consider whether such non-federal employment, or other personal activities, conflict with their government duties.
- SGEs are required to disqualify themselves from participating on matters in which an outside employer, or an organization in which they serve as an officer or board member, has a financial interest.
- SGEs may not serve as an expert witness (un/paid) in Court or before an agency in matters in which you participated as an employee or SGE in the particular matter that is subject of the proceedings.

Gifts

- Generally, SGEs may not solicit or accept a gift that is offered either:
  - Because of their position as an SGE, or
  - From anyone who has or is seeking business with or action from the Department of Commerce, is regulated by Commerce, or has interests that can be affected by performance of your federal duties.
- Exceptions may apply and permit SGE to accept gifts. For example:
  - based on their outside business or employment relationships
  - from relatives or friends
- What is a gift? Anything with monetary value, but not
  - Items of little intrinsic value intended for presentation only.
  - Light refreshments (non-alcoholic)

Misuses of Government Resources

- SGEs may not use (or allow the use) of:
  - their SGE title/position or Government affiliation for your private gain or the private gain of another, e.g., infer governmental endorsement.
  - SGE may refer to your official position as part of general biographical information.
- SGE may not disclose or misuse non-public or other protected Government information.
- SGEs generally do not provide official statements or speeches on behalf of Commerce. If you are asked to do so, please contact your DFO.

Hatch Act

- Federal employees may not engage in partisan political activities while on duty, in an official capacity, while in a federal workplace, using government equipment, or in a government vehicle
  - "Political activity" is any activity directed toward the success OR failure of a political party, partisan political group, or a candidate for partisan political office.
- General Restrictions:
  - SGEs may not wear partisan political buttons or engage in political activities while in an SGE status or in a workplace where you are performing your duties.
  - Solicit, collect, or receive political contributions.
- SGEs are covered by the Act only during the time that you are actually performing government business. (Ref. 5 U.S.C. §§7321 - 7328).

Expectations for Non-SGE Members

- RGE are federal employees and subject to the full complement of government ethics rules and regulations.
- REP members are not subject to any ethics rules and regulations; however, they are expected to:
  - Avoid misuse of government resource, whether resources, such as equipment and supplies
  - Avoid disclosure of nonpublic information - Depending on the nature of the information, improper use or release may result in criminal charges (such as for misuse of national security information) or civil liability (such as for misuse of business proprietary information or information covered by the Privacy Act).
  - Avoid misuse of government affiliation - Representatives may not use their association with the Government, including business contacts obtained through their work with the Government, to obtain personal benefits or favors for themselves, friends, relatives, or business associates.

President's Council of Advisors on Science and Technology (PCAST) Report Update

Phil Venables, Google Cloud

Introduction

- The PCAST group advises the President on Office of Science and Technology Policy (OSTP).
- Eric Horvitz, the Chief Scientific Officer of Microsoft, and Mr. Venables co-chaired a working group to drive recommendations on cyber-physical resilience.

Purpose

- Motivation behind the group:
  - Our society is becoming more of a digitized integration of cyber and physical systems.

  - Keep advocating for thinking about resilience.
  - To think about moving away from the classic, 'every time there's an event, let's figure out how to prevent that event', and start thinking about why that event was impactful.
- The tone of the report is how to think about, not just more preventative controls, but about resilience.

Four Groups of Recommendations

- First, setting more aggressive and ambitious performance goals
  - Making sure that each critical infrastructure sector started talking in terms of setting minimum viable delivery objectives.
  - An example of a minimum viable delivery objective would be that no more than 10,000 people should be without clean drinking water for more than five days; another would be that organizations should not be unable to pay their employees for more than five days.
  - Shifting a lot of the cyber performance goals from being lagging indicators of breaches and incidents and vulnerabilities more towards leading indicators of "how do we prescribe what should happen that creates the environment that drives cyber resilience."
- Second, research and development and more advanced activities.
  - Align the different federal agencies' R&D plans around a more common objective and cyber resilience.
  - Create a National Critical Infrastructure Observatory.
    - A digital twin of the U.S. critical infrastructure where we can analyze various ways to look for hidden dependencies and concentration of risks that we can use in preparedness for events to look for common vulnerabilities.
- The third group of recommendations are mainly directed towards the government to improve the resources and capabilities in sector risk management agencies (SRMA).
  - Few SRMAs have sufficient resources and expertise to do what they need to do.
- Fourth group of recommendations are mainly directed to the private sector to connect the "tone at the top with resources in the ranks."
  - Executives of pretty much every company will never say anything other than 'cybersecurity and resilience is the most important thing we absolutely have to do' and then they go about their day. The real thing we have to do is make sure that they're creating the environment in their organizations to actually do the investments that make a difference.
  - This also includes how each government agency should continue to seek the relevant authorities through either its SROs in the industry, or through actual regulation, that compels the adherence to minimum viable performance goals for that sector.
- **Ms. Flynn Goodwin** – asked if there were any deliberations looking forward towards whether AI needs to be treated as its own critical infrastructure either now or at some point in the future?
  - **Mr. Venables –** replied that they did talk about AI in the context of it being seen in the context of existing risks. Many people are concluding that most of the risk of AI is contextual in a specific sector and should be handled by the regulations in that particular sector. You don't necessarily need anything other than the AI Bill of Rights and the AI principles, etc., that the federal government is putting out.
- There's going to be more inbound coming from DHS and other places to work with NIST and others on the next steps of the cyber performance goals to shift in line what we've been talking about.
  - **Mr. Scholl** – added that OSTP has already reached out to the NITRD working groups, asking for feedback and to start putting together the committees to flesh out what an implementation plan would look like to achieve some of the strategic goals.

- **Mr. Venables –** commented that they're going to be working with OSTP on some implementation summits, for example the National Critical Infrastructure Observatory is going to need an implementation summit between the PCAST members, OSTP, NIST, DHS, and some FFRDCs that have already been working on this.

The Chair recessed the meeting for a 60-minute lunch break.

CISA Software Attestation

Shon Lyublanovits, CDPSE, C-SCRM PMO Lead, Cybersecurity Division, Cybersecurity and Infrastructure Security Agency (CISA)

Introduction

- Disclaimer: I am not a representative of OMB. I am here to provide my very best representation of CISA and the fantastic work that everyone did to support the development and the release of the Secure Software Attestation Form.
- Starts with Executive Order 14028 and the first release of M-22-18 and the subsequent release of M-23-16.

Next Steps

- Thank you to all who provided comments. We received wonderful feedback that was integral in helping us get this released.
- Over the next few weeks, we will be talking about the work that we're doing and answering any questions you have. However, understand that we're going to be limited in some of the things that I can provide, at least for the next couple of weeks.

Progress Update

- Launched the first iteration of the repository and folks can now register.
- Our goal is to have robust security and understanding of how our software producers are securing the software that we're using within the federal government. It's an opportunity to showcase how each are moving the needle in regard to security.
- We will continue to take feedback and position ourselves to make sure that the federal government has a great product they can utilize.

Questions

- **Mr. Lipner** – Do you have any idea yet of what kind of scheduled cadence you're likely to follow in terms of updating attestation?
  - **Ms. Lyublanovits** – I do not have an exact answer to that. We are taking feedback and prioritizing based on the information that we receive. We are going to defer to our OMB partners to really make that decision on what makes sense for us to do next. The main thing we want is for folks to start using it and letting us know where there are areas for us to improve.
- **Mr. Lipner** – There are three sets of considerations I can think of for evaluating or assessing the attestation process and the attestation form. One is how the agencies see the experience of using that and relying on it, one is how the vendors see the experience from the developer perspective, and the third is, are you able to tell whether software that's attested is secure or more secure or there's any improvement in security performance. Have you thought about how you're going to collect information in those three areas?
  - **Ms. Lyublanovits** – Those are three good areas to highlight. What we are telling our federal partners is to contact us via email to talk about usage and how things are going. The second thing

is, as vendors start to fill the form out and log in and work with their agencies is to, again, let us know where there are issues. From a repository standpoint, there's going to be more information that will come out about how to communicate and submit any questions or concerns that you have.

- **Mr. Lipner** – How do you know whether the attestation process is getting you improvement in the security of the software that's being delivered to the federal government?
  - **Ms. Lyublanovits** – That's the whole part about the attestation. It's that trust that the vendor is using sound techniques within the organization and is willing to sign and stand behind that. Unless there's a need for a plan, it's really hard for us to track whether there are going to be additional security items that need to be mitigated. This whole process is really about being able to trust and have confidence that our software producers have good practices.
- **Mr. Lipner** – How are you going to tell if there are things in the SSDF that weren't called out as mandatory in attestation that should have been? Or how are you going to tell if there are things that are missing from the SSDF that, in retrospect, should be added?
  - **Ms. Lyublanovits** – That is a policy question that we have to defer to OMB on regarding some of that SSDF process. We assume that we will continue to work with OMB to define or redefine some of those requirements that were listed in the form itself.
- **Ms. Moussouris** – Is there a mechanism for enforcement or to revoke someone's approved status if it's discovered that the attestation form was misleading or not accurate? For instance, if, in the vulnerability disclosure process, they attest to mitigating a class of vulnerabilities, and they even have a reporting mechanism, but it's not really in compliance with the intent of that control and leads to a "black hole". This can be discovered from the outside where it can be seen they have no mechanism to actually remediate vulnerabilities, is there a plan of action on the government's side?
  - **Ms. Lyublanovits** – Agencies are going to have to leverage their legal counsel because at that point, you have a company that's misrepresented, as well as their acquisition executives. The agency, along with their legal counsel, would have to determine if there's an opportunity to course correct.
- **Mr. Lipner** – The attestation mechanism is a common government wide online site. How much of the process, once the vendor has attested, is common, and how much of it is just my agency?
  - **Ms. Lyublanovits** – That is going to depend. Every software producer will submit. As far as the things that are listed as critical and having to do critical software first, that's going to vary by agency and that part of the process is going to look a bit different.
- **Ms. Flynn Goodwin** – What sort of data analytics are you prepared to do on the form that you get so that you're sharing back some of the bigger conclusions and takeaways just generally across submissions as they start to come in?
  - **Ms. Lyublanovits** – I am going to get back to you on that. Those are part of the feedback mechanisms that we're gathering right now. I've got my team on board taking your questions, so we'll make sure to get that answered for you.
- **Mr. Gantman** – Following the GAO report, any progress on figuring out how to track outcomes from initiatives like this?
  - **Ms. Lyublanovits** – We are working on that. I know, standard quote today.

Administration Privacy Priorities

Dr. Alan Mislove, Deputy Chief Technology Officer for Privacy, White House Office of Science and Technology Policy (OSTP)

Introduction

- Here to share both the administration's vision on privacy as well as the actions that the Biden Harris administration has taken to protect privacy actions that intersect with NIST's goal of identifying and reporting emerging issues relevant to information security and privacy.
- President Biden has been clear that privacy is a critical issue for this administration, and you'll see that reflected in the administration's actions and our priorities.
- My background:
  - Worked on security and privacy issues as a professor before joining the administration in January of 2023 where my research was focused on algorithmic auditing.
  - Goal of my research was to better understand the large-scale real world computing systems that are increasingly influencing our daily lives.
  - I work to develop scientific methodologies to identify when these systems are making decisions that may not live up to our values, such as by making, such as by leaking users' private data, or making decisions to disadvantage protected classes.
  - In this role, I worked in both academia as well as with industry to identify and mitigate problems.
  - Computer scientist by training throughout my career, but have collaborated with lawyers, policymakers, and social scientists, who consider both the design and the regulation of technical systems as essential to protecting democratic values and human rights, as well as our safety, our privacy, and our security.
  - I serve as Deputy Chief Technology Officer for privacy at the White House Office of Science and Technology Policy, otherwise known as OSTP.

Office of Science and Technology Policy (OSTP)

- Team of folks who work to maximize the benefits of science and technology to advance health, prosperity, security, environmental quality, and justice for all Americans.
- Home to the chief data scientist of the United States, the Office of the United States Chief Technology Officer, and the National AI initiative office.
- Have a key role in helping to advance privacy work across the federal government.
- We work with the private and public sectors, as well as with civil society and our international partners to ensure that technology and data support the public interest. This multi stakeholder approach to Science and Technology Policy is a hallmark of OSTP work.

Privacy Needs

- There has never been a more important time to ensure that technology that works for every member of the public, protects our privacy, our safety, and our security, and reflects democratic values and human rights.
- Privacy is a cross cutting issue that affects us all and the Biden Harris administration is committed to safeguarding it. President Biden has been clear about the need to better protect Americans privacy.
- In an op ed from January 2023, the president highlighted three critical needs, all of which significantly impact privacy.
  - Need for serious federal protections for Americans privacy. He called for clear limits on how companies can collect and use and share personal data, as well as stronger protection for kids and children online.
  - Technology companies need to take responsibility for the content they spread and the algorithms they use. The President called for far more transparency about algorithms and its effect on women, minorities, and children, and especially how it affects their mental health and their safety.

  - Need to bring more competition back to the technology sector. President Biden noted that fairer rules of the road would lead to an economy where everyone can compete on a level playing field and America can strengthen its leadership and cutting-edge innovation.
- President Biden continues to call on Congress to do its part to pass comprehensive bipartisan privacy legislation, especially to protect American servicemen and women and our children.
- In August of 2023, OSTP, along with other components of the White House, co-hosted a Roundtable:
  - Subject was on protecting Americans from harmful Data Broker practices. In an era where our daily lives are increasingly being surveilled for data, the administration has recognized the urgent need to protect Americans from these data brokers and their practices.
  - At this event, the Consumer Financial Protection Bureau or CFPB, announced that they were launching a rulemaking to ensure that modern day digital data brokers are not misusing or abusing our sensitive data.

Privacy Risk

- AI is one of the most powerful technologies of our times, and AI systems are increasingly touching every aspect of our lives.
- These systems have brought significant benefits across a wide range of domains, but at the same time, as President Biden has said, to seize all of those benefits of AI, we need to first manage its risks.
- Examples of Privacy Risks:
  - High quality images and text being used to deceive consumers.
  - More and more sensitive information being used to train AI systems like facial recognition, further eroding privacy.
  - The harms of AI are often disproportionately felt by those communities that are already underserved, such as how AI is being used to create and distribute nonconsensual intimate images of women and girls.
- These systems are having dramatic impacts on Americans lives, putting our rights, our safety, and our privacy at risk.
- President Biden's Executive Order
  - To ensure that America leads the way in seizing the benefits and the promises of AI while also managing its risks, President Biden issued an executive order on the safe, secure, and trustworthy development and use of artificial intelligence. The first significant action that any government in the world has ever taken on AI.
  - Purpose of the EO
    - Directs the establishment of new standards for AI safety and security,
    - The protection of Americans privacy,
    - The advancement of equity and civil rights,
    - It stands up for consumers and workers,
    - Promotes innovation and competition, and
    - Advances American leadership around the world.
  - Directs the Office of Management and Budget, otherwise known as OMB, to issue guidance on how federal agencies can use AI responsibly.
  - Tasks the director of OMB to evaluate and identify commercially available information procured by agencies, particularly those containing personally identifiable information. This includes data procured from data brokers and processed indirectly through vendors.
  - The President also tasked the director of OMB with exploring potential revisions to the guidance that agencies use to implement the privacy provisions of the E Government Act of 2002. These

provisions are what agencies use to conduct privacy impact assessments whenever they develop or procure new information technology that involves the collection, maintenance, or dissemination of information in identifiable form.
    - Directed further work into utilizing privacy enhancing technologies otherwise known as pets. These technologies including things like encryption, differential privacy, synthetic data generation, secure multi-party, computation, and others, are critical to help address privacy current concerns as data becomes more ubiquitous. The administration is working to identify places where they can be used to protect Americans privacy across the federal government.

AI Bill of Rights

- We have to be clear about our values, and how those values should be embedded into the systems that are influencing our lives.
- In October 2022, OSTP released the blueprint for an AI bill of rights as a guide for how to leverage AI technologies in ways that reinforce our highest values and help protect society from its risks. It is a set of practices for government and industry.
- The blueprint includes data privacy as one of the five key principles that should guide the design, use and deployment of automated systems to protect the American public in the age of artificial intelligence.
- Since releasing the blueprint, the administration has been hard at work to move those principles into practice.

Facial Recognition Technology

- A key area of AI that brings up significant privacy concerns.
- The administration has been vigilant in protecting the public from the misuse of facial recognition technologies. When this technology doesn't work, or when it's used irresponsibly, we've seen invasions of people's rights to privacy, violations of fundamental First Amendment freedoms, and false matches and wrongful arrests, all of which disproportionately harm people of color.
- If we use this technology, we must use it responsibly.

Impact on Children

- The President has been particularly focused on the impact that online services are having on children.
- Online platforms often use manipulative design techniques embedded in their products to promote addictive and compulsive use by young people to generate more revenue.
- Social media use in schools is affecting students' mental health and disrupting learning.
- Advances in AI could make these harms far worse, especially if not developed and deployed responsibly.
- Interagency task force on kids' online health and safety:
    - Stood up in May 2023 to advance the health, safety, and privacy of monitored minors online.
    - This taskforce will recommend measures and methods for assessing, preventing, and mitigating current and emerging risks and a harm to minors associated with online platforms.
    - It will develop a research agenda relating to online harms and health benefits and recommend best practices and technical standards for transparency reports and audits related to online harms to privacy, health and safety for children and teenagers.

Questions

- **Mr. Groman** – You mentioned initiatives that OMB might be doing. President Obama established the first ever privacy branch and it's been decimated. There's no one there left who has that deep knowledge required to achieve these initiatives. Who at OMB is going to be taking this role on?
  - **Dr. Mislove** – OMB would be in the best position to answer this question. I am aware that the privacy branch is searching for a new team. There is a job advertisement for a new head of the privacy branch. But even in the interim, they are you know, we are actively engaged with them.
  - **Mr. Groman** – I think that this board would love you to go back and say, if, as the speech says, this is a priority for President Biden, having no one in the privacy branch, given this breath of work, strikes us as incredibly problematic.
  - **Dr. Mislove** – I will convey the board's comments and concerns on this. It's something that we care deeply about, as well, because of the commitment to privacy.
  - **Mr. Groman** – If you're outside the government listening to these commitments, but then you look at where the resources are, we have some concerns that this is not adequately resourced giving the commitment. We think your team is excellent and we're glad that you are doing what you're doing, but you can't do it alone and the resources have not been allocated elsewhere. OMB being the worst example.
  - **Dr. Mislove** – Thanks very much for your concern and paying attention to this.
- **Mr. Gantman** – If you zoom out and look at the overall cumulative privacy protective measures, do you feel like they're keeping up with the rate of deterioration of privacy? Overall, are we still moving in the right direction or the wrong direction? Is the needle moving in the right direction with all these efforts?
  - **Dr. Mislove** – The availability of data today has exacerbated existing privacy concerns, but also brought up a tremendous number of new privacy concerns and one example of that is AI. There's certainly recognition within the administration that we are facing unique sets of privacy challenges, both in terms of the number of those challenges, as well as the type and the novelty. We are doing our best to keep up. There's a lot of emphasis on using privacy enhancing technologies and looking for places that we can embed the use of privacy enhancing technologies within the government. As the President has called for, we do need comprehensive privacy legislation in this country, and we hope to see additional action on that as well.
- **Mr. Groman** – The administration has done, and is pushing the envelope, on their current authorities. I thought the AI executive order was outstanding. Whether we can implement this is the question, but they are using their current authorities. Congress has to act. If any of us want more privacy rights, it requires legislation. Until Congress acts to protect kids or manage general privacy, whatever it is, their authority is limited. We have to have that congressional action and that limits what they can do. Do you agree with that?
  - **Dr. Mislove** – Yes, we are doing everything that's within our power to try to do that.
- **Mr. Lipner** – I share Mr. Gantman's concern with regard to whether we're getting ahead or behind. It feels to me like the problem may be that it's very fragmented and that seems to be working against progress. Are people coming out with fundamental research on the underlying results that say 'this is a way to move the bar' or are we doomed just fight this incident by incident or new system by new system?
  - **Dr. Mislove** – Since we don't have comprehensive privacy legislation in the United States, you're seeing a lot of action in domains where there are authorities under privacy. For example, the FTC, the CFPB, other agencies like that are working in that space. We are looking at what are some of the most critical places where privacy is impacting people and what can we do? One example of

that is the kids online health and safety task force, which has representatives from multiple agencies to try to identify other actions and best practices for industry to better protect privacy.

- **Mr. Lipner** – Is there any equivalent in the privacy space where there are fewer mechanisms or requirements or classes of policies or technologies that can be applied more broadly? I feel like if you have to fight this bug by bug, you're doomed?
  - **Dr. Mislove** – There's a lot of work in what's called privacy enhancing technologies. A few of those, I'll point you to that. We've seen a lot of interesting things happening. One is called synthetic data generation. The idea being if you have a dataset that's particularly sensitive and you want to let researchers study that dataset, but you're worried about revealing information, there is a lot of research into how you can create a synthetic version of that data set that shares many of the properties the original data set, but does not reveal private information, it's entirely synthetic. We're also seeing other technologies, for example, the use of differential privacy as a way to reveal statistical information without worrying as much about revealing information about individual people.
- **Mr. Groman** – One of the challenges in this AI conversation is the difficulty that is balancing; with identified risks, identified benefits, someone has to decide that it's worth it and that residual risk is acceptable, given the benefits we'll receive. We need more of that out of this OMB process, and it would complement the NIST work. Together would help create more consistency and guidance that's currently very helpful.
  - **Mr. Lipner** – agreed with Mr. Groman. These types of guidance or polies or case studies would help enable companies or agencies to make better decisions.
- **Mr. Gantman** – It almost feels like we've given up before we even get started. I don't think we would ever again see the world where I can get into a car and drive across town, buy a coffee, and not leave a permanent digital trail with a dozen different companies. What we're saying is, if we try really, really hard, maybe we can limit it to just a dozen companies and half a dozen government agencies, but they can't resell it to 1000 other companies. They can only use it to extract money from you in somewhat acceptable ways. This notion of privacy where you can do things in private and there's never a permanent record of it, in many cases, it just may be gone.
  - **Mr. Scholl** – Yes, it's a very different sense of privacy that we're trying to protect now. It may be being explicit about that. Researching what is still achievable, and what is no longer achievable, basically Baseline Privacy expectations. That expectation of what privacy is, might be very different than potentially future different generations of more tech.
  - **Mr. Gantman** – The point is, to what extent do we care as users? Do I care if it's a dozen companies and not 200 companies? Or whatever the scenario is?
- **Mr. Groman** – We also have the inconvenient truth that the number one client and purchaser of data from data brokers is the United States government. By far, the number one customer is the US government. The point you're making is that it's not that we're not making advancements, but the harms are going up and we are making progress, but it's increasing much less. We are moving directionally right, it's just that we can't keep up. How are you going to navigate the tension between this monumental demand for data for AI models and the inherent privacy problems with that?
  - **Dr. Mislove** – If you look at the executive order there are a number of tasks in there about privacy, specifically about risks of AI, privacy, and so forth because the administration recognizes that. The AI, because of the training data and its ability to understand in many ways what exactly it will output and the risks of that to a number of taskings to NIST to try to better understand that produced guidance and so forth. Things like the AI risk management framework. In terms of data brokers, that is something that is in the AI EO is a tasking to OMB to do that

inventory. You know, to better understand where's the US government purchasing data? What are the risks of that data? In terms of facial recognition technology, that is in both in the AI Executive Order, as well as in the policing executive order that was released in May of 2022, working with Department of Justice, Department, Homeland Security, to better understand the use of facial recognition in the context of law enforcement and to provide guidance to both federal state and local governments on how to responsibly use that technology so that you don't show up in every single database.

AI Risk and Threat Taxonomy

Apostol Vassilev, Senior Researcher, NIST

Purpose

- Today will focus on the risky parts of AI and bringing awareness of the problems or the risks it comes with.
- The risks we will discuss are primarily adversarial risks.

Categories of Risk

- Inherent risks
  - Unwanted bias, hallucinations, errors in the generated data, implementation flaws in the model, cybersecurity flaws in the platform on which the AI/ML models is deployed. Dealt with in other standards, e.g.,
    - 1. NIST SP 1270 "Towards a Standard for Identifying and Managing Bias in Artificial Intelligence".
    - 2. NIST SSDF Companion for LLMs – coming soon.
  - **Mr. Groman** – Why do we use the word hallucinations other than to make it sound less worse than not as bad? How is it different?
    - **Mr. Vassilev** – Many people are raising the same concerns; it may be because of the way these models operate. They try to guess what the next token is in a probabilistic form. There is no hard and fast rule defining what the next token is, there's probabilities. Depending on where probabilities are going to take you, you might take a very random looking path at some point. One of the major criticisms of the current state of technology is that it's not causally bound to reality. It's basically trained on just reading text that describes reality, but it's not reality itself.
  - **Mr. Venables** – With so called things like retrieval augmented generation, where a large language model consults, facts database that could result in a correct or an incorrect answer. Whereas without retrieval augmented generation is literally just generating content that may or may not be based in the fact it was trained on because of that probabilistic part. The errors you get from hallucination are different from the errors you might get from other means of generation. It's a useful distinction.
- Adversarial Risks
  - Deliberate actions by motivated experienced adversaries aiming to disrupt, evade, compromise, or abuse the operation of the model or its output.

Adversarial ML (AML)

- New standard NIST AI 100-2e2023
  - A taxonomy of attacks and mitigations
  - Part of the NIST trustworthy and responsible AI series

  - Maintained annually.
  - NIST will seek comments and recommendations on:
    - What are the latest attacks on the existing AI models?
    - What are the latest mitigations?
    - What are the latest trends in AI technologies that promise to transform the industry/society? What potential vulnerabilities do they come with? What promising mitigations may be developed for them?
    - Is there new terminology that needs standardization?
  - The report is a collaborative effort between representatives from industry, academia, and government that such it provides a collective approach to investigating this issue.
- **Mr. Groman** – Where would you categorize the use of an AI model for unintended purposes, or the use of a model by an adversary or anyone for a way that causes harm that could have been anticipated, but it wasn't built for that?
  - **Mr. Vassilev** – Those risks fall under another category called abuse.

AML Pace
- The report is based on the literature, largely in machine learning, as well as recent reports coming out of deployments of the technology.
- Presented a graph of the number of papers in machine learning on archive starting in 2011 all the way to 2020.
  - Exponential growth
  - If summed up it amounts to about 3500 papers published in this area alone
  - In 2022 we had more than 5000 papers in just two years
- What drives this enormous growth?
  - There are no information-theoretic security guarantees for AI algorithms.
  - Worse, information-theoretic impossibility results have been established, making the security problem intractable in the existing AI paradigm.

Trustworthy AI
- The Seven Attributes of Trustworthiness
  - Valid and Reliable
  - Safe
  - Secure and Resilient
  - Privacy Enhanced
  - Explainable and Interpretable
  - Fair Harmful Bias Mitigated
  - Accountable and Transparent
- We are going to focus on the secure and resilient attributes.

Trustworthy AI Attributes
- Particularly, what's happening between accuracy, fairness, explainability, and how they relate to privacy, adversarial robustness and the like.
- It is not possible to simultaneously maximize the performance of the AI system with respect to these attributes.
  - Accuracy vs. Adversarial Robustness tradeoff
  - Fairness vs. Adversarial Robustness
  - Explainability vs. Adversarial Robustness

  - Privacy vs Fairness
- Organizations need to accept trade-offs and decide priorities depending on the AI system, the use-case, economic, environmental, social, cultural, political, and global implications of the AI technology.
  - **Mr. Groman** – A viable outcome is to decide not to move forward with a given AI model because you can't get the right balance. Right?
    - **Mr. Vassilev** – That's very much the case, you have to make a feasibility analysis before you deploy the technology, being aware of all the factors and all the compromises or tradeoffs you have to consider. At some point, you may conclude that this is not a viable option forward because the risks are too great, and you just can't do it responsibly.

Adversarial ML (AML) cont.

- Four Dimensions
  - Learning method and stage of learning process
  - Attacker goals/objectives
  - Attacker capabilities
  - Attacker knowledge
- ML models can be attacked at all stages of their lifecycle from design to training to deployment and use.
- Methods and Stages of Learning
  - Learning Stages
    - Training
    - Deployment
  - Type
    - Generative
    - Predictive
  - Learning Method
    - Unsupervised
    - Supervised
    - Semi-supervised
    - Reinforcement
    - Federated
    - Ensemble
- Attacker Knowledge
  - Important element in deciding what attackers can do to you.
  - Three different types include:
    - Black box: where the attacker has no idea what the model architecture is, what the model training or learning are, it doesn't know anything about the data set the model was trained on, and so on.
    - White-box: opposite of black-box in that it knows everything about the model.
    - Gray-box: somewhere in the middle where the attacker knows bits and pieces of the whole architecture, they may know some of the datasets, and things like this.

Attacker Goals/Objectives Perspective

- Taxonomy of Attacks on Predictive AI Systems
  - We define three attacker objectives: availability, integrity, and privacy.

- Example of a predictive system that is used is autonomous driving. What the attacker wants to do is to cause the system, the car, to move opposite the direction of traffic, which is a great danger for occupants and other drivers. How do they do that?
  - The attackers work in hopes to deceive the autonomous vehicle into veering off into the wrong direction. Attackers hacked into the computing stack of a vehicle and inserted a piece of software that would put synthetic marks in the image that the car reads off its camera, fooling to car to believe it is going in the right direction.
  - Reference to the paper that described this attack: Jing et al., "Too Good to Be Safe: Tricking Lane Detection in Autonomous Driving with Crafted Perturbations", USENIX 2021.

- Taxonomy of Attacks on Generative AI Systems
  - We define four attacker objectives: availability, integrity, privacy, and abuse.
  - Example of generative system that is used are chatbots.

PredAI AML – Risk Mitigations

- One way of mitigating vulnerabilities in AI is Adversarial Training (AT)
  - The most robust approach known so far.
  - Due to Goodfellow et al. in 2015.
  - Improved by Madry et al. in 2018.
- But, in automotive setting AT is reactive by construction meaning not all road/traffic conditions leading to incidents are known in advance. Actual accident data is fed into the training of the next AI model.
- As powerful as this is and these seem, they don't have the same reasoning abilities as humans yet.

Certifiable Robustness

- Definition: A classifier is said to be certifiably robust if for any input x, one can guarantee that the classifier's prediction is constant within some set around x, often an L2 or L∞ ball.
- In the context of Lp norm-bounded perturbations, for a classifier g, input x, and radius r,
  $g(x) = g(x+ \delta)$, for any perturbation δ such that $\delta \leq r$.
- Given an input (e.g., image) x correctly classified by a neural network an adversary can engineer an adversarial perturbation ε so small that x + ε looks just like x to humans, yet
  $g(x) \neq g(x + \varepsilon)$ - an incorrect class. The relationship between ε and r is not absolute – what is invisible to the human eye may still be too big for AI.

Chatbots

- Training Pipeline for Chatbots
  - Pre-Training: First step in building a chatbot is creating the base model. This is done by acquiring data and the data that's required in this step is actually high quality, low quality. The result this process is unsupervised learning which then leads to a base model, but very rough on the edges.
  - Supervised Fine-Tuning: Next, you label your dataset and do a supervised fine tuning of the base model. You feed it data and put it to use to make sure it responds the way you intend it to. The result of this process is the SSD model that is more aligned with human value.
  - Reward Modeling: The next step is to develop a reward model, where the model generates specific answers to questions and people rate those things is acceptable, unacceptable, and so on. The reward model forces the model to maximize the reward, essentially, to score as many good points as it can.
  - Reinforcement Learning: Next, we perform reinforcement learning where you have the reward model, and you train the model with humans asking questions such that the model learns how to

maximize the reward according to the model they have. The final result is the RLHF model, or essentially, reinforcement learning from human feedback model.

- LLM Project Pipeline
  - What organizations should do in adopting the large language model technology:
    - Define the problem you want to apply the AI to. What is it that you want to automate.
    - Choose a model.
    - Adopt and align the model.
    - Application integration:
  - **Mr. Groman** – Is open source going to have more vulnerabilities or be less secure or less safe than going with a proprietary model with an entity?
    - **Mr. Vassilev** – In terms of security, I don't think that they are more or less secure, it's about the same but with different types of problems. If you are concerned about the best model to use, and this is not an advertisement for closed models, but closed models perform slightly better than open source.
  - **Mr. Groman** –What does it mean from an integration point of view? How do you integrate the model into your enterprise? What does it mean to deploy the model in your enterprise?
    - **Mr. Vassilev** – Starting with the LLM, to make the LLM work well in your enterprise, you have to feed it to the enterprise specific data and that comes in the form of documents or databases, or even connecting to the internet. Next you say so here's your context, tell me about that and the model begins to work. In addition to that, now that the model has captured what it needs to do in your enterprise, you want to enable it to initiate specific actions, whether that is to initiate an email on your behalf to serve as your office assistant, for example, and answer your email, you could do any of that. Or you could trigger other API calls within your infrastructure to initiate actions.

AML Integrity Violations

- Are threats that cause GenAI systems to become untrustworthy.
- Training-time attacks
  - Poisoning attacks – induce failures when poisoning only ~0.001% of data. Large-scale poisoning is feasible!
  - Model fine tuning may also be susceptible to poisoning attacks.
  - Open models open the door to backdoor poisoning attacks.
- Inference-time attacks.
  - Manipulation – instruct the model to give wrong answers.
  - Adversarially or randomly wrong summaries
  - Propagate disinformation.
- Mitigations: security is best addressed comprehensively, including software, data and model supply chains, and network and storage systems
  - Apply and use provenance and integrity checks on datasets and models. List URL's and cryptographic hashes, even PKI certificates when possible.
  - Data sanitization: Beware of limitations in detecting out-of-distribution data. Impossible to distinguish when the distributions overlap.

AML Availability Breakdowns

- Threats that cause a disruption in service with maliciously crafted inputs leading to increased computation or by overwhelming the system with a number of inputs causing a denial of service to users.

- Inference-time attacks.
  - Time-consuming background tasks
  - Muting – misuses the <|endoftext|> token – model cannot finish sentence, resulting in blank generated text.
  - Inhibiting capabilities – a maliciously crafted prompt instructs the model to avoid certain API's.
  - Disrupting input or output – indirect prompt injection instructs the model to replace text with homoglyphs causing disruption in downstream services that depend on correct text.
- Mitigations: Monitor and be prepared to act when a breach is detected. Follow the NIST AI RMF to establish robust governance structures in the enterprise.
  - Inspect user input.
  - Monitor the runtime state of the system.
  - Develop a plan for recovery from a breach. Organizations that are prepared have lower losses than unprepared organizations.

AML Privacy Compromise

- Privacy compromise: Threats that expose sensitive information about users or the model.
- Inference-time attacks.
  - Data extraction
    - Sensitive information leaks
    - Prompt and context stealing.
  - Indirect prompt injection-based privacy risks
    - Information gathering – attacks against personal assistants with access to user data or indirect prompting.
    - Unauthorized disclosure – access information on the connected system infrastructure to gain access to sensitive data through calling into APIs, malicious code-completions, etc.
- Mitigations: Existing methods offer a measure of protection but not full immunity.
  - Training for alignment
  - Prompt instruction and formatting techniques.
    - Distinguish user from system prompts.
  - Detection techniques
    - Tools that detect prompt injections have entered the market.
    - Inspect user input to detect malicious attempts or moderate the firewall for jailbreak behavior.

AML Abuse Violations

- Threats that allow the attacker to repurpose the systems' intended use to achieve own objectives. Generally, these are not model features but harms that manifest themselves in the context of model use.
- Inference-time attacks based on indirect prompt injection.
  - Fraud
    - Phishing – produce convincing phishing scams.
    - Masquerading – pretend to be an official request from a service provider to recommend fraudulent websites.
    - Deep fakes – impersonate people to defraud others.
  - Malware generation
    - Injection spreading – cause the LLM to act as a computer running and spreading harmful code.

        - Malware spreading – LLMs can be used to persuade users to visit malicious sites for 'drive-by-downloads.'
    - Manipulation
        - Historical distortion – output adversarially chosen disinformation. e.g., deny Einstein got a Nobel prize.
        - Marginally related context prompting – steer search results towards specific orientation (non-neutral) to cause bias.
- Mitigations: Existing methods offer a measure of protection but not full immunity. Major changes in the way society governs social media are needed to counter these harms effectively.
    - Reinforcement Learning from Human Feedback
        - Align the model better for the specific use-case.
    - Filter retrieved inputs.
    - Use an LLM Moderator
        - Detect attacks beyond filtering of harmful outputs.
    - Interpretability-based approaches
        - Outlier detection of prediction trajectories. Statistical methods for anomaly detection

Questions

- **Mr. Scholl** – In instances when companies put out chatbots and then the courts decide that the companies have to honor what the Chatbot say, when it's acting on the behalf of an entity, is there any hope of having any sort of confidence that you've constrained what it can say?
    - **Mr. Vassilev** – The short answer is no, but there are techniques you can use to try to limit this from happening such as additional enforcement learning from human feedback to teach it. There is also filtering the inputs to see what makes sense and what does not. You could monitor the output from another model and see if it's good or bad. There is also trying to detect the statistical properties of the output that's generated to see if it deviates from expectation or not. There are many techniques.

Disclaimer

- Certain commercial hardware, open-source software, and tools are identified in this presentation in order to explain our research. Such identification does not imply recommendation or endorsement by the National Institute of Standards and Technology (NIST), nor does it imply that the software tools identified are necessarily the best available for the purpose.

Day Review and Meeting Recessed

No public comment requests were received.

The Chair adjourned the meeting at 4:15 P.M. ET.

Thursday, March 21, 2024

The Chair opened the meeting at 10:00 A.M. ET and welcomed everyone to the call.

NIST Cybersecurity and Privacy Update

Mattew Scholl, NIST

Rodney Petersen, Interim Chief of the Applied Cybersecurity Division, NIST

Post-Quantum Cryptography Update

- Three encryption standards: FIPS 202, 203, and 204
- May still have some associated special publications to specify some of the optional parameter sets that may be decided on in the future.
- May also provide additional guidance.
- Anticipate the end of July to close comments and decisions on the last parameters done.
- Hope to finalize in December.
- After that, we will be finalizing the Falcon signature algorithm in a standard.
- April 10-12: Hosting a workshop in Rockville:
  - Cover both signatures and use cases they might need.
  - Talk about 4th round PKI KEMS they might want to standardize in the future.
- NCCoE PQC Transition Project
  - Collaboration between NIST, CISA/OMB, and industry
  - Helping folks with transition and providing initial guidance around risk management and understanding where and what to encrypt. how to prioritize, and tools and automation techniques for discovering quantum vulnerable implementations within the enterprise.
- Have not determined when we will be deprecating or disallowing the current quantum vulnerable algorithms. Will do that after some initial deployments and lessons learned,
  - Especially need a better understanding of the needs for legacy verification and legacy decryption
- **Mr. Venables** asked if there is a path to update FIPS 140 to permit the use of PQC?
- **Mr. Scholl** replied that there is a lot happening simultaneously. The team that maintains the algorithm test tool suites has spun that up in a next version of the algorithm test capability and is working in parallel with the standards team. Once we know what the final parameter selections are, they just make that switch and that deployment will happen very quickly for the algorithm test piece. On the modules, there's a meeting happening today (3/21/24) with industry and laboratories through the Crypto Module Users Forum, where NIST has deployed a new module test tool capability to the laboratories.
- Issues with validating modules
  - Many issues that we're having with modules are mostly in traceability between the products that are produced out of the lab and NIST. The security plan that the module vendor has, the test report that the laboratory produces, and the certificate that the three of us produce often do not agree.
    - Even though they are produced by different people, they should all agree.
    - It takes time to figure out why they aren't the same. 40-60% of the churn with the laboratories is getting the traceability correct.
  - Have also deployed a tool that harnesses into the laboratory for data entry and output of the test assertions. The lab and the vendor just enter data into the tool and the security policy, test report, and certificate are generated forcing them to have traceability and eliminate the traceability issues.
    - Have deployed a beta version in a couple of labs. There are a few bugs, but it seems to be working as intended.
  - The problem moving forward is that those using the tools will move through very quickly but there is a significant backlog. Today's meeting is to talk about options for those who submitted before the tool was available.

- **Mr. Venables** asked about timelines [for updating FIPS 140]. There is a concern with some companies thinking they are going to be blocked if they implement PQC because FIPS 140 certification isn't lined up to certify PQC yet.
- **Mr. Scholl** replied that they will communicate that concern to the FIPS 140 team.
- Continuing to standardize a lightweight algorithm.
  - It is an algorithm that people have asked for due to specific use cases.
  - It will not be the recommended algorithm for general purpose implementation.

Privacy Enhancing Technologies (PETs) Research

- Privacy enhancing cryptography. Zero-knowledge proof. Secure multi-party computation, Full homomorphic encryption, Group ring signatures
- Would like to have these PETs use current approved known primitives (AES, SHA), otherwise they will need to figure out the best methods, techniques, and capabilities for implementation.
- **Mr. Lipner** asked if they are transitioning them to post-quantum?
- **Mr. Scholl** replied that, where applicable, it is part of the plan. They are also looking at new block cipher modes that are wide block, more like a sponge function, but also safer to use, easier to implement, and more misuse resistant. There are a lot of good modes, but some are tricky and easy to implement poorly.

New Interim Chief, Applied Cybersecurity Division, NIST Introduction

- Rodney Petersen – temporarily replacing Kevin.
- Top priority is to hire a permanent chief.
- Has been at NIST 9 years as the NICE director.

Applied Cybersecurity Division Activities

- Education and Workforce development
- NCCoE
- Identity Management, Internet of Things (IoT), Privacy, and Cybersecurity Framework (CSF)
- New leadership
  - Cheri Pascoe – NCCoE Director
  - Naomi Lefkowitz – Group manager for Privacy, Identity, and IoT
  - Rodney Petersen – continuing in the role of NICE director as well as interim Chief.
- NCCoE Projects
  - Focusing on community profiles for the CSF
    - Addresses sectors, technologies and different use cases
    - Have developed a new guide that organizations can use for these profiles.
    - The financial service sector has updated its sector profile to reflect the new CSF version.
    - Working on helping other sectors update their profiles to the new CSF.
  - Data confidentiality
    - Recent publications on identifying and protecting assets against data breaches.
    - Held an event in January with the state of Maryland and Montgomery County to look at best practices for managing data security and privacy concerns.
  - Mobile Driver's Licenses (MDLs)
    - Had a webinar on MDLs.
    - Lots of community interest.

        - Being re-scoped to focus on use cases, starting with the use of MDLs to meet customer identification requirements for establishing financial accounts.
            - Other use cases include use by government identity providers and healthcare providers.
        - The identity team published errata update to 800-63 to discuss syncable tokens, also called passkeys, to clear up confusion on the xAL levels of a single token or passkey and to allow agencies to continue work on federating their identity programs.
            - These newer tokens provide strong assurances and phishing resistance for federal enterprises and their customers.
    - Guidance on Response and Recovery from industrial control systems cyber incidents
        - Collaborating with several vendors
    - Advancing Water Cybersecurity
        - Working with several companies and the Association of State Drinking Water administrators and local water utilities in Denver and Maryland.
- Privacy Engineering Program
    - Working with NICE on a Privacy Workforce Framework
        - Have held multiple public working groups.
        - Have a summary set of 1000 tasks, knowledge, and skill statements.
        - Will be called the NIST Privacy and Workforce Taxonomy
            - Follows similar structure as the NICE Framework
            - More on the privacy compliance side than the privacy engineering or privacy-by-design side
    - Looking at updating NIST Privacy Framework
        - 1.1 version
        - Align it to the new CSF.
        - Want to focus on creating NIST data governance profile.
        - Will be developing concept papers and sharing them in the coming weeks.
- **Ms. Flynn Goodwin** commented that she is happy to hear about the mapping between Privacy and the CSF. She asked if the team would be willing to also look at mapping Privacy and the AI Risk Management Framework at some point?
- **Mr. Petersen** replied that is definitely on the table. He and Kevin have monthly meetings to look at all the NIST frameworks. Initially they were done independently so we are now looking at how to integrate them to make it easier for the end user to make sense of them.
    - NIST SP 800-26 updates
        - Concluded a call for comments in January.
        - Expecting to adjudicate comments and have a final version this fall.
- Human-centered Cybersecurity
    - New group
    - Looking at the socio-human aspects of cybersecurity around issues of usability, contexts of privacy, expectations and requirements baselining, and different methods and mechanisms on how different groups of people are affected by different issues of security and privacy.
    - Some of the research they have done:
        - Effective psychological methods that employ phishing techniques and how they work,
        - Security for children using large surveys with children and caregivers on how some of these expectations differ and how that causes tension in security and privacy capabilities and deployment.
- CHIPS Act

- Continue to look at hardware security capabilities.
- Have been working with Intel, AMD, and SIA
- Had a workshop at NCCoE last month with chip manufacturers, industry associations, NIST, some other government agencies, and the White House came together to talk about future R&D needs for hardware security.
- Working with industry to create a hardware security profile using the CSF to protect the enterprise and environment as one mechanism; how do they protect and assure their intellectual property and design and development environment from a supply chain threat aspect.
- Still conducting research and looking at the best ways that NIST can engage in both increasing security of hardware, through design and deployment techniques and the use of hardware and security implementations as a trust route.
- **Ms. Flynn Goodwin** asked about a timeline on the hardware security profiles.
  - **Mr. Scholl** replied that they are hoping to have a draft profile out during this calendar year. They have some industry players volunteer their own profiles that they have created. These may not work for everyone. NIST will be working on a general profile that organizations can build on.
- **Mr. Venables** asked if they have partnered with the Trusted Computing Group (TCG), Open Compute Project, or the Confidential Computing Consortium (all of which are constructed as open-source foundations)? TCG just updated their TPM standards.
  - **Mr. Scholl** replied that they often meet with, and participate in, the TCG and some of their working groups, mostly in Opal interface and implementations around encryption in hardware techniques. They make sure they're not inadvertently disallowing things. They have also been working heavily with manufacturers and the Semiconductor Industry Association (SIA).
  - **Mr. Venables** commented that he thinks there's more to be done at the intersection of hardware and software. He asked if they are going to push memory safe programming? The world isn't going to rewrite all the software in Rust anytime soon so there's still a lot to be done on getting extra memory safety out of the large deployment of C and C++ that exists, which can get some hardware boost from memory tagging extensions and other things. Is that going to be or is this part of this? We know there are many techniques we could use to mitigate a lot of aspects of memory safety and C++. If there were some hardware improvements, that could reduce the performance impact and have as much effect as having tooling to move to Rust.
  - **Mr. Scholl** replied that it is not directly part of this work, but it is part of the Memory Safety Software Assurance, SSDF work, transitioning to memory safe languages and addressing legacy systems. NIST is also exploring if there is a need for a Hardware DF also.
  - **Mr. Venables** suggested that this might be a good topic for July. A session on the intersection between hardware and software. Most servers today are a large collection of processors; infrastructure processors, GPUs, CPUs, and then on every one of the processors are multiple systems on a chip. Today, a server is a loose collection of 50 OSs all interacting with each other. There has been a decrease in operating systems research as universities because everyone's focused on AI, etc. It would be good if NIST was working at that intersection of hardware and software.
  - **Mr. Scholl** replied that Barbara and Paul are very interested in the entire tool chain leading to secure code. He's not sure if their tool chain goes all the way down to the level that he's talking about.

- **Mr. Lipner** mentioned that the SSDF also includes code integrity or code provenance. The code integrity pieces overlap with operational security practices. The EO relies on the SSDF for secure development practices and the integrity in the environment. He thinks it's important to make those things clean and modular so that people know where to look for operational security without having to look in multiple places.
  - **Mr. Scholl** replied that they're doing that at the Center where they give a specific example of an implementation to show how it works in an operational environment and the specific references that work for it. They are building out multiple examples.
  - **Mr. Lipner** commented that application use cases are good. It would also be helpful to have some modularity in the framework documents.

NICE Updates

- Has been around for 15 years.
- Had some major updates to the NICE framework a couple of weeks ago.
  - Originally published in 2017 as a NIST Special Publication.
  - Revised over 3000 tasks, knowledge, and skill statements to modernize them, remove redundancies, and increase clarity.
- The NICE Framework is for employers, public and private sectors, as well as education and training providers so they can design curriculum and credentials to the framework.
  - Also learners, which could be employees, students, or job seekers.
- Also made some fine tuning of the names and descriptions to go with the categories and the 51 work roles in the framework.
- There are seven workforce categories.
  - One of them is Securely Provision
    - Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.
    - It's important as we talk about topics like technology, R&D, but also software development and architecture in the light.
- Added one new work role: Insider Threat Analysis
- All their work is based upon community input and demand.
- Other work includes operational technology and related work roles for cybersecurity.
- Finally, this version of the update finalized the addition of some competency areas, which not only address emerging topics about cross cutting issues that employees might need some information about, for example:
  - Cloud Security
  - AI Security.
  - Supply chain security.
    - Top priority because of Executive Orders and other reasons.
- Announcements came out a couple of weeks ago and he's happy to answer questions about it.
- NICE's role is to convene stakeholders.
  - They do that monthly through an interagency coordinating council meeting that he leads.
  - They also have a community council that's open to the public, co-chaired by academia, industry, and him, that consists of working groups and communities of interest.
  - This is to help implement the NICE Strategic Plan required by Congress.
    - Those working groups have project teams that implement objectives in the plan.

        - For example: our modernized talent management working group published an Employer's Guide to Writing Effective Job Descriptions.
            - There is often a disconnect between what employers are looking for, what they need, and the available supply.
        - The Transform Learning Working Group published a report using performance-based assessments, both in the academic training context and in the workforce hiring.
            - Looking at knowledge, credentials, and being able to assess what people can do.
    - They also convene people through events, webinars, and conferences.
        - They have their annual NICE conference coming up in June in Dallas.
        - Brings together over 700 people from industry, government, and academia to share effective practices and solutions, but also network with each other to find areas of collaboration and partnership.
            - Having a local stakeholders' event there next Monday.
            - Will be working with the Dallas Regional Chamber, their local Technology Association called Tech Titans, Florida International University who has a grant from NIST to run this event, and others for that event.
- They have a grant program called Regional Alliances Multi-Stakeholder Partnerships for Cybersecurity Education and Workforce Development.
    - Focused on local ecosystems, making sure K-12 schools, community colleges, universities, employers, nonprofits, economic development organizations, and localities are working together.
    - They'll be announcing 18 of those cooperative agreements in the next few weeks.
    - They'll also be announcing a second round of Notice of Funding Opportunity related to that grant program.
- **Mr. Gantman** asked if he has seen a change in the workforce.
    - **Mr. Petersen** replied that they fund a website called cyberseek.org that lays out the job demand based on current job announcements and postings.
        - This website is a good resource for helping to track those market trends as well as the available jobs.
        - The analysis is done by Livecast, in partnership with CompTIA. They update that quarterly and will be announcing an update on Monday.
        - To your question, there have been noticeable shifts in the market in terms of what employers are looking for, often related to the economy and world events.
        - They will make an announcement next week regarding significant shifts.
            - They're still coming up with the right explanation for the messaging.
            - AI is likely to be one where a lot of organizations are putting more personnel resources into but there are other areas of technology and competing, hiring and employment priorities.

Cryptography Agility and Transition R&D and Plans

Dr. Lily Chen, Senior Fellow, NIST

- **Mr. Lipner** expressed congratulations to Dr. Chen as a new NIST Senior Fellow. Dr. Chen thanked him.

Cryptographic Transition

- Cryptographic standards have been in a constant transition for:

  - Increased computing power by Moore's law and emerging quantum computers.
  - More sophisticated cryptanalysis techniques.
- NIST provided guidance for transitions in the past:
  - DES → Triple DES → AES
  - SHA1 → SHA2/3
  - 80-bits (RSA/DL 1024) → 112-bits (RSA/DL 2048 and ECC 224)
- Next revision of SP 800-131A will lay out a plan of transition to 128-bit classic security with the corresponding quantum security.

New Perspectives in Cryptographic Transition

- In the past, the transition decisions were made if:
  - An algorithm is broken, or
  - Security strength is lower than needed.
- The advancements of cryptography have introduced new perspectives for transition:
  - To consider new security features, requirements, definitions, etc.
  - Two examples:
    - Mode of operations
    - Key encapsulation mechanisms
- Referred to the chart on slide 3 of the presentation as a general example of NIST standards.
  - There is public key cryptography
    - FIPS 186
    - Key establishment – 800-56A/B/C
    - Based on discrete log-based or integer factorization-based.
  - Symmetric key cryptography
    - Block cypher – AES (FIPS 197)
    - Modes of operations (800-38A-38G)
    - HMAC (FIPS 198)
    - SHA 1/2 (FIPS 180) and SHA-3 (FIPS 202)
    - SHA3 derived functions (800-185)

Perspectives for Modes of Operations

- Catching up on all the reviews.
- Draft NIST IR 8459 summarizes a review of existing modes of operations (SP 800-38 series)
- SP 800-38A specifies encryption only modes – the oldest modes and implemented in most of the applications (e.g., CBC)
  - It has been a trend to use authenticated encryption modes (AEAD) (e.g., TLS 1.3)
- SP 800-38D (GCM) is an authenticated encryption and adopted in IETF and IEEE 802.1AE
  - GCM has limitations, e.g., very restrictive rules for the nonce and low max plaintext length.
- Desired properties for new modes
  - Misusing resistance
  - Multi-key security
  - Key commitment
- NIST plans to develop a new mode of the AES that is a tweakable, variable-input-length-strong pseudorandom permutation (VIL-SPRP) with a reduction proof to the security of the underlying block cipher.
  - Workshop: June 20-21. 2024 in NCCoE to discuss requirements, properties, parameters, and features.

- The transition to new modes is not because the old modes are broken but new modes are more robust – we need new strategies for new transitions.

New Perspectives for Key Encapsulation Mechanism

- The schemes specified in SP 800-56A (DH, MQV) and SP 800-56B(RSA) were based on X9.42, X9.63, and X9.44 developed in 1990s.
  - They are not key encapsulation mechanisms but "key exchange" or "key transport". They cannot be proved to be IND-CCA2 secure (or at the time CCA2 concept was not proposed.)
- NIST PQC call for IND-CCA2 secure KEM.
  - ML-KEM (Kyber), specified in draft FIPS 203, can be proved IND-CCA2 secure.
- The transition is beyond quantum vulnerable to quantum resistance.
  - The transition is to schemes with a more advanced security concept.
  - SP 800-227 is under development to provide guidance on using KEM in key establishment protocols.
- Informally, IND-CCA2 security requires the ciphertext is random to an attacker no matter how an attacker inquires a decryption oracle with adaptively chosen ciphertext to obtain the plaintext. That is after the attacker gets many pairs of ciphertext, plaintext, for two messages M_1 and M_2 generated by the attacker, a returned ciphertext C is an encryption of one of M_1 and M_2, selected randomly. The probability of correct guess which of M_1 and M_2 is not significantly larger than ½.

PQC Transition and Hybrid Mode

- The transition can happen in different stages.
  - The decision on when to deprecate quantum vulnerable algorithms will be based on a good understanding about the adoption of PQC, the advancement of quantum computers, and interoperability consideration.
- In each stage, hybrid mode and dual signatures will be validated differently.
  - Currently, NIST approves implementation with 56A and 56B with hybrid key derivation in 56C – allow input of another shared secret from a PQC algorithm or a QKD.
  - Slide 6 in the presentation shows diagrams of the different implementations.

Transition Challenges and Crypto-Agility

- Each transition, whether the transition is to adopt a different key/parameter size or to adopt a different algorithm, will impact hardware, software, API, protocols, and more.
- It must consider interoperability and backward compatibility – also prevent downgrade attacks.
- Crypto-agility has been considered as a key for smooth transitions.
- Crypto-agility is:
  - the ability for machines to select their security algorithms in real time and based on their combined security functions.
  - the ability to add new cryptographic features or algorithms to existing hardware or software, resulting in new, stronger security features; and
  - the ability to gracefully retire cryptographic systems that have become either vulnerable or obsolete.
- **Mr. Venables** asked if NIST has an official definition of crypto agility?
  - **Dr. Chen** replied that these are accurate definitions but not official NIST definitions. As they look into different layers of different systems, they will better see what "agility" could mean.

Crypto-agility: Notations, Requirements, Motivations

- Looking at what they hope to achieve:
  - the **feasibility** of replacing and adapting cryptographic schemes in software, hardware, and infrastructures, and should enable such procedures without interrupting the flow of a running system.
  - the **ability** to adopt and integrate new cryptographic algorithms with no significant changes to the infrastructure, and without disruptions to running systems.
  - the **capability** to apply repeated cryptographic changes (migrations) over time within a stable (non-changing) IT-architecture.
  - the **stability** towards other systems, even after adapting its cryptographic measures.
  - the **flexibility** to implement, update, and replace cryptographic components within IT-systems, without affecting its functionality.

Existing Approaches and Solutions

- Protocol agility.
- Design agility.
- Hardware agility
- API agility

Crypto-agility: Protocol and Algorithm

- Support of multiple cryptographic algorithms can be interpreted as an implementation of crypto-agility.
  - TLS, IKE, etc. allow negotiation among multiple options.
  - Hybrid mode to use multiple algorithms for key establishment.
  - PKI: composite and non-composite certificate
- RFC 7696 "Guidelines for Cryptographic Algorithm Agility and Selecting Mandatory-to-Implement Algorithms" (2015) – provides guidelines to ensure that protocols can migrate from one mandatory-to-implement algorithm suite to another over time.
- Cellular network (5G, 3GPP 133.501) supports negotiations of the algorithms for access authentication and protections of connections.
- **Mr. Venables** asked for her view on where they draw the line on protocols. The slide showed layer 3&4 protocols but something they've talked about is when they get to layer 7 protocols that have embedded assumptions about signature and key sizes and x.509 certificates that go across every industry. Should that definition of protocol agility also go up to the application layer?
  - **Dr. Chen** replied "definitely".

Crypto-agility: Design

- Expand existing infrastructure to be able to exchange cryptographic algorithms, e.g.
  - allow multiple algorithm options in design, e.g., some V2V secure communication protocol takes adaptation of key length and cryptographic algorithms during PKI operation into account.
    - "Public Key Infrastructure and Crypto Agility Concept for Intelligent Transportation Systems" https://personales.upv.es/thinkmind/dl/conferences/vehicular/vehicular_2015/vehicular_2015_1_30_30028.pdf
  - consider algorithm agility on TPM 2.0 ECC Functionalities.

  - "Algorithm Agility – Discussion on TPM 2.0 ECC Functionalities" https://link.springer.com/chapter/10.1007/978-3-319-49100-4_6
- Algorithm independent design, e.g., in blockchain.
  - "PQFabric: A Permissioned Blockchain Secure from Both Classical and Quantum Attacks" https://arxiv.org/abs/2010.06571
- **Mr. Gantman** mentioned that, in building the design layer, a lot of the assumptions are implicit. People don't even know they're making those assumptions until they break them. That's where a lot of the deployment challenges are in crypto-agility. On paper, these protocols are flexible but that doesn't always pan out in reality.
  - **Mr. Venables** added an example that is already starting to be documented is when we're doing PQC key exchanges inside TLS sessions inside browsers, the authentication exchanges are going across multiple TCP frames, which is starting to break these TLS proxy devices that made an incorrect design assumption about how authentication exchanges work; they're not violating the standard; they just made an implicit design with the assumption of how current crypto works. There's going to be so many unintended breaks that are worth thinking about.
  - **Mr. Gantman** added that brings up another dimension because changes are coming more frequently but also the changes impact a vastly larger number of systems from a broader set of suppliers and developers. We went from DES to AES, which seemed big at the time, but we probably still have more systems using SHA1 than ever used DES.
  - **Mr. Scholl** commented that it's a "harder hard problem."

Crypto-agility: Hardware

- FPGA based cryptographic accelerator, designed with algorithm-agility in mind.
  - "Algorithm-agile cryptographic coprocessor based on FPGAs"
- Repurpose hardware designed for RSA together with lattice-based algorithms (integer multiplier).
  - "Post-Quantum Cryptography with Contemporary Co-Processors" https://eprint.iacr.org/2020/1303.pdf
- Unified instruction-set architecture leverages the synergies between similar PQC schemes.
  - "A Unified Cryptoprocessor for Lattice-Based Signature and Key-Exchange" https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9920009

Crypto-agility: API

- plug-in structure in the Cryptography API: Next Generation from Microsoft to exchange cryptographic algorithms without any change to the code of the program.
  - "Security Issues on the CNG Cryptography Library (Cryptography API: Next Generation)" https://ieeexplore.ieee.org/document/6603762
- extended library that provides many PQC algorithms and makes it easy to select and interchange them in different security strength levels, e.g., LibOQS.
  - https://openquantumsafe.org/

Crypto-agility: Challenges, tradeoffs, and limitations

- Security and complexity trade-offs - having many cryptographic options opens an unknown space for attack surfaces, such as downgrade attacks.
- Resource limitations for crypto-agility:
  - Hardware size may limit how many and which algorithms can be implemented – new algorithms require additional hardware resources to be efficiently integrated into the established protocols.

  - Bandwidth may limit deploying new algorithms with large pk or sig or cipher or hybrid mode in some protocols.
- Some cryptographic schemes are primitive dependent, e.g.
  - Password-based key derivation Argon+ relies on the compress function of a hash function Blake, one of the finalists in SHA3 competition.
    - NIST SP 800-131 specifies PBKDF2 computing-hard for brute-force attack. New trend is use memory-hard password KDFs e.g., Argon+.
  - Identity-based encryption (IBE), attribute-based encryption (ABE), threshold cryptography/multi-party computation, rely on algebraic properties of the underlying cryptographic primitives.

How to evaluate Crypto-Agility?

- A proposal on a maturity model for crypto-agility assessment
  - "Towards a maturity model for crypto-agility assessment" https://arxiv.org/abs/2202.07645
  - a maturity model for determining the state of crypto-agility.
  - it consists of five levels, for each level a set of requirements have been formulated based on literature review.
- The model provides certain guidance and can be considered as a framework.
  - Is it possible to use a general framework for different "systems"?
- Level 0 - Initial/Not Possible: hardware or software limitations that do not allow subsequent changes to the original design.
- Level 1 – Possible: can be adapted so that their cryptography can respond dynamically to future cryptographic challenges.
- Level 2 – Prepared: already implement certain measures for crypto-agility but are not yet fully ready to actively realize it.
- Level 3 – Practiced: migration between different cryptographic methods is demonstrably, effectively, and securely feasible.
- Level 4 – Sophisticated: compatibility is not limited to a specific system but can be scaled across a broader infrastructure; allows for a fast and automated migration between different cryptography schemes.
- **Mr. Gantman** commented, regarding the agility maturity model and coming from the end device space, agility can be interpreted in different contexts: how easy is it to update existing devices versus how easy is it to update the design and implementation for new devices? These both come into the crypto-agility discussion.
  - **Mr. Scholl** added that Dr. Chen came to him and said that this is what we think a piece of guidance would look like and how to slice it from all these different angles coming from NIST.

Crypto-Agility: Research areas

- Security analysis on protocols and countermeasures for downgrade attack.
- Security and complexity study for systems (platforms and protocols).
- Agility for resource limited communication environments.
- Limitations and potentials for re-purposing cryptographic co-processors.

Crypto-agility: What NIST can do to move forward?

- Constantly review and update published standards and include crypto-agility as a consideration.
- Timely provide guidelines for each stage of transition and enable algorithm validation.

- Work with industry communities and standards organizations to understand challenges and explore specific agility strategies and techniques for different systems.
- Accommodate best practice – NCCoE partnership, workshops, and reports to enable crypto-agility – maturity assessment.
- Encourage research of hardware optimizations for crypto-agility.
- Promote protocol level crypto-agility through contributions to IETF initiatives.
- **Mr. Venables** added that, in addition to IETF, you have a list of other standards groups that you should engage with such as IEEE, ANSI, 5G, 6G, etc.
    - **Dr. Chen** replied that they have people who participate in different working groups. Some of those standard organizations are more operator oriented and the active parties are operators.
- **Mr. Lipner** mentioned the NCCoE project on transition and, he assumes, agility is in progress currently. Some possibilities are: 1) the transition doesn't work, and you don't get interoperability where you need it, 2) the transition appears to work but we introduced some of the fallback errors that we've seen in the past, or 3) we think the transition has worked but there's some buried uses of obsolete encryption that organization never discover until somebody attacks it. Those are three things that an agility solution needs to address. He hopes the NCCoE project will get results and best practices or rules for developers to apply in all three cases.
    - **Dr. Chen** replied that they have quite a few companies they are working with and most of them are looking into what the cryptography algorithms look in the real-life protocol applications. That will give them some experience for agility, but she doesn't think they already include agility in the current project. They're focused more on the PQC transition.

AI Risks, Threats, and Opportunities (Remote Presentation)

Dr. Zico Kolter, CMU

Introduction

- He regrets that he couldn't attend the meeting in person, but he is often in DC and would be willing to meet with the board members at another time.
- He will be talking about AI security, not maintaining AI systems or the provenance of the data but in deploying AI systems and the vulnerabilities that you open yourself up to that we currently don't know how to solve.
- As LLMs get more prevalent, we have the potential to create a massive security hole through the use of these systems.
- He will document why this is the case and present a broader picture what some of these real concerns are.

Manipulating ChatGPT

- He asked ChatGPT to insult him. It responds with, "as a language model, I'm not allowed to do this, I have to treat users with kindness and respect", etc.
    - This response is constant as long as conventional requests are made.
    - By adding quotes and a dash and other characters, ChatGPT replies with insults.
- This ability to manipulate LLM to do whatever we ask opens a genuine and pressing security challenge that will become the main differentiator of if LLMs can be used in a safe and secure manner.
- He will do a brief into on how LLMs are trained to obey the safeguards to not do things like insult people or tell people how to build a bomb and so forth.
- He will describe how they circumvented the safeguards using a simple approach and the results and implications of this approach and the study they did.

Background

- Example: Ask ChatGPT for a brief history of Carnegie Mellon University. ChatGPT works well for this kind of thing.
- But we also use it for coding, summarizing documents, and other things.
- How does it work?
  - The ChatGPT model works by picking what word is the most likely word to come next after this sentence.
    - The model is trained on a lot of the internet.
    - For the example, given the first word "Carnegie" the next likely word would be "Mellon" and so forth until there is a description of Carnegie Mellon.
- How this process works is one of the most significant scientific discoveries of the last 10 years; having models that generate text in this fashion to create coherent responses.
- There are problems with the training process:
  - If we take the whole internet's worth of data and convert it to an AI that predicts next words and create a chatbot by repeatedly predicting next words according to this model. The problem here is that there is lots of bad stuff on the internet. If you do this process and have a chatbot and then ask it to build a bomb, it will happily tell you how to go and build a bomb.
  - No judgement on if it should or shouldn't give out this information. It knows this information because the information is on the internet. A person would be able to look up how to build a bomb without the chatbot.
  - The builders of the chatbot feel that they shouldn't make it easy to get this information from the chatbot so, instead, they say, "the right answer to this question is to not tell me".
    - Inserting these types of responses is called an "alignment process" for these models and is used to fine tune the training.
    - Only requires a relatively small number of samples (~ 100,000) compared to the amount of data it is trained on in order for the model to learn it's not supposed to say certain things or give out certain data.

The Attack

- They took a phrase that the model will normally refuse, like, "tell me how to build a bomb," and appended a bunch of extra words or characters to it, such as exclamation points. Looked at the internal workings of an open-source language model and computed the exact probabilities of different responses.
- Next, they worked to raise the probability of it giving the "bad" response. To do this, they started swapping "tokens" or words in and out of the request, specifically with the goal of increasing that probability.
- It ended up being very simple. In one instance, they tried about 200 possible substitutions. They used techniques based on the differentiability of the models.
- The core point is that they tried a bunch of guesses, picked the best one, and repeated the process of swapping out words to see the effect on the probability.
- Eventually, if they picked enough of the strange words that increased the probability, they would get the "bad" response they were looking for.
- An interesting thing is that, in their design of this "buffer overflow" equivalent, is that their target response is to get the model to say, "yes, I'll give you that information." At that point, the model will then generate the rest of the information. The model had become convinced that it wants to tell you the information you asked for and it, therefore, does.

- Even though they did the original work in open-source models, they found that, if you take these phrases and plug them into closed source models like ChatGPT, it often, and very consistently, works.

Study Results

- They developed a test bench of about 500 harmful strings and harmful behaviors.
  - These are things that, normally, the models would not want to repeat or behaviors they would not want to perform.
- They found that, on a variety of open-source models, they were able to break most of those behaviors through either single or multiple target attacks.
- They found that this worked on the older models and more recent models.
- **Mr. Groman** commented that he's trying to understand when a malicious actor would engage in this behavior to circumvent these controls? Also, once these models have been broken, can anyone get access to the "bad" information or is it only the one who broke the model or just that instance of the model?
  - **Dr. Kolter** replied that it is only if you initiate this behavior into that instance of the language model. If someone is talking with ChatGPT, we are not retraining that particular model. However, there are certain bad things that you can already do with what we have done. You can quickly generate misinformation for harassment of people. Those models will not do that natively, but you can make them do it with this. However, the real threat is not chatbots. The real problem is that people use LLMs to process data from third parties. Things like using an LLM to read emails and summarize PDFs. If you can manipulate LLMs in this fashion, you can inject breaks/buffer exploits into a PDF or into your email so that whatever system you're on, the attacker has gained control over. Chatbots are limited because they are sandbox environments. They can call the web, but they don't really do actions. The danger is when the LLMs are taking actions on behalf of their users when processing third party data and injecting malicious content into that data, they can manipulate the systems into acting in an arbitrary manner.
  - **Mr. Groman** asked if the risk is similar to clicking on a phishing email containing malicious software that gets downloaded, infecting the system?
  - **Dr. Kolter** replied that it's more than that. That requires an action from the user. If you have an LLM set up to parse your emails and look for all of the invoices that were sent by a known vendor and then automatically pay those invoices, it could be possible to for a bad actor to send an email that would trigger the same payment system, even if it's not a legitimate invoice. The threat comes from the fact that these tools are starting to be deployed in a more automated way. They shouldn't be right now. Another example is setting up an LLM to summarize email. A bad actor could send an email that would cause the emails to be summarized incorrectly. Depending on how much control authority these systems have, he could write you an email that would cause you to send out another email in response to someone else, possibly insulting them or something else damaging. This is a massive security flaw that is being opened up. People think of these LLMs as intelligent agents that operated like humans so we're turning them over to act on our behalf in many scenarios. They are not. They are incredibly powerful computational engines that have security flaws. We don't know how to fix those flaws, which is the real issue.

Common Questions

- Why do these random characters work? What is happening in this string that, to us, just looks like a bunch of garbage?
  - This is analogous to other things in a lot of deep machine learning models that we've known for some time; you can take computer vision models and add very small amounts of specifically

chosen noise to this image and cause the model to classify the images entirely differently. (He showed a picture of a pig that an AI model classifies as an airplane due to noise.)

- It's not surprising that they can create these exploits. What is somewhat surprising is that the exploits transfer from open-source models to closed source models.
  - There are several hypotheses about why this might happen. The most likely scenario is that, to a certain extent, these strings are meaningful according to the training data itself.
  - These models are entirely based upon their training data, in some ways they are a synthesis of their training data.
    - The reason those weird strings work across models is that models are often trained on very similar datasets and these weird phrases, therefore, somehow emerge from this training data, likely in a way that makes them useful to the models in some in some odd way.

What can be done?

- The genuine answer right now is that we don't know.
- We've been working on a similar problem in computer vision for the last 10 years and we have not yet solved it.
- Can't create a model that isn't vulnerable to this mode of attack.
- This indicates a different set of decisions that we should be making about the release of these models. As we replace programs with queries to LLMs, what we are doing is developing agents that have security flaws that we know about but don't know how to fix, which is very concerning.
- They released the paper and the code to increase awareness of these flaws and so companies who are starting to do this understand the risks involved and how to mitigate them before they rush in.

Discussion

- **Mr. Groman** observed that he has been to around five AI conferences recently and none of this comes up. The general view of industry reps or startups is that the concerns [over AI] are overblown and we have to move forward and not stifle innovation. We have a risk management framework that comes from NIST on cybersecurity and privacy. Now we're getting to AI and it's a tool that presents a way to think about risks. But at the end of the day, they say that they are in full compliance with the NIST Risk Management Framework because they looked at it and decided to accept all risks. There are externalities but it doesn't impact them, it impacts somebody else.
  - He thinks that, at some point, we have to move to the next phase. The utility of the framework, what we need to have happen in certain contexts, is not being achieved by not helping people get to that final answer of balancing risk, acceptable levels of risk and risk tolerance. The risk is real and true.
  - What do we do with a risk framework that lists things, but the problem at the end is that someone needs to care and think?
  - **Dr. Kolter** replied that he doesn't have a solution, but he wants to differentiate between risks that are often associated with AI, which he thinks are overblown. The existential risks of machines, becoming self-conscious, taking over the world, taking over factories, replacing biological weapons kind of autonomously, etc. We need to delineate between the risks that are very speculative and those that are currently technically feasible. Everything he has described here is technically feasible. The way to move forward in the discussion of AI risks is to be very concrete. It can't be a broad swath of all risks, especially with AI because that is too broad and too big. It has to be saying, "when you have systems that have the ability to take actions XYZ," you need to understand those actions and the possible risks. We should have a good framework for this cybersecurity control. This is the control authority of applications. Do they have proper

safeguards in place to ensure that malicious inputs will not cause them to overstep their desired behavior desired functionality? If we scope regulations and requirements like that, where maybe chatbots are exempt from them, because we don't care if chatbots say mean things, then we have much more ability to have a very solid ground to stand on in terms of what we should be mandating.

- **Mr. Venables** asked if any of the research has looked at the effects of different settings on the models such as "temperature parameters"?
  - **Dr. Kolter** replied that they have, and it only has minor effect.
- **Mr. Venables** asked if they have taken that class of malicious inputs and fine-tuned on it to tell the LLM to disobey that? Does it learn the generic property, or does it only learn the specific property?
  - **Dr. Kolter** replied that is one of the main things that they are doing right now. Basically, incorporating this data into training to try to find the models that are more secure. The problem is, as you expand your space of attacks, longer sequences, more sets of questions, slightly subtle different variations in the response, you can really break them again. He thinks we will need more than just this sort of "adversarial training,"
- **Mr. Venables** commented that the image adversarial problem is uniquely difficult because humans can't see it. The malicious prompt additions are easier to see, even to a human. He's guessing that the way people would protect the model is to eliminate clear gibberish or have another machine to recognize and remove it.
  - **Dr. Kolter** replied that there are differences in the visual and text settings. He's not as confident as Mr. Venables that you can use other machines to do this as he could just break that machine too. Unless you put a human in the loop it's very hard.
  - **Mr. Venables** suggested putting a predictive AI model in the loop rather than a generative AI model.
  - **Dr. Kolter** replied that the predictive models can also be broken in similar ways, and you can bypass filters also.
  - **Mr. Gantman** asked if the fundamental conclusion is that anything that makes it into the training data can make it into the output?
  - **Dr. Kolter** replied that, while they haven't proven it yet, it is a good takeaway.
  - **Ms. Moussouris** asked if he's saying that there is no possibility to do input and filtration with the current with the current models?
  - **Dr. Kolter** replied that these are all mitigations and in certain circumstances they can help. Input filtering can definitely help. You can bypass the input filter, the model, and the output filter. There are people showing that's possible to do but it adds complexity. It's important to appreciate that there aren't fixes, these are mitigations that may help.
  - **Mr. Gantman** added that input filtering is hard because you don't have a well specified input language by which to restrict your input.
  - **Mr. Lipner** commented that it brings up memories of early attempts to mitigate cross-site scripting.
- **Mr. Groman** asked about his comment that we don't have to worry about chatbots. What about chatbots that are used in mental health? There are discussions about replacing human psychologists/psychiatrists. There is no data that says they are ready for this yet. He's been looking at them and chatting with them. Wouldn't it be possible for them to ask about suicide or "why does your life suck?" Things that could create a danger?

- **Dr. Kolter** replied that this is a great point. We do have to worry about these things in the context of the fact that they are wrong and give incorrect responses or harmful responses, even in their non-attack behavior.
  - He said chatbots are okay in the context of specifically malicious actors attempting to circumvent the desired operation of a system. He is not suggesting that there's only concerns when it comes to using generative AI broadly. Even when users are benign, there are still massive concerns to be had. What he's trying to address here is the problem of malicious actors of these chatbots also being a source of concern, in addition to the massive concerns that exist about how humans use these things.

- **Dr. Kolter** added that he needs to go but would love to follow up if there's more opportunity and to please get in touch.
- **Mr. Scholl** commented that he would share the paper and the slides.
- **Mr. Venables** commented that it's important that there are sector specific regulations and why the NIST AI risk frameworks, AI principles and at a national level, AI Bill of Rights are all necessary. Industry specific regulations in finance and healthcare, that build on existing testing frameworks to make sure that these things have the right risk safeguards in place. There are many segments of the market perhaps not as regulated as they should be where these things have been easy to deploy without controls,
  - **Mr. Gantman** indicated that it may require holding the deploying entity accountable for the output in the same way they would be accountable if it was a human that said those things.
  - **Ms. Flynn Goodwin** added that regulators may be afraid to go into the security space on AI, the SEC did their whole NPRM process on AI; we're expecting them to release their proposed rules sometime late spring, early summer, and it doesn't talk about cybersecurity. It's only focusing on conflicts of interest and abuse of AI.
  - **Mr. Venables** commented that ultimately, it's about the context of the deployment. There's plenty of examples inside companies deploying these models in highly constrained circumstances where the risks are more inherently mitigated, and they're realizing the upsides, which is very different from the use cases of deploying a chatbot to interact with people 100%. Looking at specific generative models used in particular cases in pharmaceutical development in a whole range of other things that have similar risks, but the nature of their deployment doesn't manifest the risks. This is why he thinks this is a useful thing for NIST to consider for the AI Risk Management Framework regarding context and the risk mitigations, not just the inherent properties of the model. Something that is worrisome is a lot of organizations out there think it should be solved in the model. Going back to traditional forms of machine learning, we've had this problem in the past. People solved it by putting guards around the model and managing the operational risk of the deployment. It's harder for this generative AI rather predictive AI, but it's the same principle.
- **Mr. Lipner** mentioned that the thing that is probably necessary is to be explicit about the risks. Somehow the process has to encourage folks to look specifically at examples of what could happen, and then to determine that they've mitigated those things a little bit.
  - **Ms. Flynn Goodwin** added that they don't know what the risks are, from the user perspective, so it's hard to know what you've accepted.
  - **Mr. Lipner** added that if you drill down into the application domain, then you can probably get some level of understanding of what the risks are from the user's point of view.
  - **Mr. Venables** added that the problem is not the models. It's the naïve implementation of these models. For example, some e-commerce websites are deploying generative AI to synthesize 1000s of reviews of products. You can imagine that "skunk" marketers selling dubious products

and online marketplaces generating fake reviews with all that gibberish attached to it so that their product is synthesized in the way that benefits them. We're probably days away from seeing examples of this.
    - **Mr. Gantman** asked if, even with limited deployments, it is possible to make an informed decision about risks when you don't know what's in the training data?
    - **Mr. Venables** added that it's how you think about the context of deploying it. Even in regular cybersecurity circumstances, we have all sorts of input and output filters and controls, but you still can't rely on them 100%. There are degrees of risk mitigation. He thinks this is similar. No amount of tuning is going to solve the problem of the data in the model.
    - **Mr. Gantman** commented that there's still some implicit trust there. For example, would you feel comfortable using a code generator that was provided by Alibaba?
    - **Mr. Venables** agreed. You have to understand the provenance and lineage of what went in the model. For example, we've been proposing something like a datasheet for models where you can have much more clarity over the lineage and provenance of what went into it for training.
- **Mr. Moussouris** commented that another area we didn't get to touch on with Dr. Kolter is the concept of stringing it together to execute on behalf of the user. To her, it seems that it's not just input and output guardrails, but the idea of some sort of a non-executable stack concept going into some of this is something to explore. We didn't talk about ways to categorize and classify the risk. Is there a way to determine relative risk and, therefore, amounts of mitigations/precautions are needed.
    - **Mr. Groman** mentioned that someone has to understand all the factors that go into it to be able to make an informed decision and none of that solves the problem of a lack of concern on the part of the implementers.
    - **Ms. Moussouris** added that if we can figure out a way to categorize the relative risk of different use cases of these models; speed of input to output, types of actions were executed, etc.
    - **Mr. Groman** replied that this is an issue that needs to be on the table for NIST in the RMF and elsewhere like maybe the AI RMF. The executive order says NIST needs to start contemplating the national security implications given what we know about the threat actors, what they're doing with this, and what they have done. It's not just traditional security and privacy questions. It's important to also consider how this will impact national security if an adversary gets hold of it or if it doesn't work? Companies don't know how to do that, and we haven't explained to the private sector what it is or how do to that before you launch your product. How are you going to assess if there's a national security implication that might have to trump some amount of profit?
    - **Mr. Scholl** commented that is not in NISTs scope. National security issues would be more in DHSs scope.

The Chair recessed the meeting for a 45-minute lunch break.

Update on ZTA Implementations in US Federal Agencies

Nicholas Polk, Office of the Federal Chief Information Officer, OMB, EOP

Introduction

- Branch Director within the Office of Management and Budget.
- Responsible for:
    - Coordinating federal IT and cybersecurity policy across civilian agencies for non-national security systems
    - IT budget formulation for all agencies
    - Cyber incident response on behalf of the OMB Director

- I am led by Chris DeRusha who is both the Federal Chief Information Security Officer and the National Cyber and the Deputy National Cyber Director for federal cyber.
- We drive cybersecurity across civilian agencies through execution of EO 14028, the National Cybersecurity Strategy and its constituent strategies such as M-22-09, the Federal Zero Trust Strategy.

Executive Order 14028 – National Cybersecurity Strategy

- Implemented during the SolarWinds incident.
- We experienced many unique vulnerabilities that have caused widespread impacts across the federal and private sector.
- The establishment of the EO has driven our modernization agenda and repeated throughout the National Cybersecurity Strategy.
- Under this EO we implemented the OMB Federal Zero Trust Strategy, M-22-09

M-22-09 – Federal Zero Trust Strategy

- Uses philosophy that we shouldn't trust anything on the network because any part of the network that's the weakest is what our advanced adversaries will find and exploit.
- By saying that no actor, system network, or service operating outside or inside the security perimeter is implicitly trusted, we are going to verify everything on our network and ensure that an attack doesn't occur.
- Establishes a baseline across federal agencies where we can then grow into our next evolutions of zero trust.
    - For example, CISA released Zero Trust Maturity Model 2.0, a roadmap which agencies can follow to see where they fall along their zero-trust strategy journey.

Vulnerability Disclosure Program

- Evidence based method to improve security.
- In five months of standing up the VDP program, it received 330 Vulnerability reports.
    - 180 of which were critical findings.
- We are working with CISA to modify some VDP programs that were successful in the private sector to use in the government.

Implementing Zero Trust

- Implemented the Endpoint 209
    - Requested all agencies submit a zero-trust implementation plan.
    - OMB and CISA review those plans with each agency.
    - Assists agencies in determining where they are, where they want to get, how they're going to get there, and how they're going to prioritize resources.
- Two topics of interest with regard to implementation:
    - Workforce
        - The National Cyber director issued their cyber workforce strategy:
            - Enhances the federal workforce.
            - Brings more people into the workforce that might not have considered a career in cybersecurity.
            - Addresses retaining and training the current workforce.
        - Addressing the burden of compliance on agencies

        - Discover where we can automate.
    - Budget Funding
        - M-23-18
            - Each year we issue our priorities memo.
            - Cyber priorities are aligned with the pillars of the National Cybersecurity Strategy.
            - Led to an increase in the spending on cybersecurity as represented in the President's budget.
    - Technology Modernization Fund
        - Addresses urgent IT modernization challenges.

Encryption & Post Quantum Cryptography

- Agencies continue to work on inventorying their cryptography that's vulnerable to a quantum computer.
- Once they have that inventory, they are able to start the migration to post-quantum cryptography once NIST release their standards.
- Encryption underpins almost every cyber defense we have from authentication to data in transit encryption, all of which will need to be modernized to post-quantum cryptography over the coming years.
- We continue to work with agencies to ensure that those transitions are adequately implemented.
- **Mr. Lipner** – For the post quantum transition, is there any sense of the range of proportions of COTS products to internal efforts to reconfigure and redevelop applications that use cryptography?
    - **Mr. Polk** – There is a lot of variation between COTS products where the cryptography is well documented. Where we're seeing the most work that needs to be done by agencies are the government off-the-shelf products or things that are made specifically for government. This is for two reasons:
        - In many cases this is a government to vendor relationship and the agencies need to work directly with the vendor to determine the migration strategy.
        - Legacy Information Technology. Agencies don't quite know yet which systems are legacy and will need to be replaced to migrate to PQC.
- NSM 10 (National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems) directs agencies to start migration no more than a year after NIST releases their standards.
    - Will bring visibility to what the agencies will be spending on this migration.

Measuring Success

- FISMA Metrics Working Group
    - Agencies themselves nominate representatives to help us continue to modernize metrics.
- CISA Continuous Diagnostics and Mitigation Program
    - Working to determine where metrics can be automated.

Next Steps

- Secure Software Attestation Effort
    - Led to release the secure attestation form, which agencies can adopt and use to collect secure software attestations from software vendors.
    - CISA stood up a central repository to simplify the submission of those agencies.
    - Drives the ethos behind the National Cybersecurity Strategy to shift burden from individual agency purchasers back to the software vendors for following secure development practices.

- Collaborating with CISA on their development of the focal plan.
  - Aligns operational activities across different agencies and ensures that we are aligned with CISA and CISA is aligned with us on how we support agencies and their implementation of operational and strategic policy.
- Shared Services
  - Looking into where we can deploy those more strategically.
  - Working with agencies to deploy those to drive efficiencies where possible.
  - Ensuring agencies have access to best-in-class tools and services for their cybersecurity.
- Enterprise Licensing
  - Where we can use common terms and conditions across different agencies to ensure that they are receiving the best product when it comes to software and hardware they procure.
- System Modernization
  - Working with each agency to determine where they should focus their modernization based on the criticality of the system and ability to implement modern cybersecurity defenses.

Questions

- **Ms. Moussouris** – What are you doing for integrating the findings of the vulnerability disclosure programs, because discoverability of public facing abilities is a pretty good indication that you should modernize?
  - **Mr. Polk** – That's a good question that I will have to take back. One of the biggest challenges we have, which is partially addressed by the CISA asset visibility bot, is when you identify an IP address that is doing something it shouldn't do and then you must trace it back to the source in an agency. However, in instances where we can do that, it makes sense to tie those vulnerability findings to the modernization plan.
- **Mr. Gantman** – Upon looking at NISTs cybersecurity budget trend over the years, do you see it as a growing priority or diminishing priority?
  - **Mr. Polk** – I can't speak to the budget for this year, it's still in negotiation. We and the National Cyber Director work with the budget side and Congress to ensure that we can adequately prioritize cyber and it's an ongoing prioritization exercise.
- **Mr. Lipner** – Back to zero trust. Are there lessons learned as agencies have tried to reconfigure their networks or systems, or change the way privilege works? Or is it too early to have any sort of observations about that?
  - **Mr. Polk** – We have discovered some very interesting topics or challenges:
    - When it comes to reconfiguring networks for MFA, we've learned it's sometimes difficult to tack it on especially with legacy applications. Some agencies have already found interesting solutions to that issue.
    - Also, seeing a lot related to OT and IoT and determining how to secure it.
      - IoT is very amenable to MFA, however, OT presents unique challenges.
    - MFA presents a challenge in terms of user experience, digital experience, which we are working through.
      - PIV cards aren't the best solution; looking at cases where we can use other technologies that provide similar or higher assurance.
      - Working closely with office handling accessibility to ensure solutions are 508 compliant.

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

Final Board Reviews, Recommendations and Discussions

Steve Lipner, ISPAB Chair

Topics for Future Meetings

- Discussion on the intersection of hardware and software (Brought up by Mr. Venables during the NIST Cybersecurity and Privacy Updates).
- Trusted Computing Group (TCG), Open Compute Project, or the Confidential Computing Consortium (Mr. Venables and Mr. Scholl)
- Defining Crypto-Agility (Mr. Venables)
- NVD Resourcing (Mr. Groman)
- NIST FIPS 140-2 updates (Mr. Venables)
- Follow up on the Attestation Form
- PCAST
- NMRC
- NITRD
- PPD-21
- AI and facial identity
- IoT labels
- OMB PIA RFI
- Differential privacy
- Crypto pads
- NAIR
- Kids Online Health and Safety Task Force
- Draft FISMA Update
- CMVP at PQC
- Frameworks Follow up and the Intersection between NISTs Frameworks
    - CSF
    - CPG
    - CMMI
    - FedRamp
    - AI RMF
    - Privacy Framework
    - SSDF

Potential Board Actions and Discussions

- Due to the issue with the OGE 450s and lack of quorum, no decisions will be made at this meeting.
- Mr. Lipner asked Mr. Scholl to set up a virtual special meeting to discuss and vote on things that they couldn't during this meeting.
- **Mr. Lipner** – Mr. Groman expressed concern regarding the NVD resourcing issue. Would like him to informally think about what we might want to say so we are ahead of the topic and quickly get a notice out on the subject.
- **Mr. Gantman** – Would like to have GAO present to give their take on measuring outcomes in response to the National Cybersecurity Strategy. We tend to hear about what's being done, but not necessarily about the state of attacks on federal systems. Is there anybody that produces anything like the Verizon DBIR, but for federal systems? Is anyone tasked with that? Should somebody be tasked with that?
    - **Ms. Moussouris** – I think the data is there but can only be seen at a certain clearance level.

- **Mr. Gantman** – That brings up the question, how are we meant to advise if we don't see the data?

Attestation Form

- **Ms. Moussouris** – What is the end goal of the attestation form, is it for enforcement if you've attested to something that was found to not be true? How is that going to be used?
  - **Mr. Duffy** – I think the timing will be right for the next meeting to have OMB present. The focus has been on developing the questions and getting them out and the focus here was to give the board feedback. It would be helpful for this board, helpful for NIST, and helpful for our recommendations would be what we do with it.
  - **Mr. Lipner** – My interpretation is that if you attest to those things and then demonstrate product attributes that are pretty egregious, then you may be caught for some federal contracting violation.
  - **Ms. Flynn-Goodwin** – Legally, it's an after the fact artifact. In the event that something goes wrong, the federal government has that as Exhibit A where you've made a statement and can then ask were you lying then or are you lying now? Even if it doesn't serve a particular purpose today, it's an insurance policy in the future.

Next Meeting: The July 17-18, 2024 meeting is currently being planned as a virtual meeting.

Motion made and seconded to adjourn meeting. The Chair thanked everyone for their participation and adjourned the meeting at 3:30 p.m. ET.

ISPAB – March 20-21, 2024		
Last Name	First Name	Affiliation
Board Members in Attendance		
Lipner	Steve	SAFECode (Chairperson)
Flynn Goodwin	Cristin	Advancing Cyber
Gantman	Alex	Qualcomm
Gattoni	Brian	Federal Reserve Board
Groman	Marc	Privacy Consulting
Venables	Philip	Google Cloud
Moussouris	Katie	Luta Security
Duffy	Michael	CISA Cybersecurity Division, DHS
Board Members Not in Attendance		
Baker	Brett	NARA
Fanti	Giulia	Carnegie Melon University
Fitzgerald-McKay	Jessica	NSA
Miller	Essye	Executive Business Management (EBM)
NIST Staff		
Brewer	Jeff	NIST
Scholl	Matt	NIST
Petersen	Rodney	NIST
Proud-Madruga	Diana	HII/Electrosoft
Elliott	Savannah	HII
Lurie	Kirk	HII
Speakers		
Chen	Dr. Lily	NIST

Kolter	Dr. Zico	CMU
Lyublanovitz	Shon	CISA
Massaro	Andrik	DOC
Mislove	Dr Alan	OSTP
Peterson	Rodney	NIST
Polk	Nicholas	OMB, EOP
Scholl	Mathew	NIST
Stine	Kevin	NIST
Vassilev	Apostle	NIST
Attendees		
Boldt	Douglas	AWS
Friedman	Sara	IWP News
Livesay	Jacob	Inside Cybersecurity
Mertz	Stephanie	U.S. Commerce Committee
Oliver	Theresa	Wilkinson Barker Knauer
Sakellariadis	John	Politico
Wildenauer	Leopold	ITIC

Certified and approved by

Steven B. Lipner
Chair
Information Security and Privacy Advisory Board