Information Security and Privacy Advisory Board

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

MEETING MINUTES

December 8 and 9, 2021

Virtual Meeting Platform: BlueJeans

Board Members	**Board Secretariat and NIST Staff**
Steve Lipner, SAFECode, Chair, ISPAB Dr. Brett Baker, NARA Giulia Fanti, Carnegie Mellon University Jessica Fitzgerald-McKay, NSA Brian Gattoni, DHS Marc Groman, Groman Consulting Arabella Hallawell, NETSCOUT Systems Douglas Maughan, NSF Essye Miller, Executive Business Management (EBM) Katie Moussouris, Luta Security Phil Venables, Google Cloud	Matthew Scholl, NIST Jeff Brewer, NIST Caron Carlson, Exeter Government Services LLC Warren Salisbury, Exeter Government Services LLC

Wednesday, December 8, 2021

Welcome and Opening Remarks

Steve Lipner, Chair, ISPAB, Executive Director, SAFECode

ISPAB Chair Steve Lipner, executive director of SAFECode, opened the meeting at 10 a.m. ET and welcomed everyone to the call.

The Board received a special update on issues related to Executive Order (EO) 14028 in September. Today's meeting will include further discussion of EO-related issues in addition to other topics, including privacy and crypto agility. The Chair encouraged Board members as always to ask questions and share their opinions during the meeting.

A letter was discussed at the end of the September meeting, and the Chair sent a draft text to the Board members. He received some feedback and then sent a revised draft out yesterday. The Board will discuss the letter at the end of today's session.

The Chair welcomed Chuck Romine, director of NIST's Information Technology Laboratory (ITL), back to his role as ITL director after a stint as NIST acting chief of staff during the Administration transition.

Mr. Scholl announced that the legislative team scheduled to speak today had been pulled into an unanticipated discussion that will take up most of their day. They will not be able to speak to the Board as scheduled, and the afternoon's sessions will be moved up.

Welcome and ITL Update

Charles Romine, Director, ITL

Mr. Romine said it was great to be back in his role as ITL director. He is grateful to Jim Olthoff for the trust he showed in asking him to serve as acting chief of staff of NIST during the transition. Mr. Olthoff is currently performing the non-exclusive functions and duties of the undersecretary of Commerce for Standards and Technology and NIST Director. Mr. Romine is also grateful to Jim St. Pierre and Elham Tabassi for keeping things on an even keel in ITL in his absence. He thanked the ISPAB members and noted that NIST derives an enormous value from their conversations and real-time feedback.

- NIST Cybersecurity and Privacy Update
  - Purpose of ITL: Cultivating trust in IT and metrology

    ITL takes fierce pride in the quality of work done with all stakeholders. They also take pride in the trust that the Administration, Congress, private sector and government partners have in ITL, which enables effective partnering and tackling of challenging problems.
  - Current Priority Areas

    Cryptography
    Education, Training and Workforce Development
    Emerging Technologies
    ID and Access Management
    Privacy
    Risk Management and Measurement
    Trustworthy Networks and Platforms
  - Current Mandates

    National Defense Authorization Act
    IoT Cybersecurity Improvement Act
    EO 14028
    National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems
    National Strategy to Secure 5G
  - Addressing Threats: EO 14028
    - Directs the Secretary of Commerce, through NIST, to consult with federal agencies, the private sector, academia, and other stakeholders and to identify or develop standards, tools, best practices, and other guidelines to enhance software supply chain security.
    - Resulting standards and guidelines will be used by other agencies to govern the federal government's procurement of software.
    - Directs NIST to initiate two labeling initiatives related to IoT and secure software development practices.
    - Held a workshop on Enhancing Software Supply Chain Security: June 2021
    - Published initial guidance and guidelines to enhance software supply chain security: June-July 2021
    - Released draft revision of SP 800-218, NIST Secure Software Development Framework
    - Released draft revision of 800-161, Cybersecurity Supply Chain Risk Management
    - On track to deliver on all tasks.
  - Cybersecurity Highlights
    - IoT Security
      - Final IoT cybersecurity risk management guidance for federal agencies (SP 800-213), released after revisions based on stakeholder feedback.

    - Labeling for consumer IoT Products (EO)
  - Ransomware
    - Draft Cybersecurity Framework Profile for Ransomware Risk Management (NISTIR 8374)
    - Virtual Workshop held July 14, 2021: Preventing and Recovering from Ransomware and Other Destructive Cyber Events
    - Tips and Tactics for Preparing Your Organization for Ransomware Attacks
  - Operational Technology Security
    - Tips and Tactics for Control System Cybersecurity
    - Revising NIST Guide to Industrial Control Systems Security (SP 800-82)
  - Looking Ahead
    - Request for Information (RFI) for updating NIST Cybersecurity Framework for supply chain initiative
    - Pending changes to encryption standards used by the US government for post quantum in the next 2 to 5 years.

- AI Risk Management Framework
  - RFI closed September 15, 2021
  - Workshop held October 19-21, 2021 – NIST released a brief summary of 106 sets of responses to the RFI in advance of workshop. The workshop drew more than 800 attendees. The recording is posted on the website. They are about to release a concept paper for comment.

- 2022: Celebrating 50 years of Cybersecurity Research at NIST

- ISPAB Leadership
  - Mr. Lipner's tenure as ISPAB chair is coming to a close early next year. Mr. Romine has reached out to see if he is willing to continue serving, and he has agreed verbally. There has been no formal announcement yet.
- Discussion
  - The Chair asked whether all of the latest tasks charged to ITL have been matched with resources.

    Mr. Romine said they could always do more with more, but they find ways to accommodate the requirements within the scope of resources given. The challenge is diverting resources away from productive programs to meet mandates as they arise. It can be a balancing act, but ITL has a long history of delivering high quality results on time. The budget is adequate for what they need to accomplish.

    Mr. Groman said Mr. Romine is the most diplomatic person in the U.S. government. NIST could benefit from additional resources.

  - The Chair said that at the next meeting it would be good to get an update on the AI Risk Management Framework.

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

NIST Privacy Program Update

Naomi Lefkovitz, ITL; Dylan Gilbert, ITL; Jessica Dickson, ITL

Ms. Lefkovitz introduced new team members, Dylan Gilbert and Jessica Dickson.

Mr. Gilbert began with an overview of updates to the Privacy Engineering Program.

- Privacy Engineering Program Updates
  - Privacy Framework
    - 64.8k Privacy Framework Downloads: There has been an uptick in downloads of the Privacy Framework in 2021 over 2020, and there is a nice distribution around the world. The pandemic has hampered efforts to engage in some circumstances but also made it easier to build volume, particularly on the international front with virtual meetings.
      - Domestic: Focused on marquee events, like the RSA Conference, HIPAA Summit, and International Association of Privacy Professionals events. They have also been doing targeted strategic events like the IAPP Learning Labs and Privacy Law and Technology Association events.
      - International: Regions of focus include Southeast Asia, South America, and the Middle East. Two of the top three downloaded resources are the Portuguese and Spanish translations. They are continuing to work on outreach opportunities with Department of Commerce colleagues. For example, in Brazil they can leverage the Portuguese translation and a crosswalk to Brazil's data protection law, LGPD.
    - 50+ Resources, including:
      - Quick Start Guide for Small and Medium Businesses – A tool to identify key activities and outcomes to get a privacy program off the ground or to bolster one. Even a lot of large organizations have quite small privacy programs so it became clear that there was a need for this type of resource.
      - Four-minute video presenting the Privacy Framework at a high level for those who may be uninitiated.
      - They continue to work on new resources to assist implementation, including sector-specific profiles and success stories. They just published a success story from the Arlington County, Virginia government, where they profiled their use of the Privacy Framework and how it has helped them bolster their privacy program and risk management activities. They hope to build out other mappings with compliance frameworks like HIPAA and Gramm-Leach-Bliley.
    - New Resources
      - California Consumer Privacy Act Crosswalk
      - LGPD (Brazil Data Protection Act) Crosswalk
      - Indonesia Bahasa Translation: Provided an entry point for webinars for private and public stakeholders in the region.
      - Iron in the Fire: Colleagues in the UAE have indicated interest in an Arabic translation and a webinar in that region.
    - 3000+ workshop/webinar attendees: Great engagement from stakeholders.
    - Regulatory Crosswalks: Privacy laws and regulations have been top of mind. They have heard some organizations expressing concerns that compliance could be a barrier to privacy adoption. The time was right to highlight regulatory mappings and talk about how they can be used as tools to integrate both compliance and risk management to emphasize that it's not a zero-sum game. It is being used as a way to build a foundation for Privacy Framework profiles that an organization can go above and beyond with based on their mission drivers, risk tolerance, and other considerations.

Mr. Groman asked if there were concrete next steps or specific dates coming up with the Privacy Framework.

Mr. Gilbert said they are continuing to reach out domestically and regionally, build out a resource repository with sector-specific profiles, and develop success stories from Privacy Framework implementors. Another concrete step is the workforce working group.

Mr. Groman asked if there were plans to update or revise the Privacy Framework.

Ms. Lefkovitz said there is no plan yet, but they are interested in hearing what stakeholders say about the AI Risk Management Framework and how it may or may not relate. More is going on with the Cybersecurity Framework and they want to see how that goes and then decide if it indicates whether they should also do some updating. They are thinking about exploring some short-form videos about how they have been hearing from different stakeholders using the Framework.

The Chair asked about draft guidance on consumer software labeling that ITL produced per the EO. It occurred to him that privacy was part of that space. Are they being pulled into EO responses and deliverables where appropriate? It seems like there is overlap there.

Ms. Lefkovitz said that the EO was narrowly scoped to cybersecurity, and, at the same time, they have been hearing from some stakeholders regarding privacy. Nothing has been determined yet.

- Privacy Workforce Public Working Group (PWWG) launched April 2021
  - This is an example of a Privacy Framework-associated or parallel workstream. During the Framework development, stakeholders expressed challenges with recruitment and development – demand is outpacing supply. They are creating a workforce taxonomy around the tasks, knowledge, and skills (TKSs) needed to support and describe a workforce capable of managing privacy risk. By its nature, this is interdisciplinary and involves a lot of collaboration and communication – engineering teams, IT teams, marketing teams, etc.
  - Goal: To support the development of a workforce capable of managing privacy risks by identifying and documenting TKS statements aligned with the NIST Privacy Framework and NICE Workforce Framework. The intent was to apply the NICE Framework model of TKS building blocks. The TKSs are aligned with the NIST Privacy Framework outcomes and activities.
  - Quick Facts:
    - 600+ members from around the globe
    - Two project teams (PTs) with about 100 members each: PT1 is dedicated to creating the TKS statements aligned with the risk assessment category; PT2 is dedicated to creating TKS statements aligned with the inventory mapping category.
  - Next Steps:
    - Establish a third PT team.
    - Complete TKS statements for Project Teams 1 & 2
    - Potentially finish up with the Privacy Framework in 2022

Mr. Groman asked about a roadmap for privacy careers and how to structure a privacy program. What is the balance of lawyers, engineers, technical people – senior, midlevel, junior – needed, and what do the portfolio and descriptions of the different capacities or roles look like? Will the PWWG help organizations address what a program and career trajectory look like?

Mr. Gilbert said you can think about it in two buckets. There are TKS statements for your on-the-ground workforce. Then you've got a bucket more HR-flavored and may go more towards the idea of building out work roles, doing recruitment, etc. There is a lot of overlap between them. They want to do both because they have a clearly articulated need for both. It can be challenging to strike the right balance. They want to create the whole body of TKS statements so they can eventually be leveraged to create a work role, team, or competency that can be used internally or potentially just for recruiting, training, education, etc.

Mr. Groman said he would like ISPAB to explore a communication, perhaps to the Office of Personnel Management (OPM), to suggest the development of guidance on privacy positions in the federal government. ITL's work could be leveraged for that benefit.

Ms. Miller said they went through the same thing when they created the cyber workforce across government, with establishing the competencies, the occupational series, and the common lexicon. At some point, we need to make sure OPM is in the mix so there's visibility across government.

Ms. Lefkovitz said they would be happy to talk further about that.

