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

November 6 and 7, 2024

Virtual Meeting Platform: Zoom for Government

Board Members	Board Secretariat and NIST Staff
Brett Baker, NARA	Matthew Scholl, Secretariat
Giulia Fanti, Carnegie Mellon University	Jeff Brewer, DFO
Jessica Fitzgerald-McKay, NSA	Kevin Stine, ITL Director
Alex Gantman, Qualcomm	
Brian Gattoni, Federal Reserve Board	
Cristin Goodwin, Advancing Cyber	
Marc Groman, Privacy Consulting	
Mike Duffy, CISA - DHS	
Steve Lipner, SAFECode	
Essye Miller, Executive Business Management	
Katie Moussouris, Luta Security	
Philip Venables, Google Cloud	

Wednesday, November 6th, 2024

ISPAB Meeting Notes - Day 1

---

1. Welcome and Opening Remarks

- Time: 10:00 A.M. -- 10:15 A.M.
- Speakers:
  - Steve Lipner, Chair
  - Phil Venables
  - Brett Baker
  - Katie Moussouris
  - Alex Gantman
  - Cristin Goodwin
  - Jessica Fitzgerald-McKay
  - Giulia Fanti
  - Mike Duffy

Details:

- Steve Lipner, Chair, ISPAB:
  - Opened the meeting and explained the Board's governance under the Federal Advisory Committee Act
  - Clarified rules regarding speakers, invited speakers, and guests.
  - Explained that guests are not allowed to speak during Board sessions but can participate during the public comment period.
  - Emphasized the importance of interaction with speakers during presentations.
  - Indicated there was one vacancy and one absent member, expecting 10 members plus himself.
- Board Member Introductions:
  - Phil Venables (Google Cloud CISO)
  - Brett Baker (Inspector General at National Archives)
  - Katie Moussouris (Founder/CEO of Luta Security, also on the Information Security Technical Advisory Council (ISTAC) at Commerce)
  - Alex Gantman (VP of Security Engineering at Qualcomm)
  - Cristin Goodwin (Founder and Managing Partner of Advanced Cyber Law, CEO of Advancing Cyber)
  - Jessica Fitzgerald-McKay (Lead for NSA Center for Cybersecurity Standards)
  - Giulia Fanti (Associate Professor at Carnegie Mellon, Electrical and Computer Engineering)
  - Mike Duffy (Acting Federal CISO at OMB, Associate Director at CISA)

2. ITL Update and Board Questions

- Time: 10:15 A.M. -- 11:00 A.M.
- Speakers:
  - Kevin Stine, Director, Information Technology Laboratory, NIST
  - Phil Venables, Google Cloud CISO
  - Steve Lipner, Chair, ISPAB
  - Cristin Goodwin, Founder and Managing Partner, Advanced Cyber Law; CEO, Advancing Cyber
- Details:
  - Kevin Stine:
    - Opened with a reflection on NIST's upcoming 125th anniversary in 2026, highlighting the organization's long history of advancing technology and metrology across various domains, including cybersecurity, biometrics, and applied mathematics.
    - Emphasized NIST's foundational mission of promoting innovation, advancing standards development, transitioning research into practice, and improving quality of life through technology advancement.
    - Provided detailed personnel updates, including the onboarding of Julie Chua as the new Applied Cybersecurity Division chief, ongoing

interviews for the Statistical Engineering Division Chief position, and the selection of a new ITL Chief of Staff.

        - Discussed the upcoming departure of Laurie Locascio as NIST Director in January 2025 to assume the role of President and CEO at the American National Standards Institute (ANSI), with Chuck Romine expected to serve as Acting Director until a permanent replacement is nominated and confirmed.
        - Detailed the current budget situation, explaining that NIST is operating under a continuing resolution through mid-December. The President's FY25 budget requested a $38.5M increase for NIST over FY24 but with no increase for cybersecurity and privacy programs specifically. The House mark proposed a $100M reduction from FY24 levels, while the Senate mark showed $10M less than the President's request, emphasizing the ongoing budget discussions and uncertainty at this stage.

