Wednesday, July 12, 2023

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.
- Guidance to Board members: while the board provides formal input to the agencies with board letters, the members’ comments and questions during the sessions with speakers also add value.
- Reviewed the agenda.
  - Mentioned that Deirdre Mulligan from the White House Office of Science and Technology Policy (OSTP) is unable to attend the meeting. They will try to get her back at another time.
  - Mr. Lipner described the structure of the agenda. Each speaker gets a half hour slot and then there’s a scheduled 15 minutes to allow Board members to ask questions or interact with the speakers and topics.

Board Member Introductions and Updates

Mr. Lipner, Chair –

- Executive Director of SAFECODE, software security guy, and retired from Microsoft.
- Most of his career has been spent trying to figure out how organizations can build more secure software.
Ms. Miller –
• Ms. Miller mostly focuses on the next generation of cyber talent and how we pull that out with US Cyber Challenge and the National Scholarship Foundation for Cyber.

Mr. Groman –
• Former Senior Advisor for Privacy, second term in the Obama White House.
• Prior to that, Mr. Groman was Chief Privacy Officer of the Federal Trade Commission and a prosecutor focusing on internet fraud.
• Currently teaching at Georgetown Law School, cyber and privacy for lawyers and consulting at Fort Meade with NSA.

Mr. Gattoni –
• Currently an Assistant Director at the Federal Reserve Board of Governors.
• In January, started a job involving responsibility for IT resilience and cybersecurity for the Federal Reserve System.
• Prior to that, Mr. Gattoni spent 12 years at CISA as their Chief Technology Officer.

Mr. Gantman –
• Vice President of Security Engineering at Qualcomm.
• Leads the product security team and the software team that implements the security features.

Ms. Fanti –
• Assistant Professor of Electrical and Computer Engineering at Carnegie Mellon.
• Working on security and privacy of distributed systems.

Ms. Fitzgerald-McKay -
• One of the leads for NSA Center for Cybersecurity Standards.

Dr. Baker –
• Inspector General at the National Archives.

Welcome from the NIST Director: NIST Priorities for the Future

Dr. Laurie Locascio, NIST Director and Under Secretary for standards and Technology

Introduction

• Dr. Locascio thanked ISPAB for the advice and the input that NIST gets as we talk through these sessions. She mentioned that this advice is important as they move forward in every area of their work. But it's critically important in privacy and cybersecurity efforts because their stakeholders trust their intentions, and trust that their work has value to create positive impacts and ISPAB’s guidance is a clear part of how they are building that trust.
• NIST’s cybersecurity efforts have gone on for more than 50 years.
• NIST’s goal is to continuously improve the US government in both cybersecurity and privacy.
• NIST is working to establish an independent public and transparent foundation for all of their work.
• Dr. Locascio was at NIST for 31 years, left for five years, and had the opportunity to come back last year (2022).
NIST Priorities

- When she re-joined NIST in April 2022, NIST established a set of priorities in critical and emerging technologies, manufacturing - including chips-, and international standards.
- Lots of challenges in the area of critical and emerging technologies. Society benefits greatly from the development of critical and emerging technologies but it's important that we reap the benefits of the development of these technologies in a safe, secure and privacy enhancing way that further engenders trust.
- It’s important that the US is also a leader in innovation and technology development for the future of our economy. Our economy is a tech economy.
- Underpinning that tech economy with security, safety and privacy is critical.
- NIST is working to:
  - Revitalize US manufacturing across multiple sectors and across the United States.
  - Fuel the innovation economy through investments in critical and emerging technologies.
  - Position NIST as the premier national metrology institute in the world, helping our industries to compete and thrive in the global economy.
- We will need key partnerships with those outside of NIST, like ISPAB, to help meet the nation's challenges in critical and emerging technologies.
- Critical and Emerging Technologies:
  - Focusing on funding cybersecurity and privacy, artificial intelligence, biotechnology, advanced communications, energy technologies, and quantum information science.
  - Quantum Information Science:
    - NIST is engaged with domestic and international partners, including many US companies, through the Quantum Economic Development Consortium (QEDC). That's a great forum for everyone who's innovating in the future or current quantum economy, to come together to look at where the issues are relevant to growing the market.
    - Believe that the quantum economy or the quantum market will have a transformative impact on our lives in the future.
    - We have some of the best researchers of quantum in the world, investigating the building blocks for what will become the future of quantum computing, quantum sensing, and quantum networking.
    - This will keep us at the forefront of quantum engineering and quantum science to develop new standards and measurements that will be needed to drive this entirely new industry.
    - We don't know when to anticipate the development of the quantum computer that's powerful enough to threaten our current encryption algorithms, we are preparing for that by developing post quantum cryptography standards.
      - Has culminated in the selection of encryption algorithms and the development of standards this year.
  - Biotechnology:
    - Investigating how engineering biology and bio manufacturing innovations will change how we address societal goals like supply chain resilience, food security, energy independence, and better health care outcomes.
    - All of these require attention to cybersecurity and privacy.
    - NIST, like the Department of Commerce, is not a sector specific agency. So, their biotechnology research and standards are focused on platform technologies that will enable industry to move and innovate more quickly. Some of these include automated systems for
generating predictive cellular responses, and standards for measuring the efficacy of gene editing.

- Machine Learning and AI.
  - NIST efforts are clearly focused on supporting and providing the underpinning for trustworthy AI systems.
  - AI has gotten a lot of attention lately because of generative AI, and it's going to impact so many parts of our society and our economy, including quantum AI and AI in biology.
  - In January, NIST released the AI risk management framework.
    - The response in the first three months after it's released was overwhelmingly positive.
    - It was developed using a highly collaborative approach and recognizing that managing risks of AI systems is essential toward establishing trust.
      - Developed in partnership with private and public sectors and to better manage risks to individuals, organizations, and societies.
      - All those risks associated with AI are posed across many different layers in our societies, and in our government.
    - Building off this framework, they are working in a lot of areas related to generative AI, extending that to examining the specific risks associated with generative AI.
    - Planning to expand benchmarking and evaluation of AI systems in partnership with industry to ensure that US can lead in AI innovation, while ensuring that we address the risks responsibly.

- Standards:
  - Cybersecurity Framework Updates: NIST embarked upon a revision of the Cybersecurity Framework and released the discussion draft earlier this year for the cybersecurity framework 2.0.
    - They know there will be a lot of discussion about their efforts in cybersecurity and privacy, but they are committed to continual improvement and providing trusted resources to improve the ability to prevent and protect against cybersecurity incidents.
    - They bring together the community in the NIST Cybersecurity Center of Excellence (NCCoE), to develop and implement use cases to strengthen cybersecurity across multiple industry sectors including manufacturing, healthcare, banking, and energy.
  - International Standards:
    - International standards underpin 93% of all international trade.
      - Having a robust presence from the US on international standards committees is critical to being able to open markets for our industries across the US.
    - In May, the Biden Harris Administration released the United States National Standard Strategy for Critical and Emerging Technology.
      - This is the first time the government has ever released a national standard strategy and they pointed this specifically at critical and emerging technologies.
      - It's important that we are at the standards table in order to continue to have our economy thrive in the global marketplace.
      - It outlines how the United States will work with like-minded partners and allies to advance our competitiveness and ensure the long term success of our innovation ecosystem.
      - NIST is charged with leading the implementation for the nation.
    - Key objectives:
1) Investment in research: if we do not invest in our research, we will not have the technology solutions to bring to the standards table.
   - Now many other countries have released standard strategies, ours is the only one that points out the importance of our research in the United States.
   - Our research is important in every area of the work that NIST does. If we didn't have robust research efforts that support our ability to then develop these guidance documents and standards, they really wouldn't be worth anything. So, we have to support everything that we do with robust research that backs it up.

2) Participation in standards development activities.
   - One goal we are working toward is to try to increase the US participation at the table all over the world in standards efforts.
   - They will be reaching out to the community to find out how to make sure that our experts are participating when needed, especially in critical and emerging technologies.
   - The difficulty in getting people to participate in critical and emerging technology standards is that a lot of people don't believe that we're ready for standards if the market doesn't support it yet.
     - Therefore, we can't get companies to participate in early standards efforts.
     - The US government is starting to think about how to make sure we're at the table, even if it's early, even if the market is very, very early.

3) Workforce development for a standards savvy workforce.

4) Integrity of the standards process and its governance.
   - This has been threatened in several cases around the world.
   - This is a new leadership role for NIST.
     - Education:
       - NIST supports programs across the US to advance cybersecurity education and workforce development.
     - Manufacturing:
       - Another new NIST leadership role this year is the implementation of the CHIPS program, within the CHIPS and Science Act.
         - NIST is leading the $50 billion program for the Department of Commerce.
           - $39 billion dollars of that is aimed toward bringing semiconductor manufacturing back to the United States, and $11 billion that is aimed toward R&D that will keep them here.
           - Without a robust research and development ecosystem, companies may come here, but why stay?
           - The $39 billion CHIPS incentives program for manufacturing aims to strengthen US economic resilience and national security, including through strengthening the security and resilience of the semiconductor supply chain.
           - NIST has efforts in the cybersecurity of the supply chain in providing a supply of secure semiconductors relevant for national security and bolstering the semiconductor and skilled technical workforces in the United States.
     - Key announcements:
Reached a big milestone at the end of February when CHIPS released its first Notice of Funding Opportunity (NOFO). They are seeking applications for building out manufacturing, construction and expansion, modernization of commercial facilities for front end and back end fabrication of leading edge, current generation, and mature node semiconductors.

- Many places around the world have a CHIPS act and we are trying to make sure that we coordinate with them.
- The second Notice of Funding Opportunity, or the amended Notice of Funding Opportunity, is to build out the supply chain related to CHIPS.
- The third one, that will be released later in the fall, is to support R&D facilities in this country.
- They’ve received over 300 Notice Statements of Interest from over 35 states.
- There are four specific R&D areas that will be coordinated and work with other parts of government and receive funding related to semiconductor electronics:
  - The first is the National Semiconductor Technology Center, or the NSTC, which is envisioned as an anchor for the entire chips R&D program. It aims to conduct research and prototyping of advanced semiconductor technology. It aims to grow the domestic workforce and to strengthen the economic competitiveness and the security of the domestic supply chain.
  - Our funding is five-year funding.
  - We intend for this to be a 30 – 50-year effort that will be aimed at accelerating the pace of innovation in semiconductors in the United States and ensure that the innovations form the foundation for many future industries around the world.
  - The second is the National Advanced packaging manufacturing program that will skip ahead to advanced packaging and try to regain leadership and semiconductor production in the US.
  - The third is aimed at building up to three manufacturing USA Institute's focused on semiconductors.
  - The fourth component of the R&D program is focused on metrology research that will focus on the development of new materials, physical metrology for next generation microelectronics, computational methods and tools for data validation, virtualization and automation, and reference materials, data and calibrations.
- These programs will involve workforce training.
  - Anticipate over 180,000 new jobs produced with the CHIPS funding.
  - Need to figure out the pipeline to fill those jobs.
- They are working to integrate their cybersecurity resources into all of the programs that they are building within CHIPS.

Questions
- **Mr. Groman** – Referenced where Ms. Locascio mentioned assessing risks to society from new technologies like AI. He agreed wholeheartedly and wanted to make sure everyone heard it. He stated that we often focus on risks to individuals or risks to a company or infrastructure, we need to think about risks to society. This is a new way of thinking and it's something that we haven't done well. He also stated that he thinks even our risk frameworks have not offered companies a
way to, for example, properly or thoroughly assess the risk to society from us building this new AI mechanism.

- **Ms. Locascio** – Agreed stating that one of the things that they're realizing is that while there are tremendous benefits associated with all of these innovations, we can look very locally and only see the risks associated with our personal wellbeing. But we have seen with misinformation, disinformation campaigns and multiple other layers of cybersecurity attacks, the real impact holistically on society that can happen if we don't manage those risks. We need to think about those risks as we build our guidance and frameworks and have these discussions about how we can move forward with critical and emerging technologies.

- **Mr. St. Pierre** – Agreed that the AI risk management framework specifically talks about a socio-technical approach because we see the impact from the rapid acceleration of AI on society. The generative AI group will provide input on how to develop a profile of the risk management framework for generative AI and, in the midterm, provide guidance on testing, evaluation, validation, and verification for generative AI. In the long term, they are looking at the best way to use it wisely for large national problems, in, for example, health care or the environment.

- **Mr. Stine** – Added that in the privacy framework and NIST's privacy engineering work, we see that fusion of society and technology as well. He mentioned that we'll hear more from Naomi and some others Thursday about progress being made. They have a lot of work being updated and they're trying to infuse some of the goodness from these other efforts to inform our cybersecurity updates. In their digital identity guidelines they're looking at non-biometric alternatives for identity proofing at different levels because of concerns and observations around disparities and ways different algorithms treat different classes of the community. They're starting to see those socio technical considerations being infused and informing all of NIST's efforts across the board.

- **Mr. Lipner** – Mentioned that the focus of a lot of the NIST products on cybersecurity, privacy, and AI, is on risk. That's a tough problem because it's not like fire insurance or auto insurance, where you're dealing with very measurable sorts of things. He acknowledged that the NIST staffs know that and anything that NIST can do to help the private sector and the government do risk assessment other than by gut feel would be a big contribution. It may be impossible but it's worth looking at.

- **Ms. Locascio** – Agreed and stated that's what they tried to do. They have specific use cases with various sectors and they're able to work through the problem, understand where specific risks might be, and help them manage to those risks. She feels that's one of the best ways that they can have a "boots on the ground" discussion around risks associated with specific sectors.

- **Mr. Stine** – Mentioned that the board has chatted about different parts of this challenge in the past as well. One part is from a measurement perspective. With NIST being a precision measurement organization, precision measurement and cybersecurity don't always go hand in hand; there's that soft, gooey middle where we're operating, given the dynamic nature and the pace of change. All of our organizations and resources come at cybersecurity, privacy, AI, and other technology domains through that risk management lens. This is also a research problem, trying to get a better sense of how to bring more science and data in to inform better risk management decisions. They don't have all the answers, but they have a lot of resources. There's a lot of community effort and community involvement to help further evolve those and build those out.

The CSF update process is providing a lot of additional feedback, particularly focused on
using tools like the CSF and other guidance with respect to using measurement to inform better management but this is still a work in progress and has been for many decades. They are making progress and we should see some of those findings and observations feed into future NIST guidance.

- **Ms. Locascio** – Agreed and mentioned that these kinds of measurement methods haven’t been developed ever. NIST is the National Metrology Institute for the United States. There is no other national metrology institute around the globe that has taken on the digital economy. NIST is the only one trying to develop measurement methods that are robust and can support the digital economy globally. Most others remain physical measurement institutes.

- **Mr. Gantman** – Said thank you and acknowledged NIST’s focus on semiconductor security. He asked: 1) How much interaction or collaboration is there between the different laboratories? And 2) Safety, resilience, risk management, quantification of efficacy, and measuring outcomes seem like they would be pervasive in all the disciplines. While security risk is different from fire risk, he thinks there are probably a lot of similarities as well and a lot that we can learn from these other communities; to what extent are these groups talking to each other?

- **Mr. Scholl** – Stated that NIST is a strange place, but in a good way. The division between laboratories within NIST is functional and organizational, but it is extraordinarily easy for them to cross collaborate and to work with other experts in other fields. It is also actively encouraged by how the programs are structured.

- **Mr. Gantman** – Added that it would be good to see collaboration around more abstract topics like risk management and efficacy quantification to answer questions like, “do we know that this intervention works?”

- **Mr. Scholl** – Agreed and added that sometimes they think they understand the cybersecurity measurement and then they talk to their material measurements scientists, Standards Coordination Office, and other people, and they point out other ways of thinking.

- **Mr. Gantman** – When something like that happens, do they ever get like cross listed when it applies across domains?

- **Mr. Scholl** – Responded that's a good question and he’s unaware of a cross post type of thing.

- **Mr. St. James** – Added that one document they did in cooperation with the engineering lab was on manufacturing control system security. Even though it's a cybersecurity document, they communicate that to their stakeholders very effectively. Given how much is going on in cyber, coordination between and being involved in those efforts is a challenge. They absolutely want to leverage the domain expertise of others.

- **Ms. Fanti** – Mentioned that many of the harms that can come from AI systems are large scale and you might need a lot of data to see them. It could be more than any single organization or enterprise is able to measure from their own data. She was wondering if there are efforts within NIST to think about what would be required for industry-wide or sector-wide measurement of harms that come out of AI systems?

- **Ms. Locascio** – Replied that they do not think this is a problem that NIST should tackle on its own. They have ideas for how to build out a public-private partnership to start making sure that they can address the appropriate measurements and measurement methods and think about understanding the impacts on the large language models.

- **Mr. St. Pierre** – Added that’s part of the concepts baked into the AI RMF. We want to take it as broadly as possible to look at the potential societal harms and when getting access to data is a challenge. For example, in facial recognition testing, they used data that they were able to
access through other federal agencies. They had to partner on that. He envisions similar efforts where they reach out and build partnerships.

- **Ms. Fanti** – Asked if the data was accessed through legal agreements and if privacy enhancing technologies were used?
- **Mr. St. Pierre** – He’s pretty sure their lawyers were involved. There were legal agreements to cover the transfer of that data in adherence to all human subjects regulations. We adhere to all that we have a very strong human subjects program at NIST.

  - **Mr. Groman** – Commented that it seems no one wants data minimization, and they want it forever, which rubs up against the basic core tenants of privacy and fair information principles. As a government and society, we will have to wrestle with how those two will mesh.
- **Mr. Lipner** – Asked if NIST is involved in the agreements between the US and the EU on data privacy in the way that commercial organizations can collect or manage?
- **Mr. Stine** – Mentioned he’s not entirely sure of the specific law or rule that Mr. Lipner is referring to. He knows that they do engage in a lot of US and EU forums on that topic. A lot of our interests and activities are related to the degree to which standards can be used to bring greater technical standards that can be used to provide a greater foundation of trust, regardless of the specific rules, regulatory regime, or laws that might be discussed. In the EU discussions, they get a lot of feedback from industries that want to be competitive in global markets. The role that we play most frequently involves the degree to which our resources or expertise can be supportive of the US positions.
- **Mr. Scholl** – Mentioned at the Commerce level, they work on the Privacy Shield regulation, which is a reflection of the EU privacy laws to ensure that US information and privacy considerations have technical interoperability between the US and the EU.
- **Mr. Lipner** – Mentioned that was the agreement he was thinking of. There was a new iteration that the EU has decided to accept. He is wondering if the US positions are informed by NIST?
- **Mr. Scholl** – He’s not aware of it.
- **Mr. Groman** – Mentioned that one focus of the discussion has been how the American intelligence community can access data once it's been brought to the United States. Things like NIST frameworks might be relevant, but this is an issue led by the Secretary of Commerce and other parts of commerce. The Executive Order was just issued, and Europe approved it to allow data to flow from Europe to the United States.
- **Mr. Lipner** – Was wondering if there are any technical measures or potential standards that would have helped make that work better or more efficient for the Europeans.
- **Mr. Groman** – Mentioned that it’s not about technical standards. It’s about politics and privacy more than standards,
- **Ms. Locascio** – Mentioned that NIST is involved through the U.S.-EU Trade & Technology Council (TTC). They lead one of the working groups in the TTC associated with standards and are involved through the Organization for Economic Co-operation and Development (OECD) interactions.

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

**ITL Update**
Jim St. Pierre, Acting Director, Information Technology Laboratory (ITL), NIST

**Updates**
• Thanked the ISPAB board for their time and input. It helps them continue to improve.
• Chuck Romine is now the Associate Director for laboratory programs.
  o Probably the first time in history that somebody with an IT and mathematical background has been in that position. This brings a unique perspective.

Purpose

• Stays the same as always: Cultivating trust in metrology.
  o NIST consists of dedicated public servants and it's a real honor and a thrill to work with these folks on a daily basis.

NIST Wide Critical and Emerging Technology

• We lead NIST efforts, and we partner with people across NIST, but we are the focal point of NIST efforts in:
  o Cybersecurity and Privacy
  o Artificial Intelligence
  o Biotechnologies
    ▪ For example: security of genomic data.
  o Quantum Information Science
  o Advanced Communications
    ▪ At the NCCoE, we have a new 5G cybersecurity lab.
  o Energy Technology

NIST AI Program

• The AI program has gotten a lot of attention recently.
  o We focus on conducting foundational research to advance trustworthy AI technologies.
  o We work with other laboratories who are using and starting to explore the use of AI to advance their metrology research.
    ▪ We have initiated some of that research and funded some of that early on.
  o We are establishing benchmarks and metrics to evaluate AI techniques.
  o We take a leadership role in the development of standards.
  o Our expertise is sought out in discussions and development of policy to inform AI.
    ▪ Policymakers have a lot of questions about AI technology such as facial recognition.
      - For example, Congress is very interested in understanding our measurement of bias in facial recognition so that can inform their policies.
      - They want to know what works and how well they work if there are concerns to take into consideration when developing policies.
  o One key role is ensuring that NIST has the resources and expertise to carry out its AI mission.
    ▪ Need to make sure we're communicating to the right stakeholders about what our role is.
    ▪ We often get questions about what we can we do, so it's important for us to ensure that we have sufficient resources.

Trustworthy and Responsible AI at NIST

• New activities and announcements:
The National Science Foundation’s (NSF) National AI Institute on Trustworthy AI.
  a.k.a: TRAILS
  Led by the University of Maryland in partnership with Georgetown and two other universities: Morgan State and Cornell
  Aims to transform the practice of AI from one driven primarily by technological innovation to one driven with attention to ethics, human rights, and support for communities whose voices have been marginalized into mainstream AI.
  Co-funded by NIST and NSF

We help to administer the National AI Advisory Committee and many international engagements.

NIST AI Risk Management Framework (RMF)

Like many of NIST’s documents, the Risk Management Framework is voluntary.
  There are lots of discussions about how others might use it.

Mr. Groman – Asked if it’s voluntary for the government?
  Mr. St. Pierre – Confirmed that it is voluntary.

Summary of effort:
  In 2021, they put out an RFI seeking input.
  They held a series of workshops and put out some publications and draft documents to engage the community.
  Modeled after the successful work in getting buy-in on the CSF.

AI RMF Core
  Similar to the core functions of the cybersecurity framework
  Govern – this is in the middle. This is similar to the separate Govern function found in the CSF 2.0. Governance is woven throughout but there is now also a separate Govern function.
  Map – Context is recognized, and risks related to context are identified. This happens when one is starting to think about how to apply this, understanding the risks, and making a “go-no go” decision.
  Measure – determining how to measure the different risks. This includes measuring all the different aspects of trustworthiness, such as security, resilience, and safety.
  Manage – this is putting into action things that are defined under governance, such as policies and procedures, running the ongoing programs, and making improvements and changes.

AI RMF Roadmap
  This is a roadmap put out in conjunction with the AI RMF
  There's still a lot of work to be done. He covered some of the highlights from the PPT.
    There is a lot of interest in test, evaluation, verification, validation (TEVV) from our Metrology Institute
      NIST is seeking a lot of input from public private partnerships on achieving TEVV.
    Number five on the roadmap is on the overall effectiveness of the AI RMF.
      How do we improve and evolve the AI RMF to keep up with the changes in technology and threats
    Number four is about guidance on the tradeoffs and the relationships among the many trustworthy characteristics.
    Number seven is about guidance on human factors and human-AI teaming in the context of AI risk management.
      That is looking at how to provide guidance on how to do that. For example:
        How to join some of our facial recognition work
They found that the best results were with AI and AI-enhanced human assessment of facial recognition.

Number 10 is about tutorials and other resources to help train and make people aware of multi-disciplinary and social-technical approaches to AI Risk Management on an ongoing basis.

**NIST Trustworthy AI Resource Center**

- Announced at the Summit for Democracy
- Contains things such as the
  - AI RMF playbook.
    - It's intended to present ways to achieve the outcomes described in the AI RMF
  - AI RMF profiles
    - Developed for different sectors such as Generative AI
  - NIST released “The Language of Trustworthy AI: An In-Depth Glossary of Terms”.
    - Standardizes terminology.
  - AI Metrics Hub is a link to the Organization for Economic Cooperation and Development (OECD).
    - Will continue as industry and academia develops more metrics.

**USG Standards AI Coordinator**

  - Response to EO 13859
  - Engaging in outreach to connect with all the known federal efforts relating to AI standards development.
  - Contributing to AI standards, as well as a crosswalk between two international standards,
  - Playing a key role to help harmonization between standards.

**Trustworthy AI in Law and Society (TRAILS)**

- Focuses on the ethical and societal considerations of AI and how to build systems that are trusted by people who use them and are affected by them.
- Led by University of Maryland in partnership with George Washington, and Morgan State Universities
- Co funded by NSF and NIST.

**International Engagement**

- They have ongoing engagement from their AI team and
  - US-UK cooperation,
  - The OECD network of experts on AI,
    - They have some linkage here on metrics.
    - Around 38 countries are involved.
  - Very active in standards and AI discussions, trustworthy AI, between the US and the EU.
  - The quadrilateral security dialogue standard subgroup looking at AI,
Face Recognition

- Ongoing work.
- A lot of interesting topics such as:
  - Being able to help measure how well morph can be detected.
    - This is combining the images of two people.
  - There is an ongoing evolution of this.
  - Seeing overall improvement of the technology over time which is of interest to Congress.

ISO/IEC 29794-5 – Face Image Quality

- Something that affects facial recognition tremendously is the quality and variety of the facial images you feed into the system.
  - This has an effect on bias issues that arise.
- ITL is involved with this standard.
- Two main aspects of the image:
  - The subject’s behavior;
    - What are their expressions? How is their head positioned? Are they wearing glasses, etc.
  - The camera in the environment,
    - Illumination can make a big difference, resolution, etc.
- Providing guidance that can improve facial quality will help improve the overall operation of the technology.
- **Mr. Groman** – Asked about the source of the images. Did they go out and scrape the entire internet and pick up whatever images they could, regardless of what they were created for, which could be thousands of different purposes, or did they acquire a database of photographs taken by an agency that needed to have some kind of basic clarity? It's not just the quality of the image. We need to consider the source of data being used.
  - **Mr. St. Pierre** – Replied that much of the data that they test comes from other agencies and they go through their Human Subjects Protection. They don't just grab data off the internet. They have to go through an evaluation of where they're getting the data. One of the issues they find is even those sources, such as law enforcement data, don't have the same image. So, this is an effort to provide guidance that would help drive improvements in the image quality.
  - **Ms. Miller** – Asked if all of the data they're pulling is coming from authoritative sources and not from public sources?
    - **Mr. St. Pierre** – Confirmed this is the case and it makes a difference but there are still challenges.
- **Ms. Fanti** – Asked if we are talking about training or testing data?
  - **Mr. St. Pierre** – Replied that both come from the same source, but they separate them so that when you're testing, you're using different data from the same source.
  - **Mr. Scholl** – Added that, with the FRBT program, the face recognition vendor test is a test data set that NIST hosts and that the recognition algorithms can run against and then check their accuracy, speed, throughput, and other characteristics. NIST created a test data set, using authoritative sources, to create that data set that other vendors can take and use their algorithms to check against. They work on the standards piece to help people build better references so that they can do those types of testing, capture, match, or whatever.
o Ms. Fanti - Asked if all of the test data is coming from authoritative sources, wouldn’t that be too easy of a test set? Because in the real world, you won't have a controlled environment.

o Mr. St. Pierre – Replied that even with very controlled test data, some of the algorithms still don't perform as well as others.

NCCOE Projects Underway

- The top ongoing projects are mobile deployment, wastewater Sector Project, and the genomic data Cybersecurity Framework profile.
- NIST has published a draft profile, open for public comment, for hybrid satellite networks, IoT onboarding, and migration to post Quantum cryptography.

Revision to Cybersecurity Framework

- Comment period closed May 31.
- The focus on critical infrastructure was taken away but it can still be applied in critical infrastructure.
- More emphasis on supply chain throughout the 2.0 updates.
- Over the 10 years since it was introduced, there have been big changes to technologies and threats, so it was time for us to start looking at this with input from the community.

Encryption Updates

- The end of DES, it will be disallowed within the federal government after December 31, 2023.
- The lightweight encryption algorithm selection was made.
  o Held sixth workshop on June 21, 2023.
- Planning for the AES modes workshop in October.
- Expect to have the PQC draft standard soon.
  o Ms. Miller – Asked if they have a sense of the impact to ending DES at the end of the year?
    ▪ Mr. Scholl – Replied that they reached out to a couple of industries and through public comments. There will be some disruption to some legacy systems, and they heard from some folks saying this is going to potentially be both a problem and an opportunity. There are some large industries, like power generators, some legacy space operations, and potential areas of the DoD, that are going to have to either put something in front to provide the extra protection or increase the importance of this on the legacy upgrade list.
  o Mr. Groman – Asked who the AI work reports through?
    ▪ Mr. St. Pierre – Replied that it reports up through him. Elham Tabassi is the Associate Director for Critical Emerging Technologies and AI falls under that umbrella.
- NIST has the Joint Center for Quantum Information in Computer Science (QuICS) at University of Maryland.
  o Sits at the intersection between computer science and physics.
    ▪ Developed the Error Correction Zoo: an online catalog of 430 quantum and classical error correction codes, both quantum and classical.
    ▪ Looking at a number of other aspects, including AI-based methods for tuning quantum dots for use as qubits, a powerful use of AI in that in that particular domain.
- Quantum Characterization
  o Developed methods for quantum state and process tomography.
  o Physics and Measurement Lab (PML)
They work closely with researchers in the physics lab.
- For example, they demonstrated interesting entanglement of macroscopic vibrating drumheads.
  - That was physics world's top breakthrough in 2021.

- Quantum Networking
  - NIST has a leadership role working with ARL, NRL, USNO, NASA, and NSA.
  - Synchronized network nodes to below 200 picoseconds, over 128 kilometers, and distributed entanglement over 130 kilometers.

- Quantum Information Applications
  - Developed protocols for generating random numbers based on the loophole-free Bell tests.

**NIST National Vulnerability Database (NVD)**

- NIST has had NVD for a long time.
  - It's used around the world, and they continue to make improvements to advance this.
  - Have new API's that will help industry integrate and use NVD.
    - Working towards automation because vulnerabilities are increasing.
  - Adding information to its CVE detail pages and linkage to CISA’s Known Exploited Vulnerabilities (KEVS) catalog.

**NICE**

- Continues to be very active.
- There's a new Notice of Funding Opportunity (NOFO) to establish regional and multi-partnership, multi-holder, and multi-stakeholder partnerships towards education and workforce development.
- The K-12 Conference call for proposals deadline coming up July 28
- Published NISTIR 8355: NICE Framework Competency Areas.

**Recognitions**

- NIST Software Testing paper
  - Based on the ideas of combinatorial testing that we've been looking at for a long time,
  - Recognized at the IEEE conference on software testing, verification and validation as the most influential paper in the “practical” category published during the past 10 years.
  - Rodney Peterson and Karen Wetzel from the NICE program received the National Center of Academic Excellence in Cybersecurity Service Recognition Award.
  - Department of Commerce Silver Medal Award
    - Recognized for outstanding technical innovation to strengthen the resilience of the nation’s Positioning, Navigation, and Timing (PNT) infrastructure and services.

**Discussion**

- **Mr. Lipner** – Asked if NCCoE is working on guidance and standards for the programs he mentioned, in particular the AI RMF.
  - **Mr. St. Pierre** – Confirmed that, in addition to the profiles, they’re looking at use cases of particular examples and the NCCoE has worked AI testing.
  - **Mr. Stine** – Added that some of their early work on AI had been around adversarial machine learning and having a better understanding of adversarial machine learning taxonomy to then
inform some of our other work. A lot of the work that's happening right now is to establish test infrastructure, test evaluation, verification, and validation methods and tools that can be applied in the context of different AI models. They will likely have some guidance coming out around that and make those tools and capabilities available to the broader community.

- **Mr. Lipner** – Commented that risk and risk assessment is difficult and tends to not be quantitative. He asked if there is any work at NCCoE to help with assessing risk that adds value for organizations that are trying to apply some of the standards, like both RMS standards?
  - **Mr. Stine** – Agreed that NCCoE is a good place to do that. The challenge is how to answer higher level questions like, “Am I more secure today than I was yesterday?” or, “Where, if I have $100 for cybersecurity, am I going to get that or more in terms of ROI from a cybersecurity perspective?” He agreed that they have an opportunity to build that into some of the NCCoE projects. It will likely be a combination of qualitative and quantitative, but it is an area they are paying attention to.

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

**NASA Secure by Design Use Case with Risk Management Framework**

Dr. Kymie Tan, Chief Cybersecurity Engineer, Jet Propulsion Laboratory, NASA, Engineering & Science Directorate

**Introduction**

- NIST SP 800-160 collaboration between NIST and JPL/NASA.
  - It touches on our inability to deal with cybersecurity risks on many of JPL’s missions.

**Space/Cyberspace Security**

- With the advent of the Ukrainian war and Chinese incursions into US interests, cyber security and space have become a serious concern for all of us.
- Many of the technologies used within the space missions are in almost every sector: defense, agriculture, energy and so forth,
- We are in “contested space”.
  - Requires NASA to shift their culture to be a little more defensive.
  - The civil space community that’s also growing around space and the accessibility of space is a concern for us.
- Something they have observed over the past few years is that space is becoming more accessible to businesses, schools, and so forth.
  - Many companies, especially in the southern California region, have grown up providing space assets, instruments and so forth.
    - Their efforts don't necessarily naturally encompass cyber security. Very focused on mission and mission objectives.
  - Innovation is key.
    - Space cybersecurity needs to be inculcated or injected into that environment.
- Observed that the adversaries they are seeing may be Space Engineers
  - They seem to know what they're looking for.

**NASA SMD and JPL Perspective**
• SMD is the Science Mission Directorate at NASA headquarters.
  o They tend to sponsor a lot of the work at JPL.
• JPL's main mission is robotic exploration of space, not human.
  o They go first, often before the human exploration of space.
  o SMD is a huge sponsor of a lot of the earth missions.
    ▪ Get a lot of data, particularly around climate science.
    ▪ Also do one off special flagship missions like Clipper which goes to Europa.
    ▪ It's a spacecraft that will circle the moon just to do science.
• They tend to rely on traditional ways of engineering and measuring risk.
  o Need to improve that and include cybersecurity.
  o SMD and JPL see the space cyber engineering portion as OT.
    ▪ A problem is that cyber is perceived to have grown out of the IT world, but the adversaries
      have moved into the operational world.
    ▪ In the operational world, a lot of the IT knowledge may not be as effective.
    ▪ Need to understand this problem from the mission point of view.
    ▪ There are a lot of cultural issues.
      - Need to deal with training, policy modifications.
  o They need cyber capable mission engineers,
    ▪ Putting cybersecurity experts into missions hasn’t solved the problem, because cybersecurity
      experts tend to see the world or speak in a different language from mission engineers.
    ▪ Had to train the mission engineers to be cyber capable.
      - They need to have basic knowledge of what it means to be attacked and include that in
        their risk assessments.
      - That is a cultural change that needs to happen fast.
  o Need a more in-depth set of systems engineering principles to go in and allow us to gain some
    insights as to where the risks are.
• The threats are changing fast, and the threat actors appear to have a lot of knowledge about space.
  o The Space and mission engineers need to be at the forefront of defense, not the IT cyber people
    alone.

The Problem

• Had a huge NASA-wide mission cybersecurity workshop.
  o Brought all the engineers together, including OCIO, to discuss the key issues.
  o NASA and JPL have a long history of dealing with risk, not cyber risks, but every other risk such
    as safety and reliability.
  o Cyber risks are relatively new for them.
  o Need to understand cybersecurity risks within the context of a mission and mission objectives.
  o Agreed the biggest problem is that cybersecurity risks for NASA missions are not effectively
    addressed.
• Two sets of problems identified: Technical and Non-Technical Problems
  o The non-technical problems drive a lot of these missions.
  o Technical Problems:
    ▪ A lot of the people who accept cybersecurity risks do not have the depth of knowledge to
      understand the impact of that risk to mission objectives.
- It’s hard for them to understand a lot of the cyber physical components that are on missions so they can’t fully understand the impact of certain controls on the success of the mission.
- Unless they understand the priorities at different phases of the lifecycle of a mission, they can’t talk about which objectives have become high risk.
- Safety and reliably resides within the purview of a mission, cyber risks reside within the purview of the IT group but the people who have to do the remediation are on the mission side.
  - The current process lacks alignment with the mission’s natural engineering lifecycle, it's a disconnected process that happens later in the life of the mission.
  - Resilience is hard to determine because the engineered system is a “black box.”

- Non-technical problems:
  - Ambiguous risk ROI.
    - Project managers are constantly asked for more money and resources to do cyber.
    - They have mission objectives. Cyber has to be costed out and could take away from mission and scientific experimentations.
    - The unknown costs and burden of compliance of compliance growing.
    - NASA missions have very well-established frameworks, cyber risks should flow into that framework. It currently doesn't.
  - Governance
    - With NASA missions, it's not one project manager and one mission that controls everything. This makes it difficult to capture and define all the risks.
    - Risk assessments are done at a different level, and you don't know what kind of risk assessment they were doing.
  - And then fundamental problems to the risk assessment process itself, like threat intelligence, haven’t been solved with the common risk assessment.
    - Example: threat intelligence,
      - Problem with accessibility of the information
        - Not everyone has the right clearances.
        - Inability to take that information and process it into actionable items for mission engineers.

Layered Technical and Governance Approach

- Enterprise systems go through the 800-37 (RMF) process.
- Mission systems
  - Innovative cyber physical systems
  - NIST SP 800-160
- The Office of the National Cyber Directorate (ONCD)
  - Carrying out workshops to get a better handle on space, cyber engineering, what the policies should be, what the problems are, the gaps, and so forth.
  - Frustration was expressed about the way we're doing risk management for cyber right now.
    - Checklist driven which inhibits innovation.
- NIST SP 800-160 is trying to get insights on risk and resilience by design, meaning incorporating from the start of the systems engineering process that all space missions go through.
  - Goal is to get a better idea of what we mean when the system is resilient.
Example: A lot of the mission systems right now do fault protection / fault tolerance, the effects of that can inadvertently defend against some, all, or a small group of attacks that we're currently seeing. But that kind of defense is never taken into account, because it doesn't come from the IT world. It is deeply woven in the mission world.

- To understand risk, we need to understand what natural defenses are already there.
- Proposal is mission systems might need a different way to achieve this.

Why Systems Security Engineering Approach?

- All NASA missions follow the systems engineering approach.
- Differences between traditional compliance and the systems engineering approach (shown on slide 8 of the presentation)
- Potential gains to following the systems engineering approach:
  - Focus: Move away from checklists (traditional) to having evidence of the resilience of the engineered system or insights into the defensive capabilities of the engineered system
  - Mission: Instead of treating it as a black box mission, we want something that has mission success context
  - Coverage: If you understand the system better and the mission better, you can prioritize critical systems and critical functions.
    - Right now, because the mission is not understood very well, on the IT side, there is no prioritization.
  - Timing: Traditional compliance done after the system is built
    - 800-160 is intended to be woven through the entire lifecycle.
  - Risk management: Traditional compliance has a separate authorization to operate, as opposed to being part of the systems engineering process of review, V&V, etc. at every stage of the lifecycle.
  - Leverage: We want to leverage existing systems engineering processes, versus creating more silos of new cybersecurity processes.
  - Innovation: we want to be able to anticipate future attacks and understand the system well enough to know what is naturally there that can prevent certain effects of adversaries and certain actions that they might put into our system.

Pilot Goals and Vision Objectives

- 800-160 is descriptive but does not have the kind of details that our engineers need.
- Need to bring those principles down to where the tire hits the road and how to affect it on our missions, the insights that we can gain.
- Example: there are certain terms within 800-160 about integrated functions as a separate defined group of functions
  - In Mission worlds, the integrated set of functions may not be as clearly defined.
    - May have overlaps with other critical functions,
    - Insights like this can help us perhaps move forward in terms of defense and resilience.
- Requirements: we want to be able to allow the mission project manager to do tradeoffs between security, safety, and reliability; we want to bring cyber into their purview
- Verification: want to be able to do cyber as a part of systems engineering lifecycle so that it goes all the way through.
  - Hope is that we won’t need to pay extra for the AMA process.
- Principles: We want to identify a set of repeatable activities, so that this can go to all projects
• Planning: Understand cost, complexity, & challenges integrating systems security engineering into mission engineering lifecycle
  o Suspect it would be less because there are native defenses that are there for protection,
  o Have to get the data to support that.

Mapping the SP 800-160 into the NASA Mission Lifecycle

• Have taken the NASA lifecycle phases from the NASA Engineering Handbook
  o Mapping that to the technical processes in 800-160
  o Need to go to a lower level than currently done. Example: Sensor implementation
    ▪ Fault protection does an implementation of sensors and some of those sensors will pick up the kinds of features that adversaries or an attack would manifest.
      - Not currently recognized as that
    ▪ There are a lot of these sensors implemented, inconsistently, depending upon different projects and the needs of different projects.
    ▪ Changing this is “low-hanging fruit”.
      - Make sure that all the sensors and all the data that is pulled in by the engineers for the project is consistent and would address a particular set of attacks.
      - Program managers can use that to detect those attacks.
  o Other things won’t be so easy.
    ▪ Trying to V&V AI processes that are coming into NASA missions to see how adversaries will use that will be more difficult.

Potential Pilot Projects

• Top three of the list of NASA pilot projects that we're looking at.
  o All Low Earth Orbit focused projects
  o ARCSTONE, Incas, and Sentinel 6 B
    ▪ All are looking at climate change, which, given the data that I've seen so far, is actually quite ugly.
    ▪ The data there is saying not only is it happening, but it has also been increasing in speed over the past five years. And that was a thing that is very concerning.
  o Each mission has a has a lifecycle.
    ▪ The pilot won't run from the beginning to the end of one mission. Instead, it'll leverage all the places in the lifecycle that the mission is on.
    ▪ It'll try to build a picture of a more generic mission lifecycle and the insights we can gain from that.

Summary

• Very basic questions are being asked by NASA Project managers like:
  o What is the return on investment?
  o How are you protecting my mission objectives?
  o What risks are you attempting to cover that I would care about?
  o How much money do you want from me?
• NASA missions go for 20 to 30 years.
When it comes to cybersecurity, a lot of those questions haven't been addressed but they need to be given the pressure that we're under because of various nation states, space missions, some of the wars that we're currently seeing, Viacom satellite communications, etc.

This is becoming contested space and cybersecurity sits right in the center.

Discussions

- **Ms. Miller** – Asked about the timeline for the pilots.
  - **Ms. Tan** – Replied that they are doing that analysis. There are a lot of things NASA managers want to see. Product mission managers want to see some kind of result within two to three years. Others want to see it for the flagship missions, which will go on for at least 20 years. They have to try to strike a balance. They’re trying to figure out if there are low hanging fruit that we can identify in a short period of time that will be helpful, not only to space, but also to oil and gas, and other critical infrastructure. More difficult things like AI require more time. They’re planning short-term, as well as a long-term view of this project.

- **Ms. Miller** – Asked if there is a discussion around risk tolerance and who identifies or who accepts a level of risk?
  - **Ms. Tan** – Replied that, in general, there's agreement among project managers that the ATOs chosen on the cyber side to accept risk tolerance levels aren’t qualified to make that decision. They tend to be IT; they can't speak mission language. They’re trying to change that. This is a governance problem because of current compliance laws. In the case of space missions, the CIO and the CISO are useless because the mission is treated as a black box. For example, in one project there are six different ways to remediate on that project. Each way can cost, and the cost can be huge. They went to a CISO and said, “You're going to be signing this. It's up to you who is supposed to be taking the risk. Which way are we going to pick?” He had no idea.
  - **Ms. Miller** – Commented that assumes that it is the CIO IT side that is assuming the risk. Separate the compliance process. First, the risk tolerance; does the mission owner identify the group of people who get to identify the risk tolerance?
  - **Ms. Tan** – Replied that's the problem. The area's gray right now.
  - **Mr. Groman** – Commented that it’s the head of the agency under FISMA and OMB guidance who owns the risk, and sets the agency's risk tolerance?
  - **Ms. Tan** – Replied that might be the case. The problem is, at a very high level, you don't quite work where the adversary works or where the different mission objectives work. There's this issue of layers. Maybe the right thing to do is to have risk tolerance set, or risk acceptance taken at each layer. At too high a level, you say, “Yes.” What does that mean? What risks are you actually accepting? For example, the command subsystem. If an adversary comes in and completely disrupts the command subsystem and takes down telemetry, did you see that at a high level? Did you accept that? They're struggling with a balance of detail. The difference between a high-level view and detailed technical view. The adversary tends to work in the detailed world. It's very hard for a person on a management level to understand both the mission as well as the cyber side to know the impact.
  - **Mr. Lipner** – Commented that the adversary doesn't care who signed off on the ATO or who accepted the risk. What level of management it was, or what level of competence or understanding of the mission. He agreed with Mr. Groman but asserted that doesn’t work well for operational mission stuff.
  - **Mr. Stine** – Clarified that some agency implementations do delegate this responsibility to CIOs and CISOs. He mentioned that the language he recalls is that the deciding official has to have
direct mission and budgetary responsibility, which in most cases is probably not going to be the CIO or the CISO. They should be informative to the decision, but it's not, in most cases, going to be that CIO or CISO.

- **Essye Miller** – Brought up that she thinks they have a great opportunity in NIST to help, as you're bringing these communities together, make that decision. If you're in the military, an operational commander who's on the ground will make certain decisions that are critical in its mission. You've got very specific pilots that you're working on, which gives you an opportunity to have that discussion.
  - **Ms. Tan** – Replied that they can have the discussion, but we have to push against culture and tradition that has been set. The IT versus OT issues are huge on the engineering level. These are the discussions that we've had with the ONCD workshops. The core of this is a governance problem.

- **Mr. Gantman** – Thanked Ms. Tan for speaking as an engineer. He mentioned that the problems she raised are unsolved problems that we all face in our respective spaces. He would be very interested in the outcomes from this pilot project, especially putting it in practice and how it gets translated into something that's directly usable by engineers on the ground. He asked if they are planning on writing it up and sharing?
  - **Ms. Tan** – Replied that one of the plans is to have 800-160 space version. None of this is a silver bullet. It’s an attempt to gain more insights and try to engineer a better, more resilient system. In that publication for space, we will be putting a lot of information regarding the questions detailed earlier. She added that, to her, the person accepting the risk means they understand the risk, impacts, and will pay for remediation. Right now, there is no way to know exactly what is being accepted.
  - **Mr. Groman** – Disagreed with that, gave the example of an OPM incident, and pointed out that it is part of the agency’s job to accept risk. There needs to be data sharing between the CIO/CISO and others at various levels. If we want no risk, we have no data. But we don't want that so there's always going to be some risk. We have a process to identify the various risks and the CIO may indicate that they think the project should do something based on the probability of being hacked, but someone else can modify that or they can choose to not make the change and accept the risk.
  - **Ms. Tan** – Asked how do you understand the risk when the system is treated as a black box?
  - **Mr. Lipner** – Commented that he had an element of the risk acceptance responsibility for Microsoft for software development for a period of about nine years. He based his decisions on how much would cause our developers to mitigate this risk, if the tools were good, how easy it was to get the training, and how quickly it could be done, and the consequences of doing, or not doing, it. Those things are pretty non-quantitative. A lot of it is about gut feel. In the space mission world, he imagines you face things like the spacecraft explodes or it fails to reenter. Those are consequences that can be explained to a director of NASA or a director of JPL. Then the challenge is to get the engineering organization, not the IT organization, to get the competence to see things in code that could be used to cause a problem resulting in the spacecraft exploding. Okay. And then, you know, the capability to make that set of translations may not be resident in one person. He hopes that's what they're aiming to develop and acknowledged it's not easy.
  - **Ms. Tan** – Agreed that they are trying to pull all the stuff that people have been working on, such as architecture and security, and pulling it into the systems engineering process to go into that kind of depth. It's trying to gain understanding. Right now some of the processes for this are broken; some of them do not provide the engineering insights necessary to understand impact.
o Mr. Gantman – Added that subjective judgment as an expert is going to be unavoidable. He doesn’t think they’ll be able to get to the point where they can get the mission head or the agency head to know the outcome of the process, look at the technical details, and understand the risk. What he has settled on a “logarithmic” reading of risk, borrowing from an NSA, DOD publication. It boils down to the risk and where the actual existence of the agency, or at least the position of agency head, is at risk, or it could be strategic. Maybe strategic goals are at risk, or only tactical goals are at risk. And then you figure out how to pay for the tactical risks or deal with it. You try to avoid most of the existential risk and some strategic risk.

o Ms. Tan – Added that we're always going to be reliant on the engineers whose “gut” tells them about problems. However, a lot of the principles in 800-160, although not grounded yet, will cause them to question and gain insights. They're hoping to be able to use that as leverage.

• Mr. Lipner – Mentioned that 800-160 is abstract. A lot of translation will be required to make it real, concrete, and applicable.
  o Ms. Tan – Replied that is why they reached out to NIST for support with the pilot. Because there’s a lot of room for interpretation and trying to bring it down to the engineering level, there are a lot of details that would matter. There are a lot of definitions that might be missing or that might need to be better defined. That's the whole point of this pilot. How can we do that? Are there any insights that would help us?
  o Mr. Lipner – Added that he predicts that they will end up with a document of their own that is recognizable at a high-level as related to 800-160 but all the words in the document are different.
  o Ms. Tan – Replied that it is possible. The status quo right now is not serving us well and we're suffering from it severely, not only with the adversary but also with ourselves and with the federal government. One of the questions that came out in the ONCD workshops was what happened with SPD-5? It was written with so little detailed technical knowledge; you can interpret it in 20 billion different ways. The spirit is there, just like the 160, but the details are not. There are serious technical problems here that we have to deal with, but there are also governance and policy problems that get in the way.

• Ms. Fanti – Asked if this problem can be helped by training CISOs, or cybersecurity people in space science?
  o Ms. Tan – Replied that they tried both. They tried getting very good cyber people and putting them in space missions and trying to train them. Then they tried the other way as well. They've also been running their own space CTS just to see how well their mission engineers are doing when it comes to identifying threats and cyber threats. They're getting better and it's a lot faster than it is for cyber people to understand missions. It seems faster and more effective to get the mission person understanding enough cyber to be effective. Then, once the mission people can better articulate what they need, you have the cyber IT people who help them on IT stuff.

• Mr. Lipner – Thanked her for the presentation and indicated that he would like to have her come back in about a year for an update.

NIST Cybersecurity and Privacy Update
Mathew Scholl, NIST
Kevin Stine, NIST

Introductions

• Mr. Stine started by commenting that the last panel was one of the better sessions he’s sat through.
  o From a federal policy perspective some of the tensions play out
- 800-130 largely touches on the cybersecurity space and 800-123 hits on the federal enterprise risk management space.
  - There's a communications gap or a divide between the two.
- How do we help our cybersecurity folks talk in a language that will be meaningful to the ERM folks
  - From the NIST guidance perspective and in the policy space as well.
  - NIST series of resources
    - He or Jeff will send these out to everyone.
    - Not a well-known series: NISTIR 8286, Integrating Cybersecurity and Enterprise Risk Management (ERM)
      - Four documents that focus on different dimensions of helping to communicate cybersecurity risk in the context of enterprise risk.
    - They focus on identifying and estimating cybersecurity risk in the context of ERM, prioritizing cybersecurity risk for ERM, staging for ERM and governance oversight, and using business impact analysis to inform risk prioritization and response.
    - It's about taking that cybersecurity risk information and putting it in a better context so that it can be viewed alongside of the other types in a way that's going to be more meaningful to a decision maker.
    - Developed with a cyber ERM community of interest across the entire USG.
      - Led by other agencies and NIST was invited to participate.
      - Had very fruitful and ongoing discussions
    - Not a silver bullet but it starts to get at the heart of that communication divide and gap.
- Mr. Groman – Commented that it’s not just communicating cybersecurity issues, it’s about being able to prioritize them, especially when there are 100 of them all at a number one priority.
  - Mr. Stine – Agreed and mentioned that one of the volumes focuses on how to present that prioritization.

Cybersecurity Framework (CSF) 2.0 Updates

- Some of this was covered in Jim St. Pierre’s slides. Will add a little detail on a couple of things.
  - Since the last board meeting, NIST issued a discussion draft of the CSF 2.0 core.
    - The framework has a little bit of narrative in the front and the back.
    - In the middle is the meat of the framework
    - What most people think about as the framework is the framework core,
      - The collection of outcomes that are anchored in the five functions: identify, protect, detect, respond, and recover.
  - They’ve gotten a lot of feedback already through multiple RFIs, and through a lot of in-person and virtual workshops that NIST hosted, as well as a lot of industry or different association hosted events.
    - First opportunity to put something out that folks could look at react to
    - Continuing to get feedback.
    - In the process of reviewing and adjudicating the feedback and making decisions on how to address those in the core and the narrative.
    - The official public draft of the core will go out soon.
  - They are broadening the focus of applicability beyond just critical infrastructure.
    - The originating executive order was very specific to critical infrastructure.
The adoption of the CSF has been much broader than that, not just domestically but internationally.

A lot of the public feedback indicated that the distinction between critical and non in the context of the Cybersecurity Framework is just not as important anymore so we're removing that specific distinction.

- We are adding a govern function similar to the privacy framework govern function and the AI risk management framework govern function.
  - There were already govern categories and subcategories and content in the previous version of the cybersecurity framework.
  - Elevating that to a function level puts a bright light on the importance of governance to help your cybersecurity program and the integration with the broader enterprise risk decision making processes and objectives.
  - Having the risk appetite and risk tolerance is defined by the organization to inform, influence, and guide all the other cybersecurity priorities that you have.
  - Elevating governance at that level is key.
  - Some of that governance function will be pulling existing content from the framework and putting it in a new place and some will be some new content based on our own research and the input they received.

- Integrated supply chain risk management into the framework core in the last version.
  - The NIST research program and inputs from the broader community have helped to inform the framework.
  - Use the framework as the “docking station” to tee up supply chain and then point to other standards, guides, and practices that are out there and draw more attention to supply chain and the importance of that.
  - Adding an implementation examples column to the framework and informative references, their standards, guides, and practices,
    - Working toward fleshing out some implementation examples to help guide folks’ thinking,
    - Still a design decision on whether those are going to be within the core or a complimentary resource.

- Anticipate releasing the draft core late summer 2023.
- Looking forward to feedback on that complete draft
- Also looking at the application of the cybersecurity framework to other domains
  - How to take that framework and customize or tailor it in the context of a mission objective,
  - We have different subsidiary framework profiles.
    - One is a cybersecurity framework profile for protecting genomic data.
    - Second is cybersecurity framework profile for hybrid satellite networks.
      - Satellite and satellite systems can exist with multiple different organizations and parties within the same technical environment.
      - Example: a satellite that will go on a rocket that has a different owner from the satellite. That rocket will use a launch facility that neither the rocket nor the satellite owns. You might have instrumentation on your satellite that belongs to somebody else who's leasing that for their own scientific purposes. So often, these hybrid satellites have multiple mission owners and activities.
      - It's an examination of how to manage and work with that type of hybrid environment.
• **Mr. Groman** – Added that it should also cover how to apply privacy in a hybrid satellite framework, where multiple entities are collecting data on one satellite for multiple different uses, both commercial and government.
  - **Mr. Stine** – Replied that they’re working towards that in the genomic space, because there are some unique privacy challenges there.
    - Naomi and the team are consulting and involved in that process as well. So, it's a good opportunity.
    - Current scope is on the cybersecurity of genomic data,
      - There's a good opportunity for us to make it cybersecurity and privacy of genomic data and apply more of our resources, including the privacy framework in that context.
  - **Mr. Scholl** – Agreed with Mr. Groman. They didn't do that in the hybrid satellite. They will go back and look at that through the privacy framework lens as well.
    - Third, in collaboration with Department of Energy, for liquefied natural gas.
      - This was a great cross agency collaboration.
      - Looks at the movement of liquefied natural gas, from port to point of destination and everything in between, and understanding the cybersecurity concerns, considerations, and potential ways to mitigate those risks in that context.

**The End of DES**

- DES is being deprecated for new encryption going forward.
  - These next couple of years are going to be somewhat disruptive with a lot of cryptographic changes that are going to be occurring in NIST standards and international standards, and then flowing into our technologies.
  - Would like feedback about the synchronization, the impact, and how NIST, in bringing new things in and deprecating things out, can do this in a way that is effective and efficient for those who have to implement them.
- Still have the Advanced Encryption Standard and AES block cipher, but we're receiving input and feedbacks that some of those implementations are brittle and misuse prone.
  - For example, there's some modes of operations that are not easy to do and when they're not done properly, they fail poorly.
  - Looking to bring in better and different misuse resistance modes of operation as another potential change for the future.

**Quantum Algorithms**

- Wrapping up the first set of standards and in our technical documents and submitting them for the Federal Register review.
- The ER hash team and some of the other folks on the PQC team said Sphincs+ is in very good shape.
- Might be able to get that out at the same time as CRYSTALS-Kyber and CRYSTALS-Dilithium.
  - Falcon will be standardized after we get these first three out.

**Other Standards Work**
Tomorrow we will have a presentation about privacy enhancing technologies (PET) such as zero knowledge proofs, multi-party computation, and homomorphic applications possibly using our current suite of encryption,
  o May need to have new and different ones brought in to maximize the efficiency and security of those application spaces.
  o In the next couple of years, we anticipate having significant changes in the suite of encryption algorithms that the US government will be standardizing, calling for, and asking industry to build for us so that we can bring them into our infrastructure.

Cybersecurity Maturity Model Certification (CMMC)

CMMC was a DoD program for providing or requiring security of DOD suppliers.
  o Uses 800-171 as one of the core documents that DOD suppliers would use.
    ▪ So we recently did an update to that document. There's a new rev 3 that is open for public comment.
      - That public comment closes next week.
    ▪ Working on harmonizing it with the controls that were updated in the latest revision of 800-53 so they work better together.
      - Poses challenges because there's a lot of flexibility in risk management decisions and organizational defined parameters.

NIST SP 800-63 Updates

Issued a draft for public comments in January. Comment period closed in mid-April.
This is a heavyweight document with multiple volumes corresponding to different parts of the digital identity lifecycle,
About 130 organizations submitted close to 3500 different comments
  o There are still some tricky issues that we're trying to navigate.
    ▪ One of those is providing more guidance on non-biometric options or non-biometric alternatives for identity proofing at higher levels of assurance.
    ▪ That's something that it's both a guidance challenge and research challenge.
  o Working on adjudicating the comments that we've received,
  o Part of our approach for stakeholder engagement is not just public comment periods, but a lot of workshops and other events.
    ▪ Have some hybrid workshops coming up July 25, and 26th.
      - Day one is open to the public. Day two is a fed only event.
      - Will be providing an update on where we are with respect to the digital identity guidelines, sharing some of the major themes that we've heard through the public comment process, and then discuss, at a high level, our plans for how we're going to substantively address a lot of feedback that we received.

Identity and Access Management Roadmap

Directed through the CHIPS and Science Act and the identity provisions within the science portion of that act.
  o Have issued a roadmap in the past and this was a good opportunity for us to signal activities that we have currently underway today with respect to identity and access management.
Over the next 1-5 years, some of the areas that we're going to continue to look at include continued efforts around PIV modernization, broader multifactor authentication activities, and research standardization and practical application examples around the use of mobile driver's license and other digital credentials.

Discussion

- **Mr. Groman** – Mentioned that it seems that NISTIR 8286, and what's in there, is what was missing from the NASA presentation. It appears to be a great document, notwithstanding the lead author is Kevin Stine, but it hits what we're talking about. Cybersecurity risk has been one element of overall enterprise risk, not doing your mission is another risk and they're all points that must be assessed together with all the other risks. So perhaps that document would be helpful there.

  - **Kevin Stine** – Replied that it doesn't get a lot of play. There are things we can do and opportunities we have to amplify that even more and maybe elevate it to an SP where it will get a lot more attention. The exciting part about that one is the cyber ERM community of interest, which are the practitioners across the USG. There are 100 agencies that have participation. It's one of the more vibrant grounds up federal community efforts that started as a broader ERM community. That group of ERM professionals concluded that we need to have cyber people involved.

    - That's an area where we have even more opportunity with the Cybersecurity Framework.
      - The value proposition is helping to address the communication gap or divide between cybersecurity and non-cybersecurity communities.
        - Across technology domains, Mission domains, and nations.
        - Seen significant international uptake.
      - There were a lot of companies that stated IT folks and OT folks speak different languages. But the outcomes and the way they're expressed in the cybersecurity framework can resonate with both communities.

NICE Updates

- Formerly known as National Initiative for Cybersecurity Education
  - Now it just goes by NICE.
- There’s a Notice of Funding Opportunity that went out within the last several weeks.
  - It’s for regional alliances and multistakeholder partnerships (RAMPS) to stimulate cybersecurity education and workforce.
    - Piloted this on a much smaller scale back in 2016.
      - Issued five RAMPS grants at about $200,000 each back in 2016.
      - It was very successful.
      - A couple of years ago, parts of Congress put it in NDAA.
        - Started to get funding last year to support that.
  - Will not issue any this fiscal year, but the opportunity is out there, and applications are due by August 7.
    - Expect first round of awards by the end of the calendar year.
  - RAMPS is a regional, collaboration of local businesses, local school districts, local employers, local associations and pulling those parts of the community together to understand the local cybersecurity education and workforce needs.
Funding, in many cases, comes with matching funding from other organizations at a local level to help build that local cybersecurity workforce supply to help address the local workforce demand.

- Issued some reports in the past on the pilots that we did several years ago.
- Anticipate this time around 15 to 20, awards around that $200,000.
  - It’s a small amount of funding in the grand scheme of things, but we think it'll provide some value for a lot of localities.

- Continuing to support the US Cyber Games and specifically the US cyber team.
  - It's growing in interest and sponsorship from other companies and agencies across the US.
  - The International cybersecurity competition last year was held in Greece. This year it's going to be held in the US in San Diego, August 1-4
  - Funded in part by NIST through the NICE program.
  - National teams from all over the world are coming together to compete in a variety of different challenges with respect to cybersecurity, similar to an Olympics model.

Research Areas

- Continue to look at research areas of future interest in cybersecurity.
  - Space
  - New areas of communities that are looking to us for cybersecurity assistance, such as:
    - High performance computer platforms,
    - Access control technologies for next generation interface
    - Wearables and voice for when eventually we get away from keyboard and PIV.

- Continuing to look at how we can automate and leverage technical capabilities around our conformance programs, especially when it comes to assuring the implementation of this new cryptography, so it's done correctly as we bring it into the federal infrastructure.
  - Continues to be a challenge area for us as we do these transitions, because transitions result in large volumes of new products, which have to be serviced by our conformance programs.

Day Review and Meeting Recessed

- Mr. Lipner – Called for feedback and thoughts from the Board regarding letters or guidance or wait until the end of the meetings on Thursday.
  - No proposals were made.

The Chair adjourned the meeting at 3:30 P.M. ET.
Thursday, July 13, 2023

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

**AI/ML and Security and Privacy**

Dr. Dewey Murdick, Executive Director of Center for Security and Emerging Technology (CSET)

Georgetown University

**Introduction to CSET**

- Over 60 staff
  - including 20 junior analysts
  - research led by 15 fellows drawn from government, military, intelligence community, industry, law, and academia.
  - Plus, ~20 students, ~10 affiliates

- Staff Capability
  - Policy analysts (AI, biotech, computing, economics, intelligence, IP, law), data scientists, software engineers, linguists, survey specialists, etc.; supported by editors, designers, external affairs, operations, distinguished fellows, and leadership.

**Map of Science Growth Forecast**

- Collects and organizes world research literature.
- Convergence between sectors
  - Medical imaging, manufacturing, energy research
  - Research clusters are groups of papers that cite each other.
- One statistic shown for each cluster is the percentage of AI and AI subfield relevance.
- Slides showed examples of 3 year growth forecast for medicine and business.
  - [https://sciencemap.eto.tech/?NP=100%2C13737&ai_pred=10%2C100&industry_share=1%2C67&frac_papers_cited=2%2C35&all_subjects=General%3A+business&mode=list&cols=cluster_id%Cset_extracted_phrase%2Cclass_arts%2Cai_pred%2Cro_pred%2Ccv_pred%2Cnlp_pred%2Cfrac_papers_cited%2Cindustry_share](https://sciencemap.eto.tech/?NP=100%2C13737&ai_pred=10%2C100&industry_share=1%2C67&frac_papers_cited=2%2C35&all_subjects=General%3A+business&mode=list&cols=cluster_id%Cset_extracted_phrase%2Cclass_arts%2Cai_pred%2Cro_pred%2Ccv_pred%2Cnlp_pred%2Cfrac_papers_cited%2Cindustry_share)

**Convergence Between AI and Other Sectors from Medical Imaging to Manufacturing**

- Have witnessed rapid AI advancements, and a convergence between AI and other sectors promises wide-spread innovation in areas from medical imaging to manufacturing.
  - Fostering AI literacy across the population is critical for economic competitiveness.
  - It is essential to democratic governance.
  - Cannot engage in meaningful debate about AI if we don’t know enough about it.
- This means an increasingly large fraction of U.S. citizens will encounter AI daily — we need skilled people working at all levels.
  - Need innovators from technical and nontechnical backgrounds.
  - Need to attract and retain more diverse talent from across our nation and internationally.
  - Separate from those who are building AI systems, need comprehensive AI training for the general population (K-12 curricula, certifications) — AI literacy is key.
- Presented two slides that show projected growth of AI in medicine over the next 3 years.

**The AI Triad – Powered by Human Talent**
“Machine learning systems use computing power to execute algorithms that learn from data” – Ben Buchannan

AI Triad consists of Data, Algorithms, and Computing Power
- Analysis of risk and threats

AI Talent Statistics
- 2019 – U.S. AI Workforce consisted of about 9% of employees
- The AI Workforce is Technical and non-Technical.
  - Technical and non-technical roles and responsibilities are included in the design, development, and deployment of AI.
  - That means training the AI workforce must involve education spanning all roles to ensure the safe, responsible, and effective deployment of AI.
- The AI Workforce is Geographically Concentrated.
  - The AI workforce is geographically concentrated, especially technical talent.
  - CSET finds clusters of technical talent across major metro areas, with key areas including known tech hubs and Washington, DC.
    - About 20% of total employment for all AI occupations are concentrated in 5 cities: New York City, Chicago, Washington, D.C., Los Angeles, and San Francisco
- AI and AI-related Certifications Have Limited Value—Buyers Beware.
  - A maze of unaccredited certifications are currently offered online.
  - CSET finds most employers do not use certifications as a basis for hiring.
  - Federal standards are needed to distinguish quality among the certifications.
- Talent Shortages Vary by Occupation.
  - Blanket claims of AI talent shortages are not accurate, which could negatively impact needed investment in policies and programs.
  - The biggest shortage is in top tier technical talent, such as PhD computer scientists.
  - Creating viable alternative pathways into technical fields outside of a four-year degree would expand and diversify the technical workforce to relieve additional strain.
    - for example, top tier technical talent (PhDs) are in short supply relative to demand while evidence is mixed for software engineers and data scientists.
    - Diversity and getting folks to complete training are significant issues.

Peer Innovators, Competition, Alliances, and a Long-term Wrestling Match
- U.S. AI Education Risks Lagging China
  - China exceeds the US in both scale and scope of AI education with curricula for all levels.
  - China’s STEM doctorates production is projected to greatly increase.
  - If international students are excluded from the U.S. count, Chinese STEM PhD graduates would outnumber their U.S. counterparts more than three-to-one.

AI-enabled Disinformation Campaigns
- These disinformation campaigns enable:
  - Precise targeting of intended audiences that identify societal fissures, determining sentiment, etc.
  - Development of more realistic (harder to trace) personas & pages with ML-generated images, text generation, etc.
  - Accelerated content generation at scale with large language models.
    - See https://cset.georgetown.edu/publication/truth-lies-and-automation/
  - Boost trolling and online chaos with more capable chatbots.
Importance of Human-machine Teaming

• Human-AI Teaming: helps answer:
  o Do humans feel that they can rely on the AI system consistently in required tasks?
  o Has confidence in the AI system grown over time due to its steady performance?
  o Is this confidence well founded (calibrated)? In what areas?
  o Can humans rely on the AI system to provide the same level of performance on similar tasks in a variety of circumstances?
  o Does the AI system provide clear explanations for its actions or decisions and do humans know how to use it effectively?
  o Is the AI system indicating an accurate level of uncertainty involved in its recommendations or actions?
  o Has the AI system contributed to an increase in productivity or improvement in work quality?
  o Are tasks being completed more efficiently since the deployment of the AI system?

• AI-Assisted Human Learning
  o How effectively is the AI system facilitating the learning process for team members?
  o Are the results or outputs improved or expedited due to the AI system?

• There is a need for qualifications training.
  o Does it meet the needs?

• NIST has a challenge with regard to AI and trustworthiness.
  o Humans trusting AI too much or too little.
  o Need quality training.

Global Partnership on AI (GPAI) Data Governance Working Group

• While seeking to address the UN Sustainable Development Goals, the Working Group aims:
  o To collate evidence, shape research, undertake applied AI projects and provide expertise on data governance,
  o To promote data for AI being collected, used, shared, archived, and deleted in ways that are consistent with human rights, inclusion, diversity, innovation, economic growth, and societal benefit.

• Data governance practice that
  o Contributes to justice and genuine respect for people in the way that makes people and groups visible, represented, and empowered as beneficiaries in the collection and use of data for the development of AI systems.
  o Widens the lens beyond a narrow view focused on compliance and individualized privacy and accounts for collective identities and community-level decision making.
    ▪ Privacy with authority to use data.
  o Seeks out and engages with a full set of impacted stakeholders in the design, development, and deployment of AI systems and agilely adapts when new stakeholder perspectives are discovered.

Applying Cybersecurity Lessons to Securing AI

• Defend AI systems against malicious actors seeking to subvert a system or steal the underlying model or its associated data.
• Secure AI ≠ Safe (Trustworthy) AI but reduces the chance AI systems will be deliberately misused for harm.
• Relevant Lessons from Cybersecurity
Begin now to protect data sets, trained models, and open-source libraries.
Confidentiality and integrity of models and data will become increasingly important over time.

- **Threats**
  - Recognize sensitivity of model parameter weights which can be accessed through open source sharing, stolen, or inferred.
  - Understand potential of model stealing via distillation attacks.
  - Protect against adversarial attacks.
  - Prep for downstream attacks arising as developers build integrated plug-ins.

- **Security measures**
  - Limit access to sensitive models through APIs and data confidentiality measures
  - Apply traditional network security measures (e.g., firewalls, access controls)

### Balancing Goals-in-tension Across Society

- In the face of a technology-enabled soft/hard power and a clash of values, how do we:
  - Enable the public & private tech innovation ecosystem to “run faster” and help solve pressing problems and create jobs?
  - Slow unwanted technology transfer and protect key enabling technology?
  - Ensure AI systems (etc.) are safe and operate in harmony with our best values?

- **Actionable levers of power for tech-policy**
  - Identify relevant “levers” that are operated within a decentralized, international & locally-informed system to achieve meaningful goals (almost always in tension)

### Short Term Actions

- **Talent**
  - Basic AI Literacy & K-12 Education
  - Community College & Certification
  - STEM Education
  - Diversity is a National Security Asset
  - High Skilled Immigration

- **Information Gathering (and engage the democratic process)**
  - Track AI harms via incident reporting
  - Learn how to request key model and training data used in important applications.
  - Encourage the development of the third-party auditing and red teaming ecosystem.

- **Development**
  - Measure and metric development and implementation, including human-machine teaming.
  - Improve the quality of shared resources, such as open-source training and pretrained models that form the backbone of many of today’s AI systems.

### Long Term Actions

- An expansion of U.S. analytic capacity via the Office of Global Competition Analysis, or other models, have been proposed by the House and Senate and could contribute here.
- We need to keep a close eye on our policies, each implementation needs an effective monitoring system.
- Rethink software deployment model (“run fast break things” → clinical trials)
Unlike with food, drugs, or finance, software is often released without thorough testing — this needs to change.

There is a spectrum ranging from our current approach to more rigorous testing procedures, such as those used in clinical trials.

- We need to think about where we should be on that scale, but right now we’re at one extreme end.
- We need to make changes over time to the rules about who is responsible when things go wrong with software, especially those end-user license agreements that let the companies providing the service off the hook for any or all problems.

- If we license or register AI software (a common proposal) or make sure it’s used safely, we will need to update the authorities for existing agencies — and perhaps create a new one that could:
  - Check how AI is being used in and overseen by existing agencies.
  - Be the first to deal with problems, directing those in need to the right solutions.
  - Fill gaps that existing sector-specific agencies don’t cover.
  - Work closely with NIST and industry to identify and update evaluation standards.

Discussion

- Mr. Gantman – Asked what the main take-a-ways are.
  - Mr. Murdick – Replied: 1) People matter. Need skilled people. 2) Accurate thinking about metrics and 3) how to approach qualifications of users. Culture – there is an opportunity to think about how to qualify folks on different systems. Maybe apply secure software development framework to secure AI.

- Ms. Fanti – Mentioned that these are challenges regarding testing AI models. You also mentioned standardizing this.
  - Mr. Murdick – It’s hard to evaluate systems for all cases. It’s expensive. There are opportunities for dialog. It’s difficult to pinpoint the cause of problems. There is some exciting research in this area.

JCDC and DHS Secure-by-Design and Default

Emily Paull, Cyber Operations Planner, Future Plans, Joint Cyber Defense Collaborative (JCDC)

Mission

- Joint Cyber Defense Collaborative (JCDC) mission is to unite the global cyber community in the collective defense of cyberspace.
  - It’s a public and private sector partnership of cyber defenders from organizations worldwide.
  - Leader in integrated public-private sector cyber defense planning, cybersecurity information fusion, and dissemination of cyber defense guidance.

Strategic Goals FY23-26

- Secure by design
  - CISA-wide initiative
  - Shift the balance of burden to developers.
    - Need to design secure features from the beginning.
    - Information sharing as default.
• Responsibility sharing
  • Security is at the core of product design.
    - Default – secure out of the box, no configuration needed. For example; Default MFA.
    - Memory safe languages
    - Stored procedures
    - Code reviews
    - No default passwords
  o Harness the Collaborative’s expertise and influence to address the most pressing systemic risks to the security and resilience of cyberspace such as unsafe technology and unsustainable security.
• Fight as one
  o Drive national unity and operational vigilance in cyber defense during both crisis and steady-state conditions.
• Optimize the Organization
  o Mature organizational operations and foster the inclusive culture needed to flourish.

JCDC Successes

• Log4Shell
• Support to Albania’s CERT

2023 JCDC Planning Agenda

• Remote monitoring and management (RMM) Vendors
  o Working with RMM vendors to improve the cybersecurity of SMBs, Critical Infrastructure operators, and SLTT entities at scale.
• Open-source software (OSS)
  o Improving the awareness, quality, and security of OSS used in critical infrastructure industrial control systems (ICS).
  o Developing a plan
    ▪ Held seven meetings.
    ▪ Creating a fact sheet
  o Relative to SSDF and EO
    ▪ There is very much a question of incentives to adopt these principles.
    ▪ CISA is the cybersecurity and infrastructure security agency.
      - They will be pushing out JCDC guidance as another part of the cybersecurity community.
      - This is reinforcing a message that is already out there.
      - Looking for ISPAB guidance.
• National Cyber Incident Response Plan (NCIRP) Refresh
  o Evolving and clarifying national cyber defense and incident response stakeholder roles and responsibilities.
• High-risk populations
  o Strengthening protection of civil society organizations and individuals at higher risk of being targeted by state actors.
• Water sector edge devices
  o Securing the deployment of IoT edge devices in the water sector.
• Energy sector operational collaboration
Advancing security of the energy sector by identifying cybersecurity supply chain vulnerabilities, convening stakeholders to identify areas of national security risk, and creating pathways for mitigation.

- https://www.cisa.gov/2023-jcdc-planning-agenda

- Quote from JCDC Director Jen Easterly – “Consumer safety must be front and center in all phases of the technology product lifecycle – with security designed in from the beginning.”

- Contact information:
  Emily Paull
  Planning Office
  Joint Cyber Defense Collaborative
  emily.paull@cisadhs.gov
  202-286-2133

Discussion

- **Mr. Gantman** – Great overarching philosophy. Asked about ways we can move forward.
  - **Ms. Paull** – Replied that it’s important to work toward building tools to secure software. They are building private sector partnerships to tackle difficult conversations and make sure we have safe technology.

- **Mr. Gantman and Ms. Moussouris** brought up questions around how success will be measured.
  - **Ms. Paull** – Replied that those are good questions. The average consumer doesn’t understand cybersecurity and how to secure code. She acknowledged that she doesn’t have hard numbers, but the broader point is that these principles have an impact for ordinary consumers.

- **Ms. Moussouris** – Asked what are the enforcement measures there are for organizations who don’t meet the requirements and what agencies might be involved with enforcing secure-by-design?
  - **Ms. Paull** – Replied that they are working in voluntary, non-regulatory partnerships to try and understand what makes sense for industry to implement. This is a “grassroots” effort to adopt these principles and communicate the importance of them for our national security.

- **Mr. Lipner** – Asked a question about getting code changed in OSS.
  - **Ms. Paull** – Indicated that she’s not on the team that runs the OSS initiative, but she can take this question to them and get back to him.

Software Attestation

Mitch Herckis, Office of Federal CIO, OMB
Yejin Jang, Office of Federal CIO, OMB
Jeremy McCrary, Office of Federal Procurement Policy, OMB

Secure Software Development Framework

- Executive Order 14028 highlighted the need to grow our ability to enhance the security of software development and ensure the federal government is leveraging secure software.
- Recently published guidance on this topic, including guidance on section 4 of the EO.
  - Secure software development framework (SSDF)
    - Federal government uses software produced by non-governmental organizations.
    - Need to ensure that software contains certain elements.
  - They wanted to identify minimum requirements for the federal government environment.
Identifying Requirements

- Working with agencies, outside experts, etc. over a period of time
- Want to make it accessible and understandable for all companies/organizations.
  - Received lots of feedback on items that didn’t seem very actionable.
    - Software producers had questions about the requirements, who is attesting…
  - Spent much time in public engagements with industry agencies.
  - Led to issuance of M-23-16 update (6/9/2023) of M-22-18
    - Gave more time for agencies to collect attestations from software producers.
    - Provides supplemental guidance on the scope of M-22-18’s requirements.
    - Provides further detail on how agencies should think about software in their environment that may not meet the standard. How they can keep that software. What the software producer can do to “get in line”.

Changing the Timeline

- Agencies must collect attestations for critical software no later than three months after the common form is approved by OMB.
- Six months after the common form’s approval, agencies must collect attestations for all software subject to M-22-18 requirements.
- Does not apply to all software in the environment, only specific software that has been introduced to the environment since the issuance of M-22-18 (after 9/14/2022).
  - Software that has had a major version update since 9/14/2022.
  - Software that is a continuous delivery type

Attestations – Scope

- Many of the requirements address the need to adhere to the latest software development practices needed to assure the security of those products.
- Asking software producers to follow processes that are shown to reduce risk.
  - Understand that OSS often has many authors and, if incorporating that code, they are not being held responsible for attesting to that code’s security as they may not know where it comes from
    - They are being held responsible for minimizing the risks of introducing that code.
    - They are responsible for OSS they build.
- Agency developed software.
  - Became more of an issue because of attestation.
  - If software is built by federal contractors, is this considered outside software that needs to have an attestation?
  - Discussed these questions with agencies and OMB.
    - Agency developed software requires an agency to have oversight and control over the development process.
    - In the case of confusion or uncertainty, the agency CIO should make final determination if it is agency developed or not.

Pathway for Software Already in Use
• The agency needs to engage with the producer and ask them:
  o To identify the practices to which they can’t attest.
  o Document practices they have in place to mitigate associated risks.
  o Submit a POA&M to “get it right.”
• Agency determines if the data is sufficient or not.
  o If sufficient, the agency submits an extension request to OMB.
• Also creating an opportunity to talk across the agencies and coordinate on software used by multiple agencies.

Paperwork Reduction Act
• Going through the paperwork reduction act process around secure software on a standardized form
  o Can be found on CISA’s website.
    ▪ Currently adjudicating comments
    ▪ This is an opportunity for the first generation of the common form to be as solid and helpful as possible and to make the processes as efficient as possible.

Federal Procurement Policy
• Office of Federal Procurement Policy (OFPP) is part of OMB.
• Mr. Gantman asked how we measure effectiveness once everyone complies? Will there be some kind of internal analysis?
  o Mr. Herckis replied that is difficult to answer. It gives us a baseline and visibility to start understanding what works. Over time, requirements may change. Right now, it’s a first step.
    ▪ Gives visibility into the security practices of the software producers that we haven’t had before.
    ▪ This is a foundational start.
    ▪ There is security value in discussions with software producers who feel that the EO started processes that started them thinking about these things.
      - Documenting
      - Sharing information on gaps
      - If the SSDF wasn’t being met in some way
    ▪ Having the requirements and the SSDF guide together goes beyond what they would be separately.
• Mr. Gantman asked about what happens to the attestations? There is an assumption that someone reads them and has the ability to take some action.
  o Mr. Herckis replied that they may have a third-party that evaluates the attestations to determine if the organization meets the requirements.
    ▪ The extensions may be a little harder.
    ▪ Over the long term, we should expect people are doing their due diligence.
• Mr. Lipner commented that there is an implied threat if they aren’t doing this. Are there penalties?
  o Mr. Herckis replied that this isn’t a procurement act. It’s about how agencies determine security and alignment with tools.
    ▪ There’s language that makes it clear that this is based on them making a good faith effort to doing the right thing.
    ▪ Makes it harder to lie to the USG and increases the possibility of repercussions.
• Mr. Lipner asked about the omission of some important SSDF requirements, such as root cause analysis of reported vulnerabilities, from the draft attestation form.
o Mr. Herckis stated that the form was intended to be an initial set of requirements that would be reasonably achievable by vendors.

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

Update on NIST Privacy Engineering Program and Privacy Enhancing Technologies (PETS)
Naomi Lefkowitz, NIST Privacy Engineering Lead
Angela Robinson, NIST Cryptographic Engineer

Privacy Framework
- Released in January 2020
- 124,000 total downloads
- USA, Canada, U.K., India, Australia, Brazil, Germany, Netherlands, Japan, China
  o Did a crosswalk with the Brazilian data protection law.
- Working on doing a better job of tracking analytics and providing more resources.
- Top resources
  o PF/CSF Crosswalk
  o PF/GDPR Crosswalk
  o PF/ISO/IEC 27701 Crosswalk
- Working on collecting and providing resources to help with implementation.
- Continuing to receive positive feedback.

NIST Privacy Workforce Public Working Group (PWWG)
- Over 900 members worldwide
- Currently drafting content for NIST Privacy Workforce Taxonomy
- To date, we have completed over 700 Task, Knowledge, and Skill (TKS) Statements aligned with NIST Privacy Framework Categories, including completing work on our Identify-P Function.
- We’ve implemented a workplan for 2023 with the goal of wrapping up our TKS Statement development by the end of the year.
- Our 3 active Project Teams are creating material for the Risk Management Strategy (GV.RM-P), Awareness and Training (GV.AT-P), and Data Processing Management (CT.DM-P) Categories.
- These current Project Teams will complete their work around the end of next month, at which point we will spin up the final 3 Project Teams.
- The final 3 Project Teams will create TKS Statements for the remaining Categories in our Control-P and Communicate-Functions.
- Integrating Privacy Guidance
  o Draft SP 800-60, Revision 2, Guide for Mapping Types of Information and Systems to Security Categories
    ▪ See this as a way to update PII, which wasn’t consistently addressed in 800-60
    ▪ Taking best content from 800-122 on the concept of confidentiality for PII
    ▪ Looking to retire 800-122
    ▪ Collaborating with the FISMA team
    ▪ Hopefully have a draft out for comments this summer.
  o Draft SP 800-50, Revision 1, Building a Cybersecurity and Privacy Learning Program
    ▪ Being updated by the NICE team
In line with the update to OMB circular 130 that calls for a privacy awareness program
  o Draft SP 800-63-4, Digital Identity Guidelines
    ▪ Integrating privacy
  o Final NCCoE Practice Guide, SP 1800-22, Mobile Device Security: Bring Your Own Device will be published in August.
    ▪ Integrated privacy risk assessment methodology and privacy framework to help support privacy concerns about mobile devices.
  • Co-sponsors of the US-UK PETs Prize Challenges 2023
    o Initially announced at the first Summit for Democracy in December 2021
    o Inspire innovators to build solutions that enable collaborative development of AI models while keeping sensitive information private.
    o Winners were announced at the second Summit for Democracy on March 30, 2023.
    o Focused on privacy preserving federated learning models that track:
      ▪ Financial crime.
        - Task: Develop privacy-preserving federated learning solution to detect potentially anomalous payments
        - Given:
          • Transaction information
          • Bank account flags
        - Predict:
          • Probability of transaction being fraudulent
      ▪ Public Health
        - Task: Develop privacy-preserving federated learning solution to forecast an individual’s risk of infection
        - Given:
          • Demographic information + location/activity
          • Population Contact Network (up to time $t$)
          • Infection status (up to time $t-7$ days)
        - Predict:
          • Probability of individual $x$ being infected at time $t$
    o Had two synthetic datasets for the challenge.
      ▪ Used sensitive information.
    o Centralized learning
      ▪ Participants send data to aggregator, who trains the model.
      ▪ Privacy vulnerability: Revealing training data.
    o Federated Learning
      ▪ Participants send model updates instead of data.
      ▪ Privacy vulnerability: Still reveals training data.
      ▪ Research shows that models can still be attacked to reconstruct or reveal the training data underneath.
    o Privacy-Enhancing Technologies for Federated Learning
      ▪ Input Privacy – Hides model updates during training.
      ▪ Output Privacy – Prevent privacy attacks on training models.
      ▪ Challenge goal: drive development of practical PETs for federated learning
      ▪ Teams were to combine different types of technology to see if they could prevent those attacks.
- Used a combination of fully homomorphic encryption (FHE) and secure multi-party computation (SMPC) on the input side and differential privacy (DP) on the output side.
  - 6 Teams on the US side
  - Their solutions are open source and they are in the NIST privacy engineering collaboration space
  - Collaborative Research Cycle – a community challenge to evaluate de-identification algorithms.
    - NIST released ‘Diverse Communities Excerpt Data.’
    - Research community submits de-identified instances.
    - > 320 submissions using many types of techniques (e.g., differential privacy, synthetic data, statistical disclosure limitation)
      - Run their algorithm against the diverse algorithm excerpt data that NIST created.
      - They submit their results to NIST.
      - NIST evaluates deidentified data quality and releases the data and reports for research.
  - Hosting a workshop in November for research results
  - Trying to understand what metrics are needed to improve the quality and people can begin to understand what is important.
  - Big focus for the prize challenge is increasing adoption.
    - Part of that is trust.

- Next steps
  - Intend to finalize and publish the PWWG work in early 2024 following a public comment period.
  - Some stakeholders have expressed interest in continuing the PWWG into 2024 to create privacy work roles and competencies. Later this year, we will explore this possibility with our membership in more depth to decide on next steps.
  - Identify and support PET pilots.
  - Update SP 800-30, Guide for Conducting Risk Assessments, to include privacy risk assessments.

**Updated on Privacy Enhancing Technologies**

- Privacy-enhancing technologies (PETs) enable utility/power of private data without
  - disclosing the underlying data
  - risking deanonymization of underlying data owners
- General categories
  - Data masking approaches
  - Cryptographic approaches
  - Access control techniques

**Privacy-Enhancing Cryptography (PEC) Project**

- Goal: accompany the progress of emerging technologies in the area of PEC and promote the use of cryptographic protocols that facilitate privacy goals
- Tools
  - Zero-knowledge proofs (ZKP)
  - Secure multiparty computation (SMPC)
  - Fully homomorphic encryption (FHE), private set intersection (PSI), etc.
- Developing reference material
- Doing preliminary work on evaluating the potential for standardization of PEC tools
  - Not standardizing yet
  - In general, it’s not a one-size-fits-all.
Special Topics on Privacy and Public Auditability (STPPA)

- Virtual seminar series that focuses on various PEC tools initiated in January 2020
  - Using these to gather reference material.
- Features presentations by SMEs and panel discussions.
- STPPA #6
  - Focus: Community efforts on various advanced cryptography techniques (ZKP, MPC, FHE, ABE)
    - ZKProof.org
    - HomomorphicEncryption.org
    - MPCAlliance
    - ETSI on development of ABE standards
    - ISO on development FHE standards
  - Scheduled for July 25, 2023. Event is free, registration required.
    - Grassroots efforts are a combination of industry leaders and academia.
    - All slides and video recordings available at https://csrc.nist.gov/Projects/pec/stppa
- Collaboration with ZKProof
  - ZKProof: “an open industry/academia initiative to mainstream ZKP cryptography.”
  - Annual workshops, with state-of-the-art proposals and presentations
    - Various talks from NIST-PEC
    - Working groups (developing standardization proposal).
  - NIST-PEC collaboration since 2019, supporting the development of open reference material.
- Distributed trust solves the problem of individual untrustworthiness and trustworthy subsets.
  - Working on a project to find solutions for secure distribution of trust.
  - Call for multi-party threshold schemes, including solutions that use FHE and SMPC
    - Looking for the number of participants (threshold) needed to achieve the goal of the algorithm.
- Summary
  - Pre-NIST standards approach to PETs:
    - Accompany progress and development of PETs.
    - Development of reference material
    - Initial focus on threshold algorithms

Discussion

- Mr. Groman – Asked, for de-identification, do they assess a given methodology such as when to use it and the extent to which the data is no longer linked to reality?
  - Ms. Lefkowitz – replied yes they also look at the accuracy. Do the results deviate significantly from the “truth?”
  - Mr. Groman – mentioned that many of the new laws are referring to de-identification of data. Many entities are struggling with how to demonstrate that.
  - Ms. Lefkowitz – added that there’s no one thing to do and there’s no “perfect” privacy. Rely on a “reasonableness” measure. Organizations can increase their adoption of PETs.
- Ms. Fanti – Mentioned that, essentially, de-identified data isn’t really de-identified. What are the metrics?
  - Ms. Lefkowitz – Anyone can submit an algorithm. Looking at one data set for comparison is part of the community challenge to better understand what metrics we should be applying.
• **Mr. Groman** – What we are experiencing is that legislation doesn’t match technology or reality. In these new laws, state laws and federal laws, (this is actually new to the Colorado law) when conducting mandatory data privacy impact assessments or risk assessments, the requirements that we are assessing the risk for loss of privacy confidentiality. But the assessments require now that companies look at other risks, like a risk to society and also benefits, and weigh benefits to the organization, to society, mission versus the harms and document them.
  o **Ms. Lefkowitz** – replied that we’ve talked about the privacy framework and whether it’s at the individual level or the group level, lots of surveillance can be a problematic data action that can manifest at a societal level.
  o **Mr. Groman** – commented that this often comes up in conversations and is worth further discussion.
    ▪ There have been discussions on Capitol Hill that this technology is undermining democracy.
    ▪ Thinks this is more of an issue for things like AI.
    ▪ Need a way to have this conversation as we talk more generally about adverse or potential adverse impacts on people and society.
    ▪ May need to be included as updates are made on how to conduct a privacy risk assessment.
  o **Ms. Lefkowitz** – agree. Will keep in mind as they update the privacy risk assessments.

• **Mr. Gantman** – Asked when she thinks the new crypto technology will be safe enough to be used by non-researchers?
  o **Ms. Robinson** – replied that they’re safe but there’s a mapping problem in knowing which solution applies to which problem and a lack of understanding of what the security guarantees are. There are several pilots that are doing great work and several resources as well.
    ▪ Thinks the mapping problem will be solved in 1-2 years.

• **Mr. Gantman** – mentioned that some of the largest aggregators of private data are medical agencies. To what extent do we see them adopting this technology?
  o **Ms. Robinson** – There is an interagency group, the White House OSTP, released a national strategy for privacy preserving data sharing and analytics.

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

**National Cybersecurity Strategy Update**
Nick Leiserson, Assistant National Cyber Director for Policy and Programs at the Office of the National Cyber Director (ONCD)
Drenan Dudley, Assistant National Cyber Director for Budget Review and Assessment (ONCD)

  o The NCSIP was published July 2023

**Structure of the NCSIP**

• There are 6-9 initiatives tied to each strategic objective.
  o Each initiative has a description and references that tie back to the NCS.
Only one agency is responsible for each initiative.

There is a list of folks who have significant equity in that initiative if there are available resources or guidance to the activities in the fiscal year when the activities are expected.

- It is a living document meaning it is iterative and adaptable to changes in the environment and technology.
  - Some plans, as first deliverables, will be updated.

- The way it’s been introduced is there are three big buckets.
  - First, is the plan. What are the activities? What is available through the USG?
  - Second, what do we get back from state, local, tribal, and territorial governments, industry, industry, civil society, academia, and advisory boards around the federal government.
    - Interested in focusing on furtherance of the President's vision.
      - Things the government should be doing.
      - We want to incorporate that into future iterations.
    - The NCS was formed with a wide range of stakeholders.
      - Interesting in hearing from ISPAB and around the country on what other things should be incorporated in future iterations.
  - Third, things are going to change. The technology landscape, the threat landscape, etc. As they change, the strategy and thinking for addressing them will change.
    - New things are always coming over the horizon.
    - The NSCIP needs to change with them.

Walk through one of the initiatives: 1.1.1, Establish an initiative on cyber regulatory harmonization.

- Need to explore ways to set requirements in a harmonized and simple fashion.

- Activities
  - Release a request for information (RFI) from the private sector.
  - Look for areas of contradictory and conflicting regulations.
  - Explore a framework for reciprocity of requirements and sector-specific risks.

- Hoping for better security requirements and compliance
  - Raise the bar for security.
  - Reduce costs on industry by reducing conflicting requirements and recommendations.

- The NCSIP identifies the timeline.
  - Once the RFI is out, they get responses and are able to digest the responses, they can then turn that around and determine the next steps based on feedback.

**General Information**

- This is the first time something like this has been published.
  - There have been other cybersecurity implementation plans but they’re not released/published.
  - Generally used to guide a federal agency’s current activities.

- Looking for this to be a roadmap for stakeholders outside the government
  - Government has known about these strategies for a while. Many of them helped with the development.
  - The government needs to interface with the public as we need their help in completing many of these initiatives. Cooperation is necessary.
  - This isn’t a comprehensive list of all the cybersecurity activities, but it is a list of key activities.

- Will update annually.
- FY25 budget priorities will be informed by the strategy.
• **Mr. Groman** – asked about holding state governments accountable for compliance.
  o **Mr. Leiserson** – Replied that there are a couple of things we can do. First, leverage initiative 3.4.1, Leverage Federal grants to improve infrastructure cybersecurity. The Bipartisan Infrastructure Law is about investing in new infrastructure and the digital ecosystem that supports it. This includes broadband connectivity for rural areas to new roads and bridges. It’s very practical and connected to something they have. The State Department of Transportation is sometimes strapped for resources to navigate the grant process for accessing this. This initiative has been requested to develop a playbook for grants so the US Department of Transportation can pass this to the State Department of Transportation to show how they are incorporating cybersecurity requirements and it’s part of the grant lifecycle. This may include training and providing resources and identifying products to fit their specific context.
  ▪ Another approach is to harmonize regulations, requirements, and compliance processes and activities to be more attractive to states. Work with states to identify equities they need in designing a framework for baseline cybersecurity environment that they would be willing to adopt.
  ▪ Something relevant to our state stakeholders is cybersecurity workforce. Helping to fill in some of those gaps will help.

  o **Mr. Groman** – asked about election security and government critical infrastructure.
  ▪ **Mr. Leiserson** – Replied that election security is not explicitly called out but all of pillar 1 in the strategy is critical infrastructure and elections is a sub-sector of government facilities and critical infrastructure. Also examples of research and development and the prioritization of R&D in cybersecurity, some of which could manifest for elections.

  o **Mr. Gantman** – Commented on the inclusion of section 6.1. Assessing Effectiveness. He is wondering how they will measure the security measures taken. Not really expecting an answer right now.
  ▪ **Mr. Leiserson** – Replied that, this is an iterative process, and the effectiveness will fit in the programmatic support. We want to understand the effect it’s having on the ecosystem. How are we getting to the vision outlined.
    - Looking at how the initiatives are tied directly to a measurable outcome.
    - Following up with agencies that are actively hearing questions.
    - Tracking all aspects of each initiative and seeing if they are
      ▪ Reducing risks, closing vulnerabilities, mitigating consequences
      ▪ May find that we did reach our milestones, but it hasn’t affected the landscape as expected.
    - Would be interested in hearing thoughts from ISPAB on the plan and how to measure effectiveness.

  o **Mr. Gantman** – agreed. What we are trying to do is reduce harm experienced by users and society over time.
  o **Mr. Lipner** – Added that something that has been brought up frequently is that the agency is responsible for understanding and accepting risks and that risk acceptance is difficult. Are there things in the strategy that address that?
  ▪ **Mr. Leiserson** – Replied that he believes there are. One of the strategic shifts is that we want to see more of the responsibility for cybersecurity placed on more people.
    - Doesn’t mean none of the responsibility is on an agency head or head of a company. Decisions will need to be made specific to risk appetite and context.
    - The challenge identified in the strategy is how many decisions are we throwing on these folk who have a lot of other risks to manage?
- Simplify and reduce the number of decisions that need to be made and move to a shared responsibility model where decisions are made by those who have the right expertise and who has more control over the outcomes.
- Initiative 1.2.1 is focused on secure-by-design and secure-by-default.
  - Secure-by-default example: Have a configuration for critical infrastructure from a service provider and it is the default. An uneducated user may not be able to do what is needed to change the default settings to secure ones. Secure-by-default reduces the number of decisions needed.
  - **Mr. Lipner** – Asked about education on making more informed decisions or making the enterprise experience more like the consumer experience where you can’t get away from the security.
    - **Mr. Leiserson** – On the policy side, there are compatibility, acquisition, and budgetary constraints around modernizing equipment/software. Sometimes our security posture is dictated by backwards compatibility issues.
  - **Ms. Fanti** – Asked about information sharing.
    - **Mr. Leiserson** – Replied that the strategy includes a significant push in the federal government to do more information sharing so we have a common operating picture of what’s going on. Initiative 1.2.4, investigating opportunities for new and improved information sharing and collaborative platforms, processes, and mechanisms, looks at how we think about governance models. Is the Information Sharing and Analysis Centers (ISAC) model the right model for information sharing and we need something else for collaboration? Is it something where it’s also used for collaboration within a sector? Do we need something completely different?

**Final Board Reviews, Recommendations and Discussions**

**Steve Lipner, ISPAB Chair**

**Topics for Future Meetings**

- NCSIP deliverables
- 800-160 Updates (JPL/NASA) and deliverables

**Board Actions**

- **Ms. Moussouris, Mr. Gantman, and Mr. Lipner** discussed sending a letter to CISA on questions she raised regarding goals and metrics for secure development in a variety of system architectures and strategies for enforcement of secure-by-design.
  - **Mr. Lipner** mentioned Microsoft’s approach to secure-by-design.
  - Consulting with folks already using best practices start to answer what they measure, what they have seen, and how to identify the candidates for harmonization to best practices.
  - Should include something about the fact that trying to measure one organization against another organization is often not a useful metric.
    - Metrics that tend to be more useful are measuring oneself against oneself.
    - Create measurements that would write the organization’s “backwards story.”
    - Could be good to include something about ineffective software security.
  - **Mr. Lipner** agreed to try and write something.

**Next Meeting**

- The October 25-26, 2023, meeting will be in-person in Washington, DC.
Motion made and seconded to adjourn meeting. The Chair thanked everyone for their participation and adjourned the meeting at 3:30 p.m. ET.

<table>
<thead>
<tr>
<th>ISPAB – July 12-13, 2023</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Board Members in Attendance</strong></td>
</tr>
<tr>
<td>Last Name</td>
</tr>
<tr>
<td>Lipner</td>
</tr>
<tr>
<td>Baker</td>
</tr>
<tr>
<td>Fanti</td>
</tr>
<tr>
<td>Fitzgerald-McKay</td>
</tr>
<tr>
<td>Gantman</td>
</tr>
<tr>
<td>Gattoni</td>
</tr>
<tr>
<td>Groman</td>
</tr>
<tr>
<td>Miller</td>
</tr>
<tr>
<td>Moussouris</td>
</tr>
</tbody>
</table>

| **Board Members Not in Attendance** |
| Last Name | First Name | Affiliation |
| Flynn Goodwin | Cristin | Microsoft |
| Hallawell | Arabella | WhiteSource |
| Maughan | Doug | NSF |
| Venables | Philip | Google |

| **NIST Staff** |
| Last Name | First Name | Affiliation |
| Brewer | Jeff | NIST |
| Scholl | Matt | NIST |
| Stine | Kevin | NIST |
| Proud-Madura | Diana | HII/Electrosoft |
| Elliot | Savannah | HII |
| Lurie | Kirk | HII |

| **Speakers** |
| Last Name | First Name | Affiliation |
| Dudley | Drenan | NCD.EOP |
| Herckis | Mitch | OMB |
| Jang | Yejin | OMB |
| Lefkowitz | Naomi | NIST |
| Leiserson | Nick | NCD.EOP |
| Locascio | Laurie | NIST |
| McCrory | Jeremy | OMB |
| Murdick | Dewey | Georgetown University |
| Paull | Emily | DHS |
| Robinson | Angela | NIST |
| Scholl | Matt | NIST |
| Stine | Kevin | NIST |
| St. Pierre | Jim | NIST |
| Tan | Kymie | NASA |

| **Registered Attendees** |
| Last Name | First Name | Affiliation |
| Desir | Abner | National Indian Gaming Commission |
| Friedman | Sara | Inside Cybersecurity |
| Gellert | Eric | Politico |
| Kammler | Albert | Van Scoyoc Associates |
| Kaya | Karen | Crowdstrike |
| Kennedy | Andrew | BPI |
More information from this meeting, including the Federal Register Notice (FRN), Agenda, and Selected Presentations, can be found at the NIST maintained website: https://csrc.nist.gov/Events/2023/ispab-july-2023-meeting.