- Privacy Guidance

  Ms. Dickson provided an overview of in-progress and upcoming privacy guidance:

  - In Progress
    - SP 800-53A (draft): Assessing Security and Privacy Controls in Information Systems and Organizations
      - This guidance is focused on updating the assessment procedures that correspond to the consolidated catalog of both security and privacy controls rolled out last fall as part of 800-53 Rev.5. This document existed as part of Revision 4, but this is the first time that the procedures themselves drill into privacy. They track back to the consolidated control catalog that also includes privacy.
      - 53A is currently undergoing final comment adjudication by the Risk Management Framework (RMF) team. Once the publication is final, privacy assessors are going to have a much more granular level of procedural guidance available at their fingertips.
    - SP 800-50/16: Building a Cybersecurity and Privacy Awareness and Training Program
      - They are coordinating closely with NICE and a small group of interagency co-authors to update and consolidate SP 800-50 and SP 800-16. The revised publication will fully integrate privacy and provide guidance on how to build a parallel privacy awareness and training program, just as they would their security awareness and training program.
      - They released a pre-draft call for comments that closed in November, and they are going through the comments and determining the overall direction moving forward. They anticipate publication in 2022. The exact timing is to be determined.
  - Upcoming Efforts
    - They are working closely with the RMF Team on potential updates to incorporate privacy into other publication. Three candidates:
      - SP 800-60: Guidance for Mapping Types of Information and Information Systems to Security Categories
      - SP 800-18: Guide for Developing Security Plans for Federal Information Systems
      - SP 800-30: Guide for Conducting Risk Assessments
    - The exact timing and ordering of the updates is resource-dependent.
    - Let them know if there are other publications that they should be considering similar updates for.

    - Stakeholders are leaning a bit towards SP 800-60. They would look at incorporating content from SP 800-122 into SP 800-60 and then retire SP 800-122 because there is confusion about why it is a separate document. There is interest from both privacy and security stakeholders to have everything in one place. SP 800-60 does not have PII in it as an information type at the moment.

  Ms. Fanti asked if the cybersecurity and privacy awareness training document is targeted mostly toward professionals or at educators as well.

  Ms. Lefkovitz said they are looking to makes sure it is useful to the federal privacy community as a starting point and making sure it aligns to requirements in OMB A130, but the goal is to make it universal enough that it can be used by other audiences as well.

- International Standards
  - There are two standards they have been very actively engaged in over the last several months:
    - ISO/IEC WG 5 (27557): Focused on organizational privacy risk management. Currently advancing to draft international standard (DIS) stage. The next international meeting is in March 2022.
    - ISO WG 1 (31700): Focused on privacy by design. Currently advancing to DIS stage.
  - Neither is “officially official.” They anticipate they’ll be finalized at some point in 2022, and they appear to be tracking in a positive direction.
  - By being engaged in these standards organizations and being at the table for some of the conversations on these particular standards, they have been able to incorporate NIST principles into the foundational documents. They have been able to integrate the concept of a privacy event, for example, and talk about privacy impacts as part of their work on this Standard 27557 and make various other tie-ins to the Privacy Framework as well as the NIST privacy risk assessment methodology.
  - Ms. Lefkovitz added that this is a huge deal in ISO, which has been dominated by the Europeans and the terminology that comes from their laws.
- Differential Privacy
  - They have been doing work on differential privacy for some time, and this coming year might be their moment in the sun at long last. They have been trying to focus on one topic at a time and started with de-identification. That was narrowed to differential privacy use.
  - They have more than a dozen open-source tools now in the space, so they wanted to begin thinking about how to help people better use them. How do we get to the point where we can develop good technical guidance, and then, even further down the road, perhaps take that into standards development organizations?
  - Blog Series: (14 posts total; 2 remaining) The idea was to talk to two audiences: 1) product owners, business owners, and data users; and 2) IT and engineering folks. The series has been so successful that they can now use it as a foundation to develop guidelines, which they will start in 2022.
- Privacy Enhancing Technologies (PETs) Initiatives
  - Secure Data Sharing Workshop: May 2021

        - There is a lot of interest in the Administration broadly from the standpoint of technologies that can help support democratic values and how we can work with likeminded countries on emerging technologies in a secure and privacy-preserving manner.
    - NIST co-hosted the workshop with the National Science Foundation (NSF). It looked at how we can make these valuable resources and datasets more available for research to benefit all. There are a number of barriers to opening up some of these datasets, including security and privacy issues.
- Innovation Prize Challenges: 2022
    - As an output of the workshop and the parallel tracks that the Administration is interested in, they are continuing to work with the NSF and the White House Office of Science and Technology Policy (OSTP) on developing prize challenges, both domestically and with some global partners

- Discussion
    - Ms. Moussouris asked if there were additional details about the prize challenges.

      Ms. Lefkovitz said they are working with the NSF and OSTP to better understand the specific technical barriers to using these technologies. They are working on a parallel track in the international arena, and the United Kingdom is also very interested. There is a lot of interest in synthetic data generator tools, federated learning, and combining other technologies with federated learning. Typically they get mostly academic applicants to these challenges, but it is open to the public. The prize amounts tend more toward academic needs.

      Ms. Tabassi said that the Administration would be announcing the challenges as part of the Summit for Democracy.

      Ms. Lefkovitz said that initiative was announced during the Summit for Democracy and is part of a series of international challenges on democracy-affirming technologies. The challenges will be listed on NIST's Privacy Engineering Program website and the NSF website.
    - Ms. Fanti asked about the differential privacy initiative and if the plan is to offer guidance on how to choose parameters.

      Ms. Lefkovitz said they talked about that in the blog series. Whether the challenge would be able to come up with a tool for this remains up for discussion. It would be a great area for AI. AI could potentially help with making decisions about the parameters, but it is a matter of putting in some factors specific to the organization, not just universal factors.

      Ms. Fanti said she is concerned about two things: 1) Companies using differential privacy as an excuse to collect data they weren't previously collecting and potentially using loose privacy parameters to justify that; and 2) using stringent privacy parameters so it looks like you're getting a good privacy guarantee but then collecting multiple data points over time so the privacy guarantees get corrupted. That is something seen in practice in the past.

      Ms. Lefkovitz said she would like to talk about that further because those are areas they could potentially call out in the guidelines as something to be aware of.
    - The Chair noted that in December of last year they sent a letter about privacy resources at NIST, and there was speculation that it might have fallen through a crack in the transition. They sent an update to the letter to ITL a couple months ago. Did it make its way to its destination?

Mr. Scholl said they would need a final Board approval and then they can route the letter through the proper channels.

The Chair said he would email it to Board members during the lunch break.

Ms. Miller said she thought they had agreed to sending the letter back in June.

Mr. Scholl said the required official approval is just a pro forma Board activity.

Mr. Groman said that when the Board first drafted the letter, ITL's privacy team had a total of four full time equivalents (FTEs) and Ms. Lefkovitz. They have been given more work and more mandates, but no additional FTEs. Has anything changed?

Mr. Stine said the opportunities have continued to grow, but the FTE count has remained pretty flat.

The Chair said he would send the revised version of the letter around at the lunch break and the Board could address it in the afternoon.

- The Chair said the ISO standards on privacy for consumer products reminded him of the connection to the EO deliverables. From a former vendor perspective, anything that provides unified guidance would be helpful to the industry.

The Chair recessed the meeting for a 1-hour lunch break.

NIST Cybersecurity Program Updates

Matthew Scholl, ITL, Kevin Stine, ITL

- Cybersecurity Framework (CSF) Update
    - RFI planned for early 2022: It has been over 3 years since they last updated the CSF. They have been thrilled with continued uptake across sectors and around the world. There is increasing international adoption and adaptation, and the trend is continuing on the privacy side as well. They are operating in a very dynamic environment, and there are plenty of opportunities to improve the CSF based on the changing threat landscape, evolution of technologies, and different practices and capabilities they are trying to leverage.
        - Take stock of how the CSF is being used today: Get a sense of the landscape, what is and is not working. Are there new features that could be added?
        - Opportunities for greater alignment with other resources: Look at the CSF in the context of mapping with other references, such as the Secure Software Development Framework (SSDF), NICE Framework, and other frameworks. ITL is conscious of the volume of resources issued and they want to make sure they are aligned and harmonized as much as possible.
        - Supply Chain Risk Management: They are seeking information on challenges organizations face related to the cybersecurity aspect of technology supply chain risk management. This will help inform the new effort launched by Commerce Secretary Raimondo on the heels of the White House Cybersecurity Summit in August. They are looking at software, hardware, firmware, and more. Is there more they can do on the treatment of supply chain in the CSF, and are there other resources that would provide value to the community?
- Cryptography
    - The privacy working group pulled in the encryption team, and they are still learning, from the security side, the different impacts, aspects, and language from the privacy side. Ms. Lefkovitz

and her team brought out different privacy use cases, which will be used in decisions for the next sets of privacy-enabled cryptography for standardization. They are also interested in fully homomorphic encryption, zero-knowledge proofs, private set intersection, and private set union. Working with the privacy team, they are going to look at the next sets of cryptographic primitives that will be necessary to assist with those different privacy use cases.

- Hardware Security
  - This is not emerging technology but it is a newer area of research for NIST – not just using hardware for security, but security aspects and security capabilities that should be in hardware. They have started a research effort and are currently reaching out to stakeholders, talking to academics, manufacturers, DARPA, DoD, and other agencies about what NIST could and/or should do in this space. They have some experience mostly in looking at hardware cryptographic modules and the security that a hardware module would provide against things like side channel attacks, EMI/EMC leakage, and the ability to do different types of deliberate or invasive injection attacks.
- Education, Training, and Workforce Development
  - Because of the pandemic, the workforce has undergone a major shift in how it operates. It has changed how teams are managed and interact. It has changed how they recruit, communicate, and organize their work. This has allowed them to be more flexible in hiring and not be limited to candidates in the Gaithersburg, MD geographic area. From a research perspective, it has accelerated a lot of deployments. It accelerated the perimeterless network reliability – not just end point, but endpoint health test, end-to-end type of things, Zero Trust, and strong identity mechanisms, which they had been moving at a pre-COVID-19 pace in the research world, but had to take a relook, catch up, and re-evaluate their research for the next step items. They are looking at new developments and business models around micro virtualization services and how they are secured and deployed in large-scale, multi-cloud mesh environments, and how they get integrated into a geographically distributed development environment in a way that preserves security, identity, and assurance of the source of the material. Some of that is also related to the software supply chain.
  - The Chair said it might be interesting to see a paper on lessons learned from the pandemic, remote working, and the technology used. It would be interesting to look at what was and was not important and at where we should have put more emphasis.

    Mr. Scholl said they have been looking at research being done by others. A lot of it is market oriented. One research project looks at the huge shift to eCommerce. Everyone wants to do direct marketing to consumers now, and there is a wide expansion of consumer data and widespread use of cookies for understanding consumer activities. Everyone wants to be a marketing data company now. What does that mean for earlier assumptions about security and privacy? They are also looking at this research in the context of ITL's nine priority areas. Are they still being effective, and if not, where are the gaps they need to update?

    The Chair said he was thinking it would be particularly informative in terms of how ITL prioritizes and how the research agencies prioritize.

    Mr. Scholl said they had a large piece of research significantly accelerate around privacy mechanisms for tracking and tracing devices. If they wish to use contact tracking and tracing capabilities over apps, how can that be done in a privacy-preserving and enhancing way using cryptographic mechanisms?

- NCCoE

  The NCCoE takes research and translates it into actionable and practical uses for organizations. It is a collaborative hub where they are trying to demonstrate with industry practical application of cybersecurity standards and technologies. In some ways, they provide blueprints for how organizations can use those technologies and standards to help address cybersecurity challenges. Some technical areas where they have initiated work and are making progress:

  - Zero Trust: Over the last couple years they issued guidance on Zero Trust, setting some foundational tenets. They are working with about 20 industry collaborators to take the guidance and implement technologies to demonstrate Zero Trust tenets and Zero Trust architecture implementation that can be used to help reduce cybersecurity risk. They are currently in the build phase, using real technologies to help build out the blueprints or example solutions for how an organization can implement Zero Trust architectures and capabilities within their environment. This is supportive of the federal Zero Trust strategy that has come out within the last few months.
  - Cryptographic Updates: They work closely with the cryptography team on applied cryptography projects. Two that have gotten a lot of attention are:
    - Crypto Agility: The focus is on developing practices to help organizations prepare for the eventual migration to quantum-resistant cryptographic algorithms. This is being done in partnership with the PQC standardization process. Part of the scope is to complement the post-quantum crypto standards activities and provide the types of tools and guidance that can help organizations prepare for that future transition. They are seeking industry collaborators now.
    - Cryptographic Model Validation Program (CMVP): This is an opportunity to enhance and bring greater automation to the CMVP. They will be soliciting industry collaborators to help build out that capability. They are trying to demonstrate the value and the practicality of automating parts of the CMVP to improve the efficiency and timeliness of the CMVP program operations and processes. Think of it in terms of creating a potential first-party or third-party test and tools for improving automation.
  - 5G Cybersecurity: They are in the build phase of this project, working with about 12 industry collaborators. In the lab they are designing an example solution for operators and users of 5G networks. This example focuses on the kinds of standards that are in place today and the defined cybersecurity features within those standards, as well as using the underlying cloud infrastructure that can provide the trust foundation, which is in some ways outside the scope of the current 3GPP/5G security standard but is essential for secure 5G operations. The output of the project will be a security reference architecture for 5G networks.
  - Genomic Data and DNA Sequencing: This was called out in last year's National Defense Authorization Act. Genomic data is very important and very sensitive, and that has been highlighted even more with many of the experiences around the world over the last couple years.
    - There might be unique cybersecurity requirements, challenges, or constraints around that data and how to best protect it from a cybersecurity and a privacy perspective. This potentially could lead to technical challenges to store and protect the data. They are working to identify genomic data, cybersecurity and privacy concerns, and ultimately develop guidance.
    - They will hold a virtual workshop at the end of January 2022. They are collaborating with colleagues in the Materials Measurement Lab at NIST who have expertise in broader biosecurity, bioscience, and genomic data efforts.

Ms. Miller said DoD has somewhat of a lead role in establishing security in the 5G arena, and there will be some great lessons learned coming out of that.

Mr. Stine said they have tried to maintain close contact with them to minimally track progress and provide some input. They are trying to remain in sync with them.

Mr. Scholl added that at the very end of the last Administration, they worked closely with DoD, NSF, and OSTP when they put together the R&D National Strategy for Securing 5G and Beyond. That was a great introduction into the DoD leads working not just in R&D, on RF, and security issues around it, but also in the deployment. There was a lot more significant deployment than they had realized.

■ Crypto Agility

- As they work on standardizing the next set of post-quantum algorithms and replacing some of the key management mechanisms and digital signatures, they are on track for announcing the finalists in January or February, 2022. Then they will work on the cryptographic parameters to finalize the standardization. They are making sure they understand each of the different candidates, not only from the security aspects, but also from the business and performance aspects. For example, which have intellectual property around them, and how would that affect or not affect adoption by commercial technologies or inclusion in standards? They are comparing the different implementations against the different use cases and looking at trade-offs.
- Last year they did a review of Advanced Encryption Standard (AES). They looked at all the different theoretical attacks that had been proposed against AES, and NIST is continuing to say that AES 128, AES 192, or AES 256 are still good to go. They might end up tweaking a couple of the modes based on some feedback and research. They have not yet talked openly about what they think a transition time will be for things like potential key schedules or for deprecating some of the quantum-vulnerable algorithms going forward.
- Publishing those key schedules and transition dates in Appendix C of SP 800-133 is not necessarily the most effective way of letting everyone know the day they are going to cancel an algorithm. They are working with the NCCoE and industry, DHS partners, and the National Cyber Directorate to have a more aggressive, public, and effective communication strategy to let people know about the issues and transition when the encryption is available. We will need a more aggressive outreach and awareness campaign.

■ Discussion

- The Chair asked about a CloudFlare article that talks about challenges in transitioning the web to post-quantum and the possibility of having to use several key exchange algorithms. He said it seemed complex and scary.

  Mr. Scholl said when you're using a protocol that is a bi-directional interoperable protocol requiring both sides to be at the same level of transition (to a post-quantum algorithm), you are going to be in a time of what they have been calling hybrid implementations. They have been talking about allowing different types of hybrid implementations in a TLS negotiation. When will a potential downgrade be allowed versus not allowed? What is the cut-off date or forcing function that brings everybody across? A lot of this involves discussions with major vendors and major providers. "This is the cut-off date" sometimes becomes a major incentive for everyone to say, "Ok, I'm coming across." When Edge and Microsoft say it, that becomes the major incentive. There will be a transition time when there will be hybrid multiple stack implementations, and that will require some negotiation n the establishment of those tunnels. It concerns them because it becomes an opportunity for misconfiguration and errors to creep into the implementations.

- Ms. Miller said they want to make sure the operational agencies have as much advance notice as possible. Previously there has been mission impact in doing these kinds of transitions.

  Mr. Scholl said this is true especially for large, long-life programs that the DoD has, when they've got platforms that live for 50 years. The refresh rate on a large bulk power generation is not like that in a laptop or in a cloud-offered piece of software. They are looking internally in the government right now about prioritizing outreach. They are starting those types of inventories to ensure that they have that type of effective communication to those communities. They need lead time for their infrastructures, budgeting process, technical migration. That's also why they need to do this now before the crypto-relevant quantum computer comes out.

- Ms. Hallawell said transitions affect organizations, particularly verticals like banking, that have a lot of legacy infrastructure. Are there ways of helping organizations figure out how they are impacted, how they should start planning, and what systems are likely not going to be able to be upgraded for a long time? Is there any holistic work being done on how this move changes security architectures?

  Mr. Scholl said that on Thursday the Board will hear about an NCCoE project trying to address some of those points: How do you prioritize? How do you even find if you're using affected encryption that would need to be changed out? What do you do with systems that can't be upgraded? What is the information, data, and mission that is being protected? Can you build out a discovery script that will let you know if you are using RSA? Can you do certificate discoveries to see what's where? The larger piece is the communication piece. The financial sector seems pretty aware and pretty eager to transition. NIST has good contacts from both Treasury and the regional Federal Reserves. DHS has reached out to the sectors to get the communication out.

- Ms. Moussouris said this strikes her as a supply chain issue. Also we have seen in the past, especially with encryption, the long tail of downgrade attacks in the name of interoperability. What is the messaging around how to fail safely?

  Mr. Scholl said that is a complex problem. One of the issues they looked at in the selection process for the algorithms is brittleness. How easy is it to implement safely, securely, and correctly? When we get to transition time, they are going to have to work internally with the U.S. Government and also with a lot of industry partners so they do not allow for downgraded communication. They don't currently have solid transition dates. Mr. Stine and his team started a project looking at the challenges of implementing things like TLS 1.2, and end-to-end implementations, especially in large scale environments that might have other issues around logging, tracking, reporting compliance. You want to monitor internal traffic to some extent and how you balance those two things is important as well.

- Ms. Fanti asked about how they evaluated ease of implementation or how likely it would be to have implementation errors.

  Mr. Scholl said they have looked at the use of hash-based signatures to do things like code signing. To successfully implement a hash-based signature tree, you have to keep state. You have to keep this extra piece of data in memory that you have to point back to and reference. This adds an extra level of complexity of error-checking, of implementation, that some of the other more core type of implementations don't necessarily have. There are other ways to look at software complexity, numbers of rounds, how the keys are generated and/or exchanged. It's a heuristic combination of what they know and what they think they know. The other way is to look at some of the different attack methods and how they implement to protect against them.

- Education Workforce Development
  - They just completed the annual NICE K12 Cybersecurity Education Conference, where they shared a National K12 Cybersecurity Educator Roadmap. They also recognized recipients of the President's Cybersecurity Educator Awards.
  - They are completing a 2-year review of the NICE Framework. Updates will include a revision to the document on competencies, a proposed draft change process for public comment and changes to the KSA statements. Existing ability statements were converted into skill statements or eliminated. There is an upcoming webinar, *Witnessing an Evolution- The NICE Framework and its Role in Building a Better Cybersecurity Workforce*.
- Risk Management
  - How do we help organizations manage cybersecurity risk in the context of enterprise risk? How do they integrate the cybersecurity risk management processes with other risk management? In the federal space, in many ways this is about how we bring greater alignment between the A130 world and the A123 world. There are a lot of opportunities there, and they look forward to continued feedback.
  - SP 800-53A is coming out probably at the end of January. They are integrating many of the privacy controls not only in the control catalog but also into the assessment catalog.
  - They have shifted the media that they are using to present data. SP 800-53 in the past was primarily a PDF document and then after publication they would build out CSV files and the different formats. The team has flipped that process with Rev.5. It will be published primarily as a CSV to allow for ingestion into tool sets and agency-specific scanners or implementation GRC tools. Those who wish can also publish it as a PDF. The primary work will be developing the data as data rather than as a document.
  - Probably in Q2 or maybe a little later this fiscal year, they are going to allow for almost an ongoing lifecycle of the individual controls. People can submit comments, updates, revisions, and changes to an individual control using the automated platforms throughout the lifecycle. When they feel things have reached a level of maturity, they can roll out revisions on an individual control.
  - SP 800-53 will be followed up quickly with other resources, including the Privacy Framework and NICE Framework. Anticipate larger data sets that will be available that can be ingested by different tools and capabilities.
- Discussion
  - The Chair said he envisioned OMB having to go into the repository every night and having to click a link to sign off on the update to individual controls.

    Mr. Scholl said OMB, the CIO Council, and the CISO Council were brought into the requirements process at the outset, and everyone is on board. How do we ensure that people who need to know are aware? There is a lot of built-in capability around *subscribe* and *announce*.
  - The Chair said the Board may want additional presentations on the Risk Management Framework at a future meeting.

- Ms. Miller asked if NIST had to go through OIRA [Office of Information and Regulatory Affairs] before publishing these documents.

  Mr. Scholl said when they first did the integration of privacy control into SP 800-53, OIRA was very interested in how they were including them and what types of priorities were being put or not put on privacy. The initial walkthrough with OIRA was very deliberate so they understood and were comfortable with what was done. They stay in tight communication with them.

  Ms. Miller said she would hate to see OIRA be an obstacle to responsiveness and agility.

  Mr. Scholl said there are some things they make deliberate decisions on what they publish and how they publish it. When they publish a FIPS, it goes through a very deliberative, quasi-regulatory clearance process, with Federal Register notices and agency clearances. Publishing these individual controls is a way to be agile, and then they will split out the text that might need to be in a FIPS.

The Chair recessed the meeting for an 8-minute break.

EO 14028 and DHS Cybersecurity Incident and Vulnerability Response Playbook

Jonathan Homer, Analyst, DHS

- Background
  - EO 14028 called on DHS to make a consolidated playbook that allows for a more uniform and concise response process across the federal space. Being able to respond to incidents and ensure everyone is comprehensively meeting specific requirements.
  - The playbook provides an opportunity to capitalize on lessons learned over the years from previous incidents, incorporating industry best practices.
  - It is targeted toward the federal government with specific elements in mind that are, in some cases, unique to federal departments and agencies. The basic principles apply across the board, and the public and private sectors can view it as a benchmark.
  - The playbook and NIST SP 800-61 are parallel with one another. SP 800-61 Rev.2 is a primary source, and they continue to emphasize its use by the agencies, specifically around determining level of impact, preservation of data, and a number of other areas. There is no conflict or challenge between the two. The playbook goes into greater detail and provides specific guidance about identification, coordination, remediation, recovery, and tracking.
- Scope
  - The Incident Response Playbook only applies when there is confirmed malicious cyber activity or for which a major incident has been declared. They took the definition of major incident from OMB. It comes down to incidents likely to result in demonstrable harm to national security interests, foreign relations, and the economy, or a breach that involved PII that was exfiltrated, modified, or otherwise is likely to result in demonstrable harm to national security interests. This does not apply every time a simple commodity malware hits or there’s some type of spear phishing.
- Incident Response Playbook Sections
  - Preparation: This phase allows an organization to prepare and pre-mitigate any impact. It talks about policies, instrumentation, training, and ensuring that agencies have cyber threat intelligence. They want to ensure agencies are properly postured with the data and information

they need to make informed decisions. They want to make sure they have the proper architectures and tools to communicate. A checklist at the end of the playbook shows specific line items that are required to ensure departments and agencies are doing the due diligence to be prepared and not just be in a reactive posture.

  - Detection and Analysis: This is the most challenging aspect to do accurately. It gets down to some very specific elements. There are a number of stages that CISA and partners have seen that organizations may choose to skip for various reasons but are critical to fully triaging and understanding the environment where an incident has occurred. The significant value is in the appendices at the end, which make up about half of the document. The checklists start to get into very technical specifications. For example, in performing the technical analysis, they call upon the organization to understand the scope, define it, and write it down. Then they call upon them to update the scope as an investigation progresses and as the information evolves. They have to understand what cyber threat intelligence is, form a hypothesis, and test against the hypothesis.
  - Containment: This phase involves the need for isolation and capturing images to enable evidence collection and further investigation. It talks about firewall filtering, blocking unauthorized access, closing ports, changing passwords, rotating private keys, revoking privileged access, directing the adversary to a sandbox to enable monitoring, and that all the steps are done in the proper order.
  - Eradication: Getting the threat actor out of the environment and making sure we are eliminating all points of persistence. This includes violations of code or exploited vulnerabilities. As eradication is concluded, we've removed not only the persistent access but also the methods by which they can regain access into the space. It calls for the development of written, formalized eradication plans. Threat actors often have multiple persistent back doors, and those accesses are critical to being able to identify and eradicate as part of a comprehensive effort.
  - Restoration: Getting systems back online, confirming functionality, and ensuring that increased vigilance and controls have validated that the plan that was designed in the beginning was carried out.
  - Post-incident activities: This is all about reviewing, learning lessons, and capturing and sharing what that information is. Ensuring that the infrastructure and policies are updated, and weaknesses and gaps have been addressed.

- The key point is the concept of having a well-developed plan. The playbook is a checklist that says at each stage you develop a plan, execute the plan, measure against the plan, adapt the plan, and then see where the plan had weaknesses or gaps, etc. Have a strategy for how you are approaching the problem, and along the way make sure it includes some specified elements. If you plan to succeed, you are much more likely to succeed.
- At the end of the document is a comprehensive checklist that guides an organization through the process. It is ideally applied at the operational level. If you have a SOC or incident response team or security team conducting it – whoever it is that owns responsibility for directing and coordinating – the checklist gives the requirement to comply and also a baseline by which they can ensure they are doing due-diligence of completing all necessary steps.
- Appendices: Appendix G is about whole-of-government roles and responsibilities, understanding how the CRGs [Critical Response Groups] and CISA fit in, where the National Security Council fits in, etc. There are also categorical citations.
- Vulnerability Response Playbook

This is different from the Incident Response portion and applies when a vulnerability has been observed that could be used by adversaries to gain unauthorized access. This builds on Binding Operational Directive (BOD) 2201 that CISA released earlier. It standardizes a high-level process that agencies should follow, and it applies specifically to significant risks that pose national risk across the federal government. There is a CISA-managed catalog of known exploited vulnerabilities that was established by that binding operational directive. It can be used to identify the vulnerabilities that require these response actions.

- Discussion
  - Ms. Moussouris asked whether there is a plan for those updating the list of vulnerabilities that have actively been exploited and how CISA is thinking about the sustainability of that.

    Mr. Homer said the list was compiled not as a one-time effort but recognizing that it is an ongoing, constant battle. It should not be regarded as a one-time snapshot but rather a monitoring posture to note new vulnerabilities. It is not designed to be comprehensive of all vulnerabilities – just those posing the greatest threat to the national risk posture. They have stressed the criticality of patching all vulnerabilities that apply in that space. Because every organization is unique, each has different components, different software, different hardware elements.
  - Ms. Moussouris said those were the points of her question. What is the plan for sustainability and ensuring that organizations don't take this only as far as they need to go to comply? It is incredibly difficult to keep vulnerability data updated in real time. Some of the oldest CVEs were being given a 6-month window whereas some released in 2021 were given a 2-week window. How were those decisions made? Is it going to be the policy going forward that the latest vulnerabilities have the highest priority for application and some of the oldest known vulnerabilities are being given an even longer grace period?

    Mr. Homer said it was determined through significant discussion and planning. It was recognized that there are challenges and complications. With some of the older vulnerabilities that had been exempt for whatever reasons within specific organizations, it would not be plausible to be able to immediately apply a patch. These systems may be legacy or have other challenges an operator faces. For that and other reasons, there is a larger window with some of the more complex situations. As we move forward, the focus is on what the threats are, coming back to the national risk posture. They are evaluating the full gamut of vulnerabilities all the time, but the critical ones and those that are going to pose the greatest danger are mostly likely to emerge in the forefront. He would expect that that we are going to see things that are "this week" and "this month" types of timeframe. There will be a quicker turnaround because they are in the newer products.

    Mr. Scholl added that NIST and DHS worked closely on that. They are not publishing an NVD, metric, or measure about what is currently under exploit. NIST does not have that information.
  - Ms. Miller asked how this takes into account the requirement for information sharing between government and industry and how it changes any requirements that are currently leveled on defense contractors.

    Mr. Homer said information-sharing is a clear element within the executive order. It's challenging to break it out and say how it is addressed in the playbook. The playbook integrates two very specific elements. There are very articulate moments or reporting requirements that align with other areas and other reporting requirements to be able to provide information and the level of detail. Integrated within the playbook checklist are line items where it says something has to be reported within a timeframe and that the report must contain the impact or the anticipated plan for recovery or whatever the appropriate element would be at that stage. Those elements are critical to being able to have the department or agency report back to CISA. Then CISA has responsibility for sharing that information through the various information-sharing requirements and authorities. There will be an element in looking at the maturity of how all of this data flows in to be able to be shared and worked as well. There's also almost an underlying element – if we can get organizations that are boots-on-the-ground to be more consistent about what data they collect and how they approach a problem, allowing them flexibility to adapt to specific conditions, but enabling the capability for them to always report the same types of data and ensure that we're comprehensive. We can start to understand, track, and trend, not just at CISA but also with industry partners and leaders in cyber firms, etc. to have standardized or semi-standardized data, to be able to understand how things look when comparing between and across incidents. So, the playbook itself does not necessarily mandate that you must share with third parties or other elements that are beyond the authorities and requirements established by policy. But it sets a standard by which such things can take place, and there is opportunity for us collectively in the future to further mature that and capitalize on that as this data starts to normalize.

- The Chair asked if they have tried exercising the playbook, running drills or simulations.

  Mr. Homer said yes. They recognize that there will be opportunities for improvement. There are some major components of the playbook that call on existing, publicly well-known, time-proven materials that they were using in-house or specific agencies had. The compilation was not about starting with a blank sheet of paper. It was about leveraging some proven techniques and pulling the best from different sources that were across the board. In that regard, they have seen the success of the checklist in a number of different incidents, including some fairly high-profile ones. They recognize that it is not going to be perfect. The playbook is directly called upon to do regular updates. They are open to receiving feedback as organizations have insights into what works and what does not. He would anticipate there will be feedback that will lead to revisions.

- The Chair asked if this is getting so that you can update based on experience and lessons learned?

  Mr. Homer said the checklist calls for the submission of the hot wash to conduct the lessons learned analysis and identify the gaps and unclear roles, and to be able to incorporate that and then to coordinate with CISA throughout the process. Checklist item 11G is to provide post incident updates as directed by CISA. As the checklist is being integrated, organizations provide feedback on what worked and didn't work, tactically and strategically.

- The Chair said it would be great if in 6 months or a year there is an incident that can be discussed and Mr. Homer can come back and describe what was done, how it worked, and what the strengths and weaknesses were.

  Mr. Homer said he would see what he could do.

- Ms. Moussouris said the binding operational directive (BOD) for vulnerability disclosure programs did not have a lot of guidance on how to carry out successful vulnerability disclosure programs. In terms of a gap that is relevant to incident response and the execution of vulnerability disclosure programs, is there a plan for adding guidance or an update to the binding operational directive VDP that integrates the investigation steps that should occur internally to determine whether an inbound vulnerability report for a band-new novel vulnerability potentially has an incident that is also happening that the agency was unaware of?

Mr. Homer said he does not have any confirmation of updates to the BOD, but he can confirm that they have active conversations and active process improvement, internally and externally, about how vulnerability investigations and incident responses are not two distinct efforts but play together. They have to intertwine and invoke one another's thought processes, services, etc. As they learn more, they have a great appetite to share what they learn externally. He does not know if it is going to come in the form of a BOD or some other kind of directive, but he is certain they will continue to educate and share guidance about how to do this in more detail. To the point that when a vulnerability is discovered, does it trigger an incident and what does that mean, that is a fantastic area to provide more clarity and it is a conversation they are having.

Public Comment, Summary of Day 1, and Board Discussions

- No public comments were received.
- Board Discussion
  - Privacy Resources Letter
    - The Chair said he received enough positive feedback on the draft letter on privacy resources to take it as a unanimous vote for transmission. He will work with the secretariat at NIST to get it sent.
  - EO 14028 Implementation Prioritization Letter
    - The Chair said that at the September meeting, Ms. Moussouris suggested drafting a recommendation on EO implementation prioritization. The Chair attempted to write draft language and he sent it around for comments.
    - Mr. Groman said he did not feel particularly strongly about the letter, but if it moves forward he has three suggestions:
      - Change the tone slightly. Instead of assuming they have not thought about prioritization, pose it more as a question about how they are thinking about it.
      - The EO exists in the bigger context of 10+ years of implementation of cybersecurity. Prioritization is not just about the EO items, but how they fit in with everything else the agencies are grappling with. Ask how they are prioritizing the competing priorities.
      - The EO places responsibility for cybersecurity on the head of the agency. In Mr. Groman's experience, it is the CIO or the person above the CIO [who takes responsibility for implementation]. The agency head has a lot on his plate and this hits their radar after a problem or breach. In fact, it is the head of the agency who has to own this because the CIO is never going to implement an effective cyber program without the support of the agency head. How are the agencies conveying this to the agency heads, and how will the agency heads be held accountable?
    - The Chair said it seems like there could be a tension between the responsibility of the agency head and the role or responsibility of CISA and OMB in issuing directives that may or may not get adhered to or implemented.
    - Mr. Groman said the agency head is often a political appointee and does not want to be told that something will be slowed down because of a security vulnerability that must be fixed first. We can no longer sacrifice cybersecurity to do things bigger, better, faster. That tension is a huge problem. They need to be told that cybersecurity can't be sacrificed.

- Mr. Gattoni said he agreed. He tried to convince agency heads or mission leaders that every quality of goodness they would use bigger, better, faster is for naught if it is not also secure. Getting security concepts accepted into their vernacular is part of the culture change as opposed to seeing it as a barrier or trade-off that's acceptable in managing risk. There has to be a quality inherent to achieving the mission that it must be done securely. It is a giant challenge with a lot of tension. It is a false trade-off when looking at good versus secure. Make sure security is always on the side of good in those conversations and look elsewhere for the trade-offs.
- The Chair asked members to look at Mr. Groman's mark-up overnight and send an email with revisions with the intent of taking it up tomorrow.
- Ms. Miller asked for clarification on the intent of the memo. Most CIOs look at this as another unfunded mandate.
- Ms. Moussouris said the EO contains many important initiatives, but they come across as all being weighted the same. The goal of the memo was to look at it from the standpoint of prioritization based on ROI for the different directives. Some are very heavy lift items, including rolling out multifactor authentication, but there is proven ROI for doing this, direct evidence, and plenty of solutions. Another heavy lift is SBOM. With finite resources, there should be a distinction between things that have a proven ROI and things that do not. We've got too much to do, too little time, and too few people to do it. She is not sure the draft letter reflects her intent, but she is ok with it.
- Ms. Hallawell asked what Ms. Moussouris thinks the ROI is for SBOM.
- Ms. Moussouris said she has never gotten an answer from the SBOM working group or its proponents. The EO has some very unequal directives in terms of what has proven ROI and what does not.
- Mr Venable said SBOM is a necessary but not sufficient condition to solve end-to-end secure software supply chain risk. SBOM is a useful component, but the real challenge is broader. The real security improvements and the real ROI come in rearchitecting of the end-to-end software supply chain process. It's easier to talk about the ROI in that broader context because SBOM is just a component, and as a component it is not going to enjoy an ROI in itself. It is the broader transformation that represents not just security but also ROI improvements in terms of the ability to increase cycle time updates and increased developer productivity, increase predictability and reliability as well as security.
- Ms. Hallawell said ROI is an important metric. Shouldn't risk reduction also be part of this discussion? The ROI around secure software development is not just around software developers doing it faster, it's the fact that ultimately oftentimes code gets released because it couldn't be scanned either because no one wanted to or it was going to delete things. People made that risk trade-off that they would prefer to release code than test it. Some of that is because it is done post production or too late in the cycle. Part of this discussion should be around where are the areas you can reduce your risk the most.
- The Chair said knowing what you're shipping is fundamental in knowing its security posture – fundamental to being able to ship secure software. When you get to telling end user organizations that they have to have the SBOM of the software they are consuming, he is much more skeptical of the value of that SBOM model. What does the SBOM do for an end user organization? It really lets them beat up their suppliers to make sure the suppliers are doing sufficient due diligence. He thinks it is doable in a lighter weight way than we are

seeing with all the SBOM that has come out. That is his take, and it is nuanced and hard to make into a one liner because it is not just always absolutely the solution to everything but not of no value either.

- The Chair asked what people want to do with the letter.
- Ms. Moussouris said it is hard to capture and has not been captured in the existing draft. It is the idea that there needs to be a prioritization of the items in the EO based on the relative level of effort in exchange for what you get. That is what she means by ROI. To give an example from the vulnerability management world, if you get a report with a list of vulnerabilities, one way to prioritize them isn't necessarily by criticality but by impact and level of effort to remediate. In a bubble chart with quadrants, high discoverability and exploitability and then the size of the bubble represent the badness that will happen to your organization. You have a quadrant in that graph that is your highest priority remediation even if some of the vulnerabilities in that quadrant are not as high criticality as others that are harder to exploit or incredibly difficult to remediate, for example. We need to have some kind of a bubble chart for these directives or ask agencies to think that through in terms of the other factors here.
- Mr. Groman said that makes sense but he would be loathe for ISPAB to send a letter telling OMB how to prioritize as opposed to suggesting that they need a prioritization methodology. A letter could make it clear that agencies need a way to prioritize this EO versus everything else but not more granular in specifying how the prioritization should take place. There are so many factors that are going to be potentially differing by agency and context. Take multifactor authentication as one example.
- The Chair asked everyone to look overnight at Mr. Groman's edit of the draft and send around comments. He will attempt to integrate it and have it ready to discuss at the end of the meeting tomorrow.
- Mr. Groman clarified that he was not advocating for the letter or for his suggested changes. If it does not capture the intent, then maybe don't send it.
- The Chair said he thinks it is worth going forward. Ms. Moussouris should weigh in to bring it back to the intent she had in September.

The Chair adjourned the meeting for the afternoon.

Thursday December 9, 2021

The Chair opened the meeting at 10 a.m. ET and welcomed everyone to the call. He noted that about half of the sessions today will focus on EO 14028.

EO 14028 and NIST SP 800-161

Angela Smith, Co-PI, NIST Supply Chain Risk Management Program

- Update to SP 800-161
    - First major revision to the foundational guidance: A lot has changed in the past 5 years, and they are finally getting the type of attention needed in this area. A lot of incidents have been in the headlines, but there has also been new legislation and the federal government has matured in terms of awareness, understanding, and capabilities. The guidance has evolved and adapted to the changes.

- Objectives
  - Make the publication relevant to a diverse set of stakeholders. They are moving beyond the traditional IT security audience to people who are not used to reading NIST publications, such as acquisition professionals, suppliers, and lawyers.
  - Make sure the publication is something people can pick up, use, and readily find the information they are looking for. They tried to make it more modular.
  - They tried to capture leading practices in agencies and industry and incorporate new concepts and practices.
  - They tried to speak to the vast spectrum of knowledge, capabilities, and skills sets. They looked for tools and templates for those just getting started.
- Major changes
  - Foundational Elements: Introduced a paradigm of organizing in line with capability maturity. Often people don't know where to start.
  - They showed the importance of integration into broader enterprise risk management strategies.
  - Line-by-line review of C-SCRM controls and updated supplemental guidance. They tried to identify which controls might be applicable for flowing down from a prime contractor into the sub-tier.
  - They introduced templates to be used in reference to building out policies.
  - Implementation plan
  - Requirement for separate CSCRM system-level plan
  - Critical success factors
    - Acquisition processes: They introduced discussion around where C-SCRM considerations need to be built in throughout the entire procurement lifecycle. They discussed the importance of identifying critical suppliers and building requirements in contracts.
    - Information sharing
    - Awareness and training: There isn't a lot of curricula for C-SCRM, and the government is just now getting some training resources put in place. There is a need for general training resources and awareness as well as role-based training for specific functions.
    - Measurement and metrics
    - Resources: They spent a good deal of time talking about the importance of dedicated resources. This is about building and augmenting functions that many are already performing across the board and adding in the view into the supply chain space.
- April 2021: Issued initial public draft
  - This was before the EO was issued so it did not incorporate any of the software supply chain requirements and directives. They received more than 700 discrete line item comments. Common themes included:
    - Document is too long/Document is missing things: They restructured content so the main document is under 100 pages, and a lot of content was moved into appendices.
    - What is most relevant: They developed audience reader profiles and provided some upfront material about 10 sections that will be most relevant to people's needs.
    - They added language for smaller organizations to see themselves in the document.
    - Guidance around contract requirements: They will continue to work with the interagency on contract requirements. There may be an opportunity for OMB or somebody else to put

out guidance to help understand how guidance from the acquisition community is complementary to NIST guidance.

- Risk appetite and tolerance: They revised some of the language and included graphics.

- October 2021: Released 2nd public draft – Currently open for public comment

- Discussion
  - Mr. Groman said this is a core foundational problem with this issue and others. Who makes the decision for risk tolerance, for understanding risk, identifying it, and owning it? What has NIST heard in terms of those being accountable for risk tolerance decisions?

    Ms. Smith said that while developing the publication there was also a GAO review that looked into what the major CFO agencies have done with regard to establishing things like risk tolerance and risk appetite. It wasn't good news. Internal controls guidance has been more on the financial side of the house, where there are clear standards, and the concepts of materiality and risk are tied to fraudulent activities. That evolution has not really moved forward in establishing enterprise risk management practices within federal agencies and departments. It is a more perfunctory exercise tied to things like GAO risks and things that IGs fund versus true integration across all layers of the organization. To the point about accountability, the second public draft enhances this in that accountability must begin at the top, with the leaders establishing a risk appetite. In one of the new appendices, there is more specific guidance related to risk assessment processes with regard to significant risks that compel senior agency-level sign- off.

  - Mr. Groman said this could produce the most outstanding guidance possible but until it is baked into agencies across the government, the impact will not be what we need it to be. He has never seen an overstaffed procurement office in the government, and procurement is already slow. This introduces another layer in procurement and nobody is going to be excited about that. You can get your widget 2 years from now and not 1 year from now, and somebody has to say that’s ok.

    Ms. Smith said they continue to assert that the procurement official or contract officer is not the risk owner. This must be a team effort. There needs to be planning for security early on in the acquisition and the procurement process. Security is going to be the fourth pillar of cost schedule performance. It isn’t NIST’s space, but there is a role for compliance coming out of other areas so they have the ability to make faster go/no go decisions.

  - New Appendices
    - Federal Acquisition Supply Chain Security Act
      - The legislation 1) granted authority to do exclusion removal orders. There was limited ability to exclude suppliers to significant supply chain risks, especially from adversarial concerns; 2) established the Federal Acquisition Security Council, which is interdisciplinary and brings together some of the key agencies involved in C-SCRM activities, including NIST, FBI, ODNI, etc. and established a framework for government-wide information sharing and coordination; and 3) mandated that all federal executive branch agencies follow this guidance and perform supply chain risk management activities.
      - The guidance is intended to set out a baseline and even treatment of how assessments occur to facilitate comparison and to help mitigate what could happen with regard to eventual litigation.

- Appendix F
    - Preliminary guidance for enhancing software supply chain security per EO Section 4c. Help agencies understand what they need to do to implement the requirements of the EO.
    - They wanted to facilitate prioritization and practical implementation. They presented the guidance using the same foundational sustaining and enhancing paradigm. They wanted to reflect that, on the supplier side, there is a range of maturity and capability.
    - It covers the three areas of identifying, listing, or developing new standards, tools, and best practices.
    - They included references for software verification and provided guidance around what to require of suppliers. It briefly mentions the IoT labeling and the consumer software labeling program. It describes SBOM and talks about enhanced vendor risk assessment, open source software controls, and vulnerability management practices. They include a table of references to existing standards, tools, and recommended practices and describe them briefly.

- Discussion

- Ms. Moussouris said she is glad they added capability language that would help smaller organizations. That was one of the biggest hurdles to adoption of the vulnerability disclosure ISO standards.

- Mr. Groman said it is a daunting document if you are looking at it for the first time and unfamiliar with the context. On other hand, in the introduction there is a paragraph that is brilliantly diplomatic about incorporating much of the work of other documents and things that are already mandatory. Someone less diplomatic could have written that you should already be doing all of this. Most of this isn't new. Essentially, it is taking the tried-and-true concepts of other publications and applying them in a more narrow area.

  Ms. Smith agreed. However, there are many organizations that are coming to this space for the first time. They want to be open to new IoT vendors who used to build toasters and now are doing security.

- Ms. Fitzgerald-McKay agreed that some of this should be happening already. How much related attention needs to be paid to automating some of these recommendations in a way that NIST can then just say, “Use tools that meet this set of requirements.” Is there a sense that that would add value to this or simplify it for consumers?

  Ms. Smith said there are many vendors that do third-party assessments and many organizations want to outsource their assessment. That can assist, but you need to have those fundamental processes in place. You can’t outsource your risk tolerance determinations. They hammered home that there are foundational elements that have to be in place. They might be able to see if there is more opportunity to build in language about automation.

  Mr. Scholl said they have built out at least an initial set of reference tools or beta tools for organizations to pick up, modify, and customize. They are initially focused on self-assessment tools, supply chain risk assessment tools. They are macro spreadsheet-based right now so folks can put in their specific variables.

  Mr. Stine said there are also opportunities to extend work into the NCCoE to build out example solutions to implement the guidance. There is an active project with several companies focusing on supply chain assurance for hardware. What are the tools available to do that? There is a glide path for a lot of the guidance to end up at the NCCoE to develop examples.

- Mr. Venables asked if there is any reason they are not more prominently advocating mentioning SLSA [Supply Chain Levels for Software Artifacts], a broader framework owned by the Linux Foundation.

  Ms. Smith said part of it is they were already working on the SP 800-161 revisions, and then the EO came out. There are ongoing conversations. They are expecting the updated guidance to come out in February of 2022, and there will be an opportunity to build additional context in. It is already on the radar screen.

  Mr. Scholl said they have had conversations with the Linux Foundation, and their inputs will be reflected in some of the SSDF references. They can't necessarily call out a single implementation, but they can provide pointers and references.

- The Chair said he noticed that the scenarios integrate the controls listed in an earlier appendix. The more real scale and the more detailed you get, the more useful they are. Looking at Appendix F almost felt like it was a way to force the EO to align with the guidance in SP 800-161 rather than the other way around – here's how you adopt the guidance in SP 800-161 to meet the guidance in the EO. Is it still being modified?

  Ms. Smith said there are a lot of moving parts to the EO. It is not certain how it's going to play out.

  Mr. Scholl added that it is in flight. It is bringing the two items together. SP 800-161 has a history that predates the EO. NIST said it was going to do its best to use current references and point to existing work as much as possible rather than give people a new document.

EO 14028 and Software Security Development Framework (SSDF)

Karen Scarfone, NIST Associate and SSDF co-author; Murugiah Souppaya, NIST

- Introduction
  - Approach Similar to the Cybersecurity Framework
    - Provides a common language to describe fundamental, sound secure software development (SSD) practices. There are other publications on SSD, but most were specific to a platform, language, or sector. This was an opportunity to bring those together so that people using different documents could better communicate.
    - Highlights the most important practices and helps organizations adopt a risk-based approach to document SSD practices today and define future target practices as part of a continuous improvement process
    - Leverages existing SSD practices from established standards, guidance, and practice documents.
    - Does no harm (to organization that have already adopted established practices).
  - SSDF Publication Basics
    - Targeted to both software producers and consumers
    - Can be used by organizations in any sector or community
    - Can be integrated into any existing software development workflow and automated toolchain
    - Is broadly applicable
  - Goals for SSDF Practices

Recognizing that there are different priorities and security objectives among organizations, projects, producers, and consumers, they are promoting a risk-based approach that is:

- Flexible
- Customizable
- Selective

- SSDF Practice Groups
  - Prepare the Organization (PO) – Prepare people, processes, and technology.
  - Protect the Software (PS) – Protect all components of the software from tampering and unauthorized access.
  - Produce well-secured Software – Minimize the vulnerabilities in released software.
  - Respond to Vulnerabilities (RV) – Respond appropriately and prevent similar vulnerabilities in the future.
- Elements of an SSDF Practice
  - Task – An individual action needed to accomplish a practice. For each practice, they define one or more tasks.
  - Implementation Example – An example of a type of tool, process or other method you could use to implement the task(s).
  - Reference – An established secure development practice document. At this point they have mappings to 22 or 23 different reference documents in the SSDF.

- Changes made to the original SSDF to support EO 14028
  - Asked for public input on EO Sections 4b and 4e
    - EO issued May 12
    - Section 4b directed NIST to solicit input from the federal government, private sector, academia, and other appropriate actors to identify existing or develop new standards, tools, and best practices for complying with the standards, procedures or criteria in Section 4(e).
      - The original SSDF already addressed much of what 4b and 4e were asking for, so it made sense to make fairly minor updates to the SSDF to address what it wasn't covering.
      - Virtual Workshop June 2-3, 2021: Received more than 150 position papers
      - Reviewed all suggestions, which included suggestions for new and updated practices, tasks, examples, and references.
  - Draft SP 800-218 on SSDF v1.1
    - Released at the end of September.
    - Replaces original SSDF paper.
    - Added references based on public input, including references that would map to industrial control systems and operational technology, mobile devices, supply chain security, and vulnerability disclosure standards.
    - Made other changes to address the EO and latest threats.
    - Created Appendix A to map EO clauses to the SSDF practices and tasks that help address each clause.
  - Addressing 4(e)

    4(e) directed NIST to issue guidance identifying practices that enhance the security of the software supply chain. It includes a set of 10 clauses, which logically group in other ways [i.e., not in numerical order]:

(vi) – Maintaining provenance of software code or components and controls on software components, tools, and services.

- Added PS.3.2: collect, maintain, and share provenance data for all components and other dependencies of each software release
- PO.1.3, PO.3.2, PO.5.1, PS.3.1, PW.4.1, PW.4.5, RV.1.2 –

(vii) – Providing an SBOM for each product.

- Added PS.3.2

(viii) – Participating in a vulnerability disclosure program. They already had tasks and implementation examples for this.

- RV.1.3. – Having a policy addressing vulnerability disclosure, and remediation and implementing the roles, responsibilities, and processes to support that.
- RV.1.1, RV.1.2, RV.2.2, RV.3.3

(i) – Securing software development environments.
(ii) – Providing artifacts that demonstrate conformance to processes from (i). This was an area that they intentionally had made out of scope in the original SSDF. Because of the EO, they expanded the scope of SSDF to include software development environment security.

- Added PO.5: Implement and maintain secure environment for software development
- Added PO.5.1: Separate and protect each environment involved in software development
- Added PO.5.2: Secure and harden development endpoints
- PO.3.2
- PO.3.3

(iii) – Maintaining trusted source code supply chains
(iv) – Checking for vulnerabilities
(v) – Remediating vulnerabilities
There are many practices and tasks in the SSDF that map to clauses (iii), (iv), and (v).
(ix) – Attesting the conformity with SSD practices – which really all practices and tasks in the SSDF could potentially apply to.
(x)

- Public Comment Summary
  - Comment period ended November 5. They are in the process of reviewing and adjudicating comments.
  - Received more than 35 sets of comments and approximately 360 comments within those sets.
  - The majority of comments were suggesting changes or additions, or in a few cases, deletions of practices, tasks, and examples. A lot of people suggested additional examples. There was not much duplication of comments or themes.
  - Two commenters suggested additional references that had not previously been suggested.
  - Three comments on the EO appendix.
  - Themes
    - Clarifying the meaning or the scope of terms like *provenance*, *build environment*, and *dependencies*. They will do that in the next SSDF iteration and take or adapt definitions from existing NIST publications.
    - Addressing the effect of resource limitations on performing practices and tasks at scale. How does a small organization or an organization with very limited cybersecurity knowledge scale these things up? How does a large organization implement these practices? Basically, this is

        getting at automation for larger organizations. How can we make the SSDF more strongly encourage the use of automation?
    - Adding prioritization guidance or context on how to use the SSDF. They would probably address that in a separate document.
    - There's a perception that it gives uneven treatment to commercial and open source software because they talk about implementing least privilege for code access. Some people are misinterpreting that to think that you shouldn't ever give anybody access to any source code. They will clear that up.
    - Concerns about having a single leader or leadership team with responsibility becoming a bottleneck.
  - Other Public Comments to Consider
    - Adding a new practice on security documentation and guidance for implementers and users. Pieces of this are already in the SSDF, but this would bring them together and give them more attention.
    - Don't focus the SSDF on minimizing vulnerabilities – it should really focus on risk. You do need to reduce vulnerabilities to reduce risk in the framework of the SSDF. If you were developing software, especially for other parties, you don't know what their risk appetite is. You don't know what controls they're going to have in place. You need to focus on reducing vulnerabilities and designing things in a secure way. They may need to tweak some wording on that.
    - Not enough discussion of "resilience."
    - Not enough discussion of insider threats.

- Next Steps
  - Finish adjudicating public comments.
  - Revise the SSDF and get stakeholder feedback.
  - Either publish as final or do a second public comment period.
  - Continue to encourage standards, developers, and others to add reference mappings.
  - Consider developing appendices with more specifics for particular scenarios.
  - Consider establishing an NCCoE project that would develop examples of solutions that follow the SSDF and the E.O. recommended practices.
  - Next Steps for EO 14028: Artifacts and Attestation
    - All 4(e) clauses involve artifacts or attestation.
    - Already added "evidence" and "artifacts" to some SSDF tasks and examples.
    - Solicited feedback on the topic in the SP 800-218 Note to Reviewers.
    - Addressing this in a separate guidance document.
      - Shifting the mindset from generating artifacts for each release to generating artifacts for how development is done: processes, automation, etc.
      - Emphasizing the value of self-declaration and attestation.

- Discussion
  - Ms. Fanti asked about SBOM and if there is any discussion of what to do with that information once you have it.

Ms. Scarfone said they do not talk about that in the SSDF, but they do point to the NTIA document on SBOMs.

Mr. Souppaya added that the goal is to be able to showcase practices. There are a lot of other components that need to be brought into place to take advantage of SBOM.

- Ms. Fitzgerald-McKay noted that the SSDF is focused on what a vendor needs to do to prove the security of their development. What consumers do with the security artifacts would be a valuable addition to this work.
- Ms. Moussouris asked if there are plans to add anything about the time it takes to decide what components to include and perform all the checks. By the time you are ready to implement, the security posture of those components has changed. What do you do in that situation?

  Ms. Scarfone said they talk about making sure you are monitoring at all times and constantly looking for vulnerabilities in the components of your software and any dependencies your software has. The implementation detail is out of their scope.

  Ms. Moussouris said the guidance to constantly check for vulnerabilities means you will probably always find them and never be able to build anything. Is there some kind of language that talks about how to manage risk around those decisions and notes that you will have to make a trade-off at some point?

  Ms. Scarfone said they talk about making risk-based decisions but not about how to do that.

  Mr. Souppaya said if you think of the SSDF as a catalog of security practices, they are trying to provide a single document for people to review all these practices. They always go back to some of the high-level recommendations – the notion of risk-based, continuous monitoring of the landscape. Maybe an organization could define its risk appetite from classes or vulnerabilities that they want to mitigate, and they would have tools and capabilities on their toolchain to continuously make sure that what they developed yesterday and shipped is still in the shape they're trying to achieve. Then they would have automated tools to identify that and go back to root cause. NIST would like to understand how an organization is integrating these practices as part of the day-to-day operation.
- Mr. Groman said that gets to the rub with all of these documents and publications. As brilliant as they may be, at the end of the day someone at some level must make a risk decision, identify risk, and accept it. Nobody at any level wants to own the risk. Who bears the responsibility for the liability that will arise? That is not happening in a systemic, thoughtful way. It’s people bouncing risk around. It has to come from the top, not from a CIO or a CISO. It is the board of a directors at a company or a secretary in government.

  The Chair said it is being done implicitly because people are operating.

  Ms. Moussouris said there’s risk acceptance in practice but no risk ownership.

  Mr. Groman said that security, if implemented correctly and thoroughly, is difficult. We can’t say security should be easy. It’s not going to be. What [the SSDF] does, if done effectively, is highlight all the potential risk and vulnerabilities, and enable people to make informed decisions. That's what the framework does. Taking it from inference or implicit to a concrete understanding of the risks we're owning is a big part of this. The documents are outstanding and hit all the points.

Mr. Souppaya said they have received a lot of feedback from the community in general. He personally believes that there are a couple of innovative companies that are starting to implement, automate, and orchestrate the things Mr. Groman refers to. They are presenting that data in a very actionable way for decision makers. It is hard for NIST to be able to compose that as a kind of turnkey solution. They are trying to make sure that they have the right ingredients or the right practices that they could leverage.

Mr. Groman said NIST can’t give the acceptable level of risk. NIST can provide the tool, but making the decision on the acceptable level of risk will never be a NIST document.

Mr. Stine said a NIST document can’t give the answer but can lay out the considerations, the pros and cons organizations should consider, and the information they need to make a more informed decision. A follow-on to that is how you take advantage of technology and automation to help improve the quality or speed of the decision-making process. Are they producing resources that are the most useable to help organizations put these practices in place? If risk management is an area the Board wants to spend more time on, they could delve into the pain points at a future meeting. Both the public and private sectors are challenged by this. What are the best practices that leading organizations are putting in place from a risk perspective, and how do we incorporate those into the resources and institutionalize them across agencies, sectors, and organizations?

The Chair said this is an important topic. One of the things they are looking at in the context of SP 800-161 is the fact that you do this process, get this evidence, and then dump it on the desk of the CISO at Veterans Affairs or HHS, and the next question is, what the heck do you do with that? That is inherently a translation process. The SSDF is high level because it has to be, and yet bad consequences happen because of a few lines of buried code. He said this would be a good topic to follow up on at a future meeting if they can figure out who to invite and get a diverse set of perspectives.

Ms. Miller said it may be beneficial to talk to the CISO Council to get their take on this because of the diversity and complexity of missions across government. There will be a range of solutions. She would be leery of laying out a plan that says everybody will do this, without consideration for the diversity, but the CISO Council would be able to offer good insight.

Mr. Stine agreed and said they would want to reflect the diversity of mission, business objectives, and risk tolerance.

Ms. Moussouris asked if the document contains the idea that, at some point, risk will have to be accepted. Since we know that at some point risk will have to be accepted, you have to have a mechanism for tracking not only the accepted risk but also the operational reasons or assumptions why – the security assumptions that led to that decision, led to that exemption of the rule. The critical decision making that caused them to make the risk acceptance decision in the first place is something NIST documents should be able to tell them, without being prescriptive of the level of risk.

Mr. Groman said the RMF and the Privacy Framework direct agencies to address enterprise risk at the top level. You want consistency in how risk is assessed across an enterprise. But different agencies, or companies, or divisions within a single entity have different missions, with different kinds of data and different technology and will therefore have to make different decisions. You should get a sense from the top of how much risk an entity is willing to absorb and then have a methodology for applying that across the board, taking into account contextual factors in mission and the like.

Mr. Stine asked how they integrate cybersecurity risk into the broader enterprise risk umbrella. Because you're managing cybersecurity risk, or privacy, or supply chain, alongside reputation, finance, safety, operations… Are they providing that information in a way that will be meaningful to the broader enterprise risk decision makers who have to balance it across all those different domains?

The Chair noted that they were running behind schedule and recessed the meeting for a 5-minute break.

Crypto Agility Project at NCCoE

William Curt Barker, NIST Associate; William Newhouse, ITL, NIST

- Migration to Post-Quantum Cryptography (PQC) Project
  - Collaboration with industry participants
    - Product developers and service providers
    - Standards development organizations
    - Service providers and major user organizations
    - Government organizations, including DHS
  - Discovery of where public-key cryptography is used

    One of the things they are trying to learn to do better is help their customers understand how to carry out their advice. When they start talking about migrating to new algorithms – something that tends to take 10 to 20 years – if they want it to happen in a fairly timely manner they are going to have to understand the factors that go into organizations' roadmaps as they change. They are not going to know what to change unless they can actually discover where they are currently using public-key cryptography, which is far more pervasive than we might anticipate.

    They are finding some lessons learned from organizations like the Army, which is still trying to work out how they are going to go from RSA2048 to RSA4096 before the 2030s.
  - Prioritization
    - Figuring out how to communicate areas of need. Whatever NIST needs to add to the messaging to get organizations to think about this migration challenge.
    - Figuring this out for hardware, firmware, and software, with a lot of different protocols.
  - "Identification of need

    Step one is identifying and employing discovery tools. A companion step is working out what the other aspects of the roadmap are. How we are going to utilize the new algorithms in our protocols? What is this going to do to TLS? What does hybrid mean? Do we look at doing certificates that have keys for both the legacy algorithm and the new algorithm, or is that creating an extra step that is not only unnecessary but may actually slow down the migration?

- Timeline
  - Describe the problem: They already published the Federal Register notice.
  - Form the team: They are currently at this stage. People submitted letters of interest, and now they need to ask them what they're thinking about bringing.
  - Design: An iterative process that they will do at least a couple times.
  - Build Plan
  - Build
  - Document
  - Outreach
- Next Steps

  They will continue to communicate the project status, tell people where they stand, and then bring the team together. After that, they start developing guidance and documents, and then continue to do this over and over again in the 7 to 18 months that follow.

- Discussion
  - Mr. Venable asked what they are doing to reach out to other standards bodies. There is inevitably work going on to set standards that may be mistakenly building in different assumptions about how cryptography should be used. Will there be a concerted effort to work with the IETF and the 5G/6G standards groups to make sure they're building in crypto agility? Not just the ability to accept the new PQC algorithms, but crypto agility in general, and enabling those new standards to be accepting of many different types of evolution of PQC?

    Mr. Barker said they are pursuing it to different degrees. They are monitoring what the IETF is doing. They are receiving interest from international and other national standards bodies. The challenge is that they are going to be basing this on the algorithms they publish in the standards. There will be a desire on the part of some international players to suggest something else, but so far the interactions are promising that that is not going to be much of a problem. When talking about some of the other communications standards in the 5G space, the answer is yes, they are going to be exploring that but aren't as far along as with the internet standards.

    Mr. Venables said he is most nervous that there would be a group somewhere setting standards, and if we can find them and get them to set crypto agile standards then we will be ahead of the curve.

    Mr. Barker said he takes the point that they are going to have to be proactive in creating interactions.

    Mr. Scholl said members of the team are participants in the groups. The focus is on IETF, ANSI and ISO. They will reach out through their standards office to other standards bodies.
  - Mr. Venables said an additional point is that this is kind of a Y2K problem in some respects. There is a surprising amount of hard-coded assumptions baked into application layer protocols in various industries and end-user applications. There are a number of different sectors, whether it's energy, health, or finance, that have solid hard-coded assumptions in protocols that are embedded in business applications. When you think about crypto agility, it's not just about ensuring people adopt the new algorithms, it's also ensuring that they insulate themselves from algorithm-specific dependencies higher up the stack. Many companies are going to have to crack open applications

like they did in a Y2K sense and look for these dependencies. We are also going to have to reach out more forcefully to the sector-specific agencies and align with what they need to be doing on driving crypto agility in their industries. He recommends two streams, PQC work and crypto agility work.

Mr. Barker said they are also somewhat concerned with respect to the handshakes associated with both the establishment for the new algorithms and the role that it plays in the establishment. They learned a long time ago in fielding new algorithms that getting the algorithm right the first time is in some ways the easy part. The hard part is getting it used in a secure and responsible manner. There are a lot of hard-coded dependencies which have to be one of the foci of the discovery activity at the NCCoE, helping people identify what the dependencies are and trying to identify tools that may make that a little easier. Trying to do it manually is going to be possibly a fool's errand.

Mr. Venables asked if they have designated contacts in the sector-specific agencies who are the focal point on the crypto agility work.

Mr. Newhouse said there is a Sector Coordinating Council and a Cross-Sector Coordinating Council that brings the government leads. It also brings industry leads, and then it brings them together as well.

Mr. Barker said the SSAs are more mature in some sectors than in others, but that is one of the areas in which they are trying to coordinate with DHS.

Mr. Scholl said they want to be sure to do this right for the quantum effort as well because without an actual cryptographically relevant quantum machine, they are still not quite sure what actually could be exercised. It is not insane to think that we might have to do another flip migration to another set after something is learned, after a machine comes online. The common joke that they try to avoid is, "Building Tomorrow's Legacy Today."

- Ms. Moussouris said that for interoperability purposes, there will be legacy-supported cryptographic algorithms for quite some time. This outreach is supply chain based, and it needs to include some guidance on how to end-of-life your interoperability because it tends to expose one to a very long tail of cryptographic downgraded attacks.
- The Chair asked if the NCCoE project is bringing in sectors other than the tech industry, such as finance or energy.

Mr. Newhouse said there is strong intertest from the financial services sector. They probably need to make a concerted effort to use DHS mechanisms to get into those places.

The Chair said the awareness of post quantum is probably strongest in the big tech industry.

Mr. Newhouse said the Cloud Security Alliance has a quantum working group that put out a paper in this space, and they're not the only ones. A landscape survey is important because they may not need to restate it, but just affirm it. He would like to publish on a pretty regular cadence for this project, just to keep the awareness angle going.

Mr. Barker said end of life for interoperability is a real concern with respect to some of the financial entities. The data is a privacy issue, a business issue, and a liability issue. There are glib approaches they could voice that are simply not practical, such as decrypting and re-encrypting. They have always advertised that the center of gravity of expertise lies in the private sector. They need the inputs from private sector collaborators to even understand the problems they’re facing.

- The Chair said it is worth considering the SSDF as a tool. It is not only building things to be feasible with the new algorithms and new key lengths and so on, but also understanding ways to integrate so you don't introduce software vulnerabilities that get you fallback attacks and other things we have experienced in the past.

  Mr. Newhouse agreed. A lot of the NCCoE projects have been focused on the functionality of adding more security, not necessarily on being able to measure how much you had to begin with. For this one, they are going to need to be more particular and take advantage of the other publications on systems security engineering and proper software security development.

  Mr. Barker said that in the field of cryptography it is really easy either to make an implementation error or add an embellishment that undoes everything you were trying to accomplish.

  Mr. Newhouse said they are still accepting letters of interest. Please encourage people to reach out. If someone has an open source tool that does some discovery, students at universities can start playing with it and you start growing a community that leads the thinking in this space.

  The Chair said to let them know if there's anything the Board can do to help the project get the support and awareness it needs.

The Chair recessed the meeting for a lunch break.

EO 14028 Section FedRAMP Updates

Brian Conrad, Acting Director, FedRAMP, GSA

Mr. Scholl restated that as a federal advisory committee, ISPAB is subject to the Federal Advisory Committee Act rules. One of those rules is getting consensus advice from this Board, so while the audience is certainly welcome to observe, participation is limited to the vetted and cleared Board members. The audience is reminded to leave their video and mic off.

The Chair welcomed Brian Conrad, Acting Director for FedRAMP, to discuss program updates.

- Update to the NIST SP 800-53 Rev.5 Control Baselines for FedRAMP
  - Overview of Rev.5 Transition Schedule
    - The control baselines were finalized in September of last year, and that's where FedRAMP's work began to make sure that the baselines were brought into FedRAMP. They work closely with the Joint Authorization Board (JAB) to add additional controls to what is published by NIST that makes it more applicable to the commercial cloud service providers.
    - They are going to have a 90-day public comment period and also reach out to different stakeholder groups about what they are seeing in the baselines and any concerns that they may have.
    - After that, they will go into the adjudication process, which they anticipate will take two to three months. In that time, they will also update and finalize an abundance of documents that need to be updated or changed to reflect NIST 800-53 Rev.5 and the associated controls.
    - They will release the baselines as finals after sign-off from the JAB and the CIOs of DHS, DOD, and GSA. Once they release the baselines, they will also be releasing the transition plan for commercial cloud service providers to make the switch from Rev.4 to Rev.5.
    - The transition will take 6 months to a year, and there will be overlap where commercial cloud providers will be on the Rev.4 baselines and moving to the Rev.5 baselines. It depends on when their annual assessment falls, the size of the organization, the complexity of their

system, etc. They understand that this is not an easy change to make, and so the plan is to have significant runway for the commercial cloud service providers.

The Chair asked when SP 800-53 Rev.5 was released.

Mr. Conrad said in September of 2020, but the test case workbooks are another story. One of the conversations they need to have is about how to be more agile with this process.

The Chair asked if there has been input from cloud providers on what would facilitate a more agile process.

Mr. Conrad said no. The focus is getting the baselines crafted and out for public comment, and then they will have an opportunity to look at internal processes to figure out how they can do it better.

- Rev.5 Baseline Development
  - FedRAMP has worked with NIST and .govCAR to create a threat scoring methodology against the controls. Typically, when the baselines are made, they have the NIST published baselines and then the JAB adds on controls that they feel are necessary for commercial cloud service providers to meet in order to protect federal information in the cloud.
  - The controls are scored against the MITRE ATT&CK framework on their ability to protect, detect, and respond to real-world threats. They took this threat-based framework – this defensible mathematics-based methodology against the traditional controls that JAB typically puts on top of the NIST published baselines, and that is the delta between what NIST publishes and what the JAB usually includes.
  - They have kept the delta controls that have a protection value in the top 80% of the controls scored and removed the delta controls where the protection value was in the bottom 20% based on this methodology. They released a whitepaper on this methodology about six months ago.
  - As a result of applying this threat-based methodology, they have been able to reduce the net number of controls in the FedRAMP baseline – not the NIST baseline but the FedRAMP baseline, which includes the NIST baseline plus the JAB-added controls. The only corollary is the low baselines where the SP 800-53 Rev.5 catalog actually added controls to the low baseline. They did not do anything there.
  - They have reduced by about 21 for the moderate baseline and by about 30 or 40 for the high baseline. In total, there is a net reduction in the number of controls that cloud service providers are going to have to meet for the FedRAMP baselines because they applied the threat-based methodology to make sure that the critical controls with a protection value in the top 80% are incorporated.

- Discussion
  - Ms. Miller asked if they are giving any consideration to the CSPs going through the FedRAMP process now.

    Mr. Conrad said no because they are still using Rev.4.
  - Mr. Scholl asked if there were NIST baseline controls that should be considered for either reducing where they are in the baselines or moving to an optional. Is that something worth NIST and GSA or NIST and FedRAMP having discussions about?

Mr. Conrad said they are open to having conversations with NIST about applying this methodology to the catalog.

- The Chair asked about the EO's impact on FedRAMP.

  Mr. Conrad said there is a series of specified tasks in the EO.

  - They want to increase transparency between tasks to automate the FedRAMP program as much as they can. They have been working very closely with NIST in the development of OSCAL [Open Security Controls Assessment Language] to allow stakeholders to generate security artifacts and transmit them.
  - They are hoping to move away from the 600- to 800-page Word document and have it in a form that can be easily generated and automated. Part of the development of OSCAL is having the automated validations in place so CSPs, 3PAOs, and agencies can run automated validations even before sending their packages or do the automated validations even before sending it to the government.
  - Part of the strategic initiatives for FY22 is to understand that they need to look at internal business processes as well.
  - Communication with stakeholders and providing training to stakeholders are things they do on a consistent basis. The EO asks them to be more stakeholder-focused in development of training. The agency liaison program is something they stood up in the summer of last year where there's a designated subject matter expert on FedRAMP at each agency. The EO asks them to automate communication with stakeholders.
  - The other place where automation will pay off is on the JAB side. CIOs and DHS, DOD, and DOJ each provide a team to do the initial assessments and the continuous monitoring of the cloud service offering packages to come through the JAB side. They select only 12 a year because that is as much as the current JAB teams can handle. If they could spend an equal amount of time doing initial assessments and continuous monitoring, it would increase the throughput of the JAB pipeline.

- The Chair asked about the assessment process. How far into the weeds is everything authenticated? Do they look at a control and see if it is met – that the router ACLs are in place, and if someone tries to ping this port they get no response?

  Mr. Conrad said that is why they have the third-party assessment program in FedRAMP. It's the third-party assessors that do the assessment on the commercial cloud services. When they do a kickoff meeting during initial assessment for a cloud service offering, they get a brief on their architecture, their data flow diagrams, the discrete authorization boundary that they're bringing to FedRAMP for an authorization. The review teams from the JAB see these diagrams, digging through the SSP, and looking at control implementations. But they are also getting a security assessment report from the third-party assessors, who have done things like the social engineering, the phishing attacks, and other pen testing associated with that security assessment report.

- The Chair asked how it works operationally. Would a federal agency be better off from a security perspective going with a FedRAMP CSP than building their own data center and deploying their own computing environment?

  Mr. Conrad said the push across the federal government is cloud, and there is a wide variety of offerings available. The value proposition of FedRAMP is that somebody has already done the assessment work for you. They are trying to look at ways to grow the marketplace to get more vendors in. Roughly 30% of the offerings in the FedRAMP marketplace are small business, but that's not to say there aren't barriers still.

- The Chair asked if an agency would expect a significantly lower probably of a security incident by going with a FedRAMP provider than if it attempted to set up its own IT.

  Mr. Conrad said vulnerabilities are discovered all the time, and if you use a system that was given a provisional authorization from the JAB the continuous monitoring is being done for you. There are requirements for cloud service providers to meet a certain standard in addressing vulnerabilities. If a cloud service offering gets an authorization from an agency, it is a FedRAMP authorization that way. Each agency is responsible for doing continuous monitoring. You can get the package from FedRAMP and look through it to see if the level of risk that's been accepted is good enough for you. If there's something you don't like, you might ask the CSP to add additional controls to satisfy your risk appetite.

- Ms. Miller asked where they are on the call for reciprocity between FedRAMP and CMMC.

  Mr. Conrad said FedRAMP is funded by the Federal Citizens Services Fund, and so they authorize commercial cloud services for use by federal entities. They also look at the discrete authorization boundary that a vendor brings them and authorize that service, but they do not look at the whole company per se. There are a couple things that would preclude reciprocity between CMMC and FedRAMP. They don't have any agreements in place, mostly because of those factors.

- Mr. Scholl asked about challenges in the new privacy controls that are added into Rev.5.

  Mr. Conrad said he doesn't really see any issues there. FedRAMP is providing a standardized baseline and agencies can ask commercial cloud service providers to implement additional controls. They have seen that with regard to personnel. There are agencies who say they want to have restrictions on who is dealing with their data. They can ask the CSP to implement that restriction, and they will do the testing on those controls before they sign their ATO.

- The Chair said he may ask Mr. Conrad to come back in a year or so and talk about how the experience has been with the Rev.5 roll-out and the EO.

  Mr. Conrad said he would be delighted.

Update to FIPS 201-3 Revision and Identity Mechanisms

Hildegard Ferraiolo, ITL, NIST

- Overview of Changes
  - They have finished the FIPS 201-3 revisions, and the package is collecting signatures and approval. OMB has seen it. It is hard to say when it will be published.
  - Homeland Security Presidential Directive 12 was issued in 2004 to create a common ID standard for federal employees and contractors for accessing federally controlled facilities and federal information systems.
  - Results: Achieving an increased level of government efficiency.
    - A standard, interoperable credential: the PIV credential

        - Consistent process for identity vetting and proofing: These processes are accredited by department and agency as well.
        - A common, secure approach for accessing facilities and networks.
        - An increased level of government efficiency.
    - One Revision at a Time
        - Incorporate lessons learned from stakeholders (departments, vendors, integrators) throughout all the revisions.
        - Update based on technological advancements (mobile devices, etc.)
        - Align with new policy (e.g., OMB, OPM)
    - FIPS 201-2
        - Specified derived PIV Credential for Mobile Devices
            - Embedded or removable derived PIV Credential
            - A PKI-Credential – 2-factor authentication
            - Specified in SP 800-157
    - FIPS 201-3 Goals
        - Align with NIST SP 800-60-3 requirements and terminology (new digital identity guidelines). (-4 is currently being worked, and next year there may be a draft.)
        - Support government-wide ICAM policy and guidance
        - Adapt to current best practices and provide flexibility to meet future agency needs
- Major Updates
    - Authenticators
        - Support new authenticators as derived PIV credentials at AAL2 and AAL3 (phishing resistant authenticators become increasingly important).
        - Allow derived PIV credentials on additional platforms – They opened up derived PIV credentials to allow any kind of AEL or AEL 3 tokens or authenticator with the caveat that certain kinds are likely out. More and more, platforms do not support smart cards. Real estate is expensive and therefore derived PIV credential is the way to go for these platforms.
        - Revision 1 of SP 800-157 to specify details. Projected to have a draft out next year.
    - Federation
        - Facilitate interagency interoperability and trust (facilitates use of SAML/OpenID Connect; simplified support on relying parties). Many departments and agencies already use federation in one way or another and single sign-on mechanism using SAML or OpenID Connect.
        - More details in new SP → SP 800-217
    - PIV cards will remain primary authenticator – about 5 million in circulation today
    - Identity Proofing/Issuance
        - Align with SP 800-63-3 – Digital Identity Guidelines
            - Follow IAL-3 processes for PIV Card credentials
            - Allow for supervised remote proofing at identity assurance level.
            - Post-issuance binding for derived PIV credentials
            - SP 800-79 will be updated to reflect issuer controls for PIV card/DPC issuer
    - Physical Access Control

    - Removal of CHUID authentication mechanism
    - Addition of SM-Auth as optional Authentication mechanism
    - Deprecation of VIS (not accurate) and SYM-AK authentication mechanism (not scalable)
    - SP 800-116 Revision 2 to reflect FIPS 201-3

      Ms. Fanti asked about PIV cards that can be removed from mobile devices and if they would be like a secondary SIM that sits adjacent to the initial SIM card.

      Ms. Ferraiolo said that is doable but they have not seen implementations like that. Mostly they see it either implemented in the software or the hardware. They have seen some uptake on using a USB.

  - PIV Identity Account (M-19-17 motivated)

    They had to stop thinking about card management and take a more holistic view of credential tools. They should move more toward an enterprise-wide identity system.

- PIV/DPC Lifecycle
  - PIV Registration/Issuance
    - Create the PIV Identity Account in IDMS
    - Create a PIV Card
    - Bind the PIV Card to the account
  - Registration of Derived PIP Credentials
    - Bind to PIV identity account after successful authentication with PIV credential
    - Managed by cardholder’s home agency
  - PIV Credential Usage
    - Direct or federation between systems/agencies
    - Federation required to use non-PKI authenticators as DPCs
  - Termination of Credentials
    - Revoking PKI certificates, as appropriate
    - Unbind/invalidate PIV credentials in PIV account
- Major Goals/Updates
  - Facilitate stronger, centralized ID management
  - Maintain high assurance identity proofing.
  - Increase flexibility to accommodate emerging use cases and architectures
  - Focus on federation for interoperability and interagency trust
- More Work Ahead

  They are currently working on a host of special publications that go with the new revision. The details of the changes will be in the special publications. The effective time periods are dependent on when the special publications are released.
- On the Horizon: Zero Trust Architecture (ZTA)
  - ZTA
    - Move to SSO and application-level protection/authentication and

    - De-emphasize perimeter-only protection
  - ZTA and PIV
    - PIV can provide solid identity as an essential building block for ZT implementations
    - Centralized IDMS is key.
- Discussion
  - The Chair asked whether, regarding physical access, there will be a transition to using a phone to get into a federal facility.

    Ms. Ferraiolo said she doesn't envision this. Card readers and infrastructure talk a certain language. New technology often means two-way communication. They are currently trying to do PKI-based authentication on the gate or door reader. There are successes there. The reading of a number there needs to be changed on the back end. It is usually an expensive piece to replace.
  - The Chair asked about PKI and post quantum.

    Ms. Ferraiolo said post quantum is something they keep their finger on. Some of the PIV card credentials are 112 bit crypto. Next year it will be updated to 128 bit. Assuming there is a reliable algorithm in quantum, they will take it and make it quantum resilient.

    Mr. Scholl said this is a big use case for quantum.

    The chair asked if there is a candidate algorithm where success is plausible?

    Mr. Scholl said yes
  - Mr. Scholl asked if anyone using derived PIV in mobile in the US government.

    Ms. Ferraiolo said Treasury and Census are using some for mobile devices. Census was particularly interested because of their survey and the explosion of workers that they have to go door-to-door. The DOD has looked into it too, and they also deploy some.

    Ms. Miller said they found it very burdensome, so it's not a widespread use.

    Ms. Ferraiolo said DOD initially tried to use the mobile device with the PIV card. But it required a PIV card to be close to the mobile device for it to work. Why create yet another credential when you have something on the PIV card that can work? That went away, and the NSA then evaluated it and said that they're going with embedded credential on the card.

Final Board Reviews, Recommendations and Discussions

- Meeting Dates for 2022.

  The Chair said an email with potential meeting dates for 2022 was sent around the week before.

  Mr. Groman said the March date will not work for him.

  Ms. Miller said the March date will not work for her.

  Ms. Moussouris said the June date might not work for her.

  The Chair suggested the week of July 11.

  Mr. Scholl asked about shifting the June date to avoid the July 4th holiday and about shifting the March date as well. They will propose shifted dates for March and June.
- Letter on EO Implementation and Prioritization of Tasks

The Chair had sent around a revised letter, incorporating members' input, especially Mr. Groman's. The Board has three options: 1) Send the letter with minor revisions; 2) take another cut at drafting the letter; or 3) drop the whole thing.

Ms. Moussouris said she liked the revisions but is struggling with how to be both more and less prescriptive about prioritization. She would add one line stating the importance of prioritizing tasks with proven good security outcomes.

The Chair said that sounded like a good addition

Ms. Miller said she liked this version better than the previous one because it makes the overarching entities responsible for providing more context and insight, which the agencies are probably looking for as well.

The Chair asked Ms. Moussouris to write the additional line and then he would send it around to the members. He asked for agreement from the Board. There were no votes opposed.

- Topics for Future Meetings
  - Legislative/Policy Update

    Ms. Moussouris asked about the Congressional staff session that was cancelled and whether it could be rescheduled at a later meeting.

    Mr. Scholl said they try to bring in Congressional staff semi-frequently. They will attend the next meeting. He is also hoping to hear from National Cyber Director Chris Inglis and Laurie Locascio, incoming NIST director, at a future meeting.

  - FISMA and SP 800-53 Compliance

    The Chair said he has had discussions about including a session on FISMA and SP 800-53 at a meeting next year.

    Mr. Scholl said the ideas he had jotted down for future meetings includes Risk ownership/tolerance; AI Risk Management Framework; Agility and standards bodies; Crypto brittleness; Communications to sectors on pending transitions; Automation

    Ms. Miller suggested timing the FISMA discussion so the Board could shape or influence the next round of Congressional hearings on it.

    The Chair said it would be good to get input from agencies that have to comply with FISMA before talking to policy makers.

    Mr. Groman asked that when they reach out to speakers about FISMA to be sure they can address the privacy metrics also.

  - Useable Security

    Mr. Romine asked if the Board was interested in an update on the Useable Security program.

    The Chair said it would be good to be aware of it and how it is being translated into application.

    Ms. Moussouris said a good overlay would be how it maps to Zero Trust.

  - Privacy Workforce Initiative

Mr. Groman said he wanted to follow up on the Privacy Workforce initiative and see if there is a role for OPM to take it another step. He would like to see a set of profiles for privacy professionals, similar to those in IT.

Mr. Scholl said that something was brought up about sending out the job series through OPM to include privacy professionals, similar to what they had done for cybersecurity a few years ago.

- Update from NICE

  The Chair said he would like to hear an update from NICE and what they are doing to get cybersecurity qualifications out to the broader workforce.

- Ms. Moussouris asked what triggers special meetings of the Board like the one they had in September.

  Mr. Scholl said that the Board had made a decision that with all of the activities in the executive order with deliverables that were coming out prior to this meeting, they wanted to do a quick in-progress check of some of those higher-end items. It is rare to do this, but it has been done every now and then in the past. Online meetings make that kind of audible call to pull in a little bit easier. The only restriction is the publication in the Federal Register announcing the meeting.

The Chair thanked everyone for their participation and adjourned the meeting at 3:20 p.m. ET.

ISPAB – December 8 and 9, 2021		
Last Name	First Name	Affiliation
Board Members		
Baker	Brett	Nuclear Regulatory Commission
Fitzgerald-McKay	Jessica	NSA
Gattoni	Brian	DHS
Groman	Marc	Privacy Consulting
Hallawell	Arabella	NETSCOUT SYSTEMS
Lipner	Steve	SAFECode (Board Chair)
Maughan	Doug	NSF
Miller	Essye	Executive Business Management (EBM), LLC
Venables	Philip	Google
Fanti	Giulia	Carnegie Mellon University
Moussouris	Katie	Luta Security
NIST Staff		
Brewer	Jeff	NIST
Scholl	Matt	NIST
Carlson	Caron	HII
Salisbury	Warren	HII
McConnell	Andy	HII
Lurie	Kirk	HII
Speakers		
Romine	Chuck	NIST
Stine	Kevin	NIST
Tabassi	Elham	NIST
Lefkovitz	Naomi	NIST
Gilbert	Dylan	NIST
Dickson	Jessica	NIST
Homer	Jonathan	DHS
Smith	Angela	NIST
Scarfone	Karen	NIST Associate
Souppaya	Murugiah	NIST
Newhouse	Bill	NIST
Barker	Curt	NIST Associate
Conrad	Brian	GSA
Ferraiolo	Hildegard	NIST
Registered Attendees		
Anderson	Meghan	NIST
Anderson	Janet	NSA
Atkinson	Kathy	GSA
Bagley	Drew	Crowdstrike
Baksh	Marian	Government Executive Media Group
Beutel	Richard	Cyrrus Analytics
Boeckl	Katie	NIST
Cohen	Dylan	Committee on Science, Space and Technology
Cummins	Kevin	Zscaler Inc
Doubleday	Justin	Federal News Network
Friedman	Sara	Inside Washington Publishers
Fu	Kevin	University of Michigan
Fuller	Robert	Toggle Inc.
Funn	Kelby	SEC
Geller	Eric	Politico
Gugle	Anjali	Cisco

Heckman	Jory	Federal News Network
Heyman	Mat	NIST
Hodziewich	Nicole	Lockheed Martin
Jenkins	Mary Margaret	Deloitte
Johnson	Derek	Cyber Alliance
Leithauser	Thomas	Wolters Kluwer
Lynch	Devin	SecurityScorecard
Mahn	Amy	NIST
McElroy	Andrew	Ambit Inc
Mitchell	Charlie	Inside Washington Publishers
Querry	Randy	A2LA
Richardson	Shawn	NVIDIA
Sedwick	Adam	NIST
Shields	Robert	International Technology and Trade Association, INC
Smith	Denell	Cisco
Sokol	Annie	NIST
Souppaya	Murugiah	NIST
Starzak	Alissa	CloudFlare
Steward	Donna	Hi Trust Alliance
Stombler	Robin	Auburn Health Strategies
Throneberry	Saundra	Lockheed Martin
Tupitza	Charlie	RightExposure
Underwood	Rosa	GSA
Weinberger	Peter	Google
Wood	Jennifer	Luta Security
Yaniv	Orlie	Gigamon