- Provided programmatic updates on key focus areas and accomplishments since the last ISPAB meeting:
    - Post-Quantum Cryptography (PQC) standards:
        - Highlighted the launch of the first three PQC algorithm standards in August 2022, celebrated at a White House event attended by NIST leadership and the PQC team.
        - Outlined ongoing work, including drafting a fourth FIPS, preparing a proposed deprecation timeline, and collaborating with industry partners on transition guidance and implementation examples.
        - Shared examples of early industry adoption by major tech companies and plans for future chipset inclusion.
    - International standards engagement:
        - Announced a five-year, $15 million cooperative agreement with ASTM International to establish a center of excellence supporting U.S. engagement in international standardization for critical and emerging technologies.
        - Emphasized the center's alignment with national strategies and focus areas, including pre-standardization engagement, workforce capacity building, and industry-driven standards development.
    - Digital Identity guidelines:
        - Discussed the release of draft SP 800-63-4 for public comment, incorporating updated guidance on identity-proofing methods, digital wallets, and accessibility considerations.
        - Highlighted the broader impact of NIST's digital identity work on mobile driver's licenses, verifiable credentials, and government PIP modernization efforts.
    - Artificial Intelligence (AI) initiatives:
        - Referenced the release of four publications in July 2024 aimed at improving the safety, security, and trustworthiness of AI systems in support of the President's Executive Order on AI.

        - Announced a new $6 million cooperative agreement with Carnegie Mellon University to establish a joint center for AI testing, evaluation, and experimentation.
    - Internet of Things (IoT) developments:
        - Discussed the release of the IoT Advisory Board's report on barriers to U.S. IoT adoption and recommendations for establishing greater trust in IoT technologies.
        - Commended the work of the NIST IoT team in supporting the advisory board's efforts over the past two years.
    - Cybersecurity workforce and training:
        - Highlighted the award of $3 million in cooperative agreements through the NICE Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS) Cybersecurity Education and Workforce Development (RAMPS Program) to support cybersecurity education and workforce development initiatives in 11 states.
        - Emphasized the program's focus on engaging local communities and addressing regional workforce needs.
    - Cybersecurity Framework (CSF) 2.0 transition:
        - Provided an update on the expansion of CSF 2.0 resources, including the release of Quick Start Guides, translations, and a new introductory video during Cybersecurity Awareness Month.
        - Discussed ongoing efforts to promote adoption and share success stories from organizations and sectors leveraging the framework domestically and internationally.

 Staff recognition:

- Highlighted recent recognitions and accomplishments of NIST staff members:
    - The PQC team's receipt of the Cyber Scoop 50 Innovation of the Year award and their visit to the White House to celebrate the launch of the PQC standards.
    - Elham Tabassi's selection as one of the 50 most influential women in national security for her contributions to AI research and leadership.
    - Cherilyn Pascoe's recognition in the Cyber Scoop 50 for her government leadership as the NCCOE Director.
- Emphasized the importance of acknowledging and celebrating the hard work and achievements of NIST staff in driving impactful research and advancing the organization's mission.

    - Discussion Participants:
        - Phil Venables:
            - Raised concerns about resource constraints at NIST given the increasing demands for their expertise across various government initiatives and executive orders.

    - Questioned how NIST manages its workload and prioritizes projects in the face of constant new requirements and responsibilities.
    - Kevin Stine acknowledged the challenges posed by resource constraints and increasing demands, noting that each new requirement causes NIST to re-prioritize its efforts. In an ideal situation, new requirements would leverage existing work, allowing NIST to address them more efficiently.
    - He emphasized that while budget cuts pose challenges, NIST is prioritizing critical programs and leveraging partnerships to maintain its capabilities. Kevin assured the Board that NIST will continue to put its best effort into everything it is asked to do, working closely with industry experts to support its mission.
- Steve Lipner:
    - Acknowledged NIST's impressive track record of consistently meeting deadlines and delivering high-quality work despite resource constraints, noting that not all government agencies maintain similar performance levels under pressure.
    - Inquired about the specific budget implications and potential impacts of the continuing resolution on NIST's operations and ongoing projects.
    - Kevin Stine agreed with the observation, emphasizing that while NIST strives to meet deadlines and maintain productivity, it becomes increasingly challenging with each new requirement, especially when no additional resources are provided.
    - He acknowledged that aggressive timelines could take a toll on staff morale and program prioritization but assured the Board that NIST will continue to do its best to meet expectations while working closely with industry experts to support their efforts.
- Cristin Goodwin:
    - Commended NIST for recognizing the achievements and contributions of its staff members, expressing appreciation for the public acknowledgment of their hard work and expertise.
    - Emphasized the importance of highlighting these accomplishments to showcase the value and impact of NIST's work to both internal and external stakeholders.
    - Kevin Stine expressed his appreciation for the feedback, acknowledging that he always feels hesitant when presenting staff recognition slides, as he fears inadvertently omitting a deserving individual's accomplishments.
    - He committed to improving the tracking and recognition of staff achievements to ensure that all deserving individuals are acknowledged for their hard work and expertise, emphasizing the importance of showcasing the value and impact of NIST's work to both internal and external stakeholders, as it helps to maintain

morale and demonstrates the organization's continued relevance and effectiveness.

3. NIST Small Business Cybersecurity Program and Board Questions

- Time: 11:15 A.M. -- 12:00 P.M.
- Speakers:
    - Daniel Eliot, NIST Lead for Small Business Engagement, ITL, NIST
    - Jessica Fitzgerald-McKay
    - Cristin Goodwin
    - Steve Lipner, Chair
- Details:
    - Daniel Eliot:
        - Provided a comprehensive overview of his first year in the role, detailing the program's authorization under two legislative acts and the coordination efforts across NIST, government agencies, and the small business ecosystem.
        - Emphasized the program's focus on under-resourced organizations, including nonprofits and small school systems, aiming to expand awareness of NIST's role in innovation, create accessible content, connect efforts across NIST programs, and facilitate regular stakeholder communication.
        - Detailed the Small Business Cybersecurity Corner website, which houses approximately 100 resources from various government agencies, nonprofits, and industry groups. The site underwent a reorganization in 2024, adding four new sections and reporting a 10% increase in traffic over the past year.
        - Described engagement activities, including hosting six well-attended cybersecurity webinars, growing the small business community of interest to over 13,000 subscribers, holding quarterly meetings with owner/operator groups and vendor/resource partners, and participating in 24 external speaking engagements to promote resources and listen to challenges.
        - Discussed key publications, such as the CSF 2.0 Small Business Quick Start Guide, translations of materials in five languages, updated fact sheets on MFA and phishing guidance, and strategic blog posts during National Entrepreneurship Week.
        - Outlined plans for fiscal year 2025, including continuing the webinar series, planning an in-person event at the NCCOE, developing additional quick start guides, and revising NISTIR 7621 on small business information security fundamentals.

Discussion Participants:

- Jessica Fitzgerald-McKay:

  - Asked about the selection process and methodology for determining high-priority items and critical security measures for small businesses.
    - Daniel Eliot explained that the selection process focuses on items that are not a huge cost burden for small businesses and tasks that can be realistically achieved with minimal budget or cybersecurity expertise. The team also considers guidance from other agencies like CISA to ensure alignment and circulates materials within the small business community to gather feedback on the relevance and effectiveness of the prioritized items.
- Cristin Goodwin:
  - Inquired about the target audience, metrics for measuring program effectiveness, and potential framework adoption challenges.
    - Daniel Eliot clarified that the program primarily targets the CISO level, focusing on those responsible for implementing and communicating cybersecurity measures within small businesses. He acknowledged the challenges in measuring effectiveness, relying on website analytics, feedback from partners like Small Business Development Centers, and input from the small business community through webinars and other engagements. Adoption challenges are addressed by providing accessible, simplified guidance and resources tailored to the small business audience including "cut and paste" language samples for such things as RFPs.
  - Discussed the importance of community engagement and the role of MSPs and CSPs in supporting small business cybersecurity.
    - Daniel Eliot agreed with the importance of engaging Managed Service Providers (MSP) and Managed Security Service Providers (MSSP) as force multipliers in reaching and supporting the small business community. He emphasized the program's efforts to increase participation and awareness among these service providers, recognizing their critical role in delivering cybersecurity solutions to small businesses that often lack in-house expertise.
- Steve Lipner, Chair:
  - Questioned how the program segments and targets different small business sizes and what priority cybersecurity areas are identified for this diverse group.
    - Daniel Eliot acknowledged the wide range of small businesses, from single owner-operators to larger enterprises, and the challenges in segmenting this diverse group. He highlighted the use of the Cybersecurity Framework and its adaptability to various audiences as a key tool in communicating cybersecurity priorities. Daniel noted that according to SBA numbers, approximately 80% of small businesses are single owner-operators, which helps inform the focus of NISTIR 7621 and its revision. The program also focuses on specific sectors, such as manufacturing, through collaboration with NIST's Manufacturing Extension Partnership.
  - Discussed the challenges in measuring program effectiveness given the heterogeneous nature of the small business population and the difficulty in collecting consistent data across various sectors and sizes.

    - Daniel Eliot recognized the difficulties in measuring effectiveness across the diverse small business landscape. The program relies on website analytics, feedback from partners, and input gathered through webinars and other engagements to gauge impact. He emphasized the importance of the Small Business Cybersecurity Corner website as a central resource hub and the use of website traffic data as an indicator of program reach and effectiveness.
  - Emphasized the importance of providing clear, actionable guidance to small businesses and MSPs/CSPs, as they often lack the resources and expertise to navigate complex cybersecurity frameworks and requirements on their own.
    - Daniel Eliot agreed with the need for clear, actionable guidance tailored to the small business audience. He highlighted the program's efforts to create accessible, simplified resources like the Cybersecurity Framework Quick Start Guide, which provides prioritized actions and practical steps for small businesses to improve their cybersecurity posture. The program also engages with MSPs and Cloud Service Providers (CSP) to promote the adoption of these resources and best practices among their small business clients.
    - expertise.
- Phil Venables:
  - Emphasized the critical role of service providers in the small business ecosystem, noting that small businesses are essentially 'a loose flying collection of vendors' including not just technology providers but banks, payment providers, tax services, and merchant services.
  - Suggested exploring a 'secure by default' pledge similar to CISA's secure by design initiative, where service providers would commit to implementing secure default configurations. Venables noted that this approach would be particularly impactful since many small businesses rely on default settings and have limited ability to evaluate security features.
- Daniel Eliot:
  - Elaborated on his community engagement approach, explaining that communities of interest serve as the primary channel for gathering input and feedback. He described how these communities, which include over 13,000 subscribers, are structured into subgroups co-led by industry participants to ensure real-world perspectives are incorporated into NIST's guidance.
- Cristin Goodwin:
  - Inquired about communities that have proven difficult to reach and discussed potential strategies for expanding outreach to underserved segments.
    - Daniel acknowledged ongoing challenges in engaging certain segments of the small business ecosystem, particularly those without dedicated IT staff or security expertise.

4. Panel Brief on NIST Frameworks and Board Questions

- Time: 1:00 P.M. -- 2:00 P.M.

- Speakers:
  - Introduction and Overview, Rodney Petersen, ACD, NIST
  - Risk Management Framework, Victoria Pillitteri, CSD, NIST
  - Cybersecurity Framework, Stephen Quinn, CSD, NIST
  - Privacy Framework, Dylan Gilbert, ACD, NIST
  - Workforce Framework for Cybersecurity, Karen Wetzel, ACD, NIST
  - Alex Gantman
  - Cristin Goodwin
  - Marc Groman
  - Steve Lipner
- Details:
  - Rodney Petersen:
    - Introduced the panel discussion focusing on the alignment and harmonization of NIST's different frameworks. He explained that while these frameworks were originally developed independently of each other, efforts are now underway to align and harmonize them.
    - Emphasized that although each framework has its own unique scope and purpose, they are designed to be complementary. The panel will explore how the frameworks can be used together to address an organization's diverse needs while still meeting the specific requirements each framework was created to address.
  - Victoria Pillitteri:
    - Provided a comprehensive history of the Risk Management Framework (RMF), tracing its origins back to the Federal Information Security Management Act (FISMA) of 2002. She detailed how the RMF provides a portfolio of standards that were originally designed to help federal agencies fulfill their FISMA responsibilities.
    - Highlighted that while the RMF was created for federal agencies, it has seen voluntary adoption by academia, nonprofits, and national and international organizations. The flexibility of the RMF allows it to be applicable to all types of systems and organizations.
    - Summarized the key RMF documents including SP 800-37 (risk management methodology as mandated by OMB Circular A-130) and 800-53 (the cybersecurity control catalog).
    - Outlined the RMF program's priorities for fiscal year 2025 and beyond, including:
      - Issuing updates to key publications such as FIPS 200 and associated NISTIRs
      - Developing additional implementation and user resources to help organizations better utilize the guidance.
      - Collaborating with the CSF team on a CSF 2.0/RMF/ERM Quick Start Guide to help organizations understand how to use these frameworks together.
      - Making improvements to the SP 800-53 public comment website to enable real-time feedback on the controls catalog

    - Emphasized the RMF's ongoing harmonization efforts with the other NIST frameworks represented on the panel. By working collaboratively across these different programs, NIST aims to provide a cohesive and complementary suite of resources for managing cybersecurity and privacy risks.
- Stephen Quinn:
    - Discussed the extensive development process behind the Cybersecurity Framework version 2.0 (CSF 2.0), noting that NIST consulted with over 400 organizations and adjudicated more than 3,000 comments to ensure the updated framework incorporated diverse stakeholder feedback.
    - Highlighted key changes introduced in CSF 2.0, including the integration of enterprise risk management concepts and the addition of a new Govern function. These updates were driven by factors such as the need to communicate cybersecurity risk in the language of business executives and increased emphasis on cyber supply chain risk management.
    - Provided an overview of the implementation resources released alongside CSF 2.0, including a comprehensive Implementation Guide, Quick Start Guides, and a suite of tools to assist organizations in adopting and applying the framework. Translations of the framework into multiple languages have further expanded its accessibility.
    - Shared recent survey results indicating that 50-60% of organizations plan to adopt CSF 2.0, demonstrating continued growth in framework usage. Ongoing priorities include developing automated mechanisms to facilitate framework implementation and assessment, including work to automate mapping between frameworks such as between the CSF and 800-53 controls. The team is using an integrated database called the Cybersecurity and Privacy Platform (CPP) that contains mappings between all these frameworks and can accept external mappings to NIST frameworks, providing the data in JSON and Excel formats for automated processing.
- Dylan Gilbert:
    - Discussed the growth in both engagement with the Privacy Framework and the development of implementation resources since its initial release. Metrics tracking through tools like Google Analytics has provided insights into framework adoption and usage patterns.
    - Highlighted the program's international engagement efforts to promote the Privacy Framework globally and learn from different jurisdictions' experiences with privacy risk management. These collaborations have informed plans for the next iteration of the framework, Privacy Framework 1.1.
    - Provided an update on the progress of the privacy workforce public working group, which has grown to over 950 members worldwide. The group has developed a privacy workforce taxonomy aligning roles, tasks, and skills with both the NICE Workforce Framework and the Privacy Framework. A draft taxonomy is slated for release in early FY25.
    - Outlined cross-framework collaboration initiatives, including:

            - Development of quick start guides for using the Privacy Framework
            - Creation of a data governance and management profile
            - Development of an integrated privacy, cybersecurity, and AI risk management profile in partnership with the CSF and ERM teams
            - Work on implementation examples and community profiles showcasing real-world applications.
        - This work aims to provide organizations with practical guidance on managing privacy and cybersecurity risks cohesively while making the framework more accessible to different audiences.
    - Karen Wetzel:
        - Presented recent updates to the structure of the NICE Workforce Framework for Cybersecurity, including the introduction of competency areas, realignment of workforce categories, and revision of work role definitions to optimize the framework's applicability and use.
        - Detailed the expansion of the framework to include an additional 11 competency areas and over 80 revised work roles. These additions were developed through extensive collaboration with industry and government stakeholders to ensure the framework reflects the evolving needs of the cybersecurity workforce.
        - Highlighted the global impact of the NICE Framework, discussing its translation into multiple languages and the development of supporting resources to facilitate international adoption. Collaborative efforts with countries such as Japan, Brazil, and the UK have promoted consistent usage of the framework worldwide.
        - Outlined ongoing framework development priorities, including the definition of AI and data science competencies to address emerging workforce needs. Continued evolution of the framework through minor updates and working group activities will ensure its relevance and usefulness for the cybersecurity community.

Discussion Participants:

- Alex Gantman:
    - Raised the question of how the effectiveness of NIST's frameworks is being measured, underscoring the importance of empirical evidence demonstrating tangible security improvements resulting from framework adoption.
        - The panel acknowledged the challenges in measuring the effectiveness of frameworks, noting that while anecdotal evidence exists, quantifying the direct impact on an organization's cybersecurity posture remains difficult due to the multitude of factors influencing risk. They emphasized the ongoing efforts to develop meaningful metrics and gather empirical data to assess framework effectiveness, such as tracking adoption rates, conducting case studies, and soliciting feedback from users.

  - Discussed the challenges inherent in quantifying the impact of framework usage on an organization's cybersecurity posture, given the multitude of factors influencing risk. Developing meaningful metrics to assess framework effectiveness remains an ongoing priority.
    - The speakers recognized the complexity of attributing security improvements solely to framework adoption, as organizations' risk environments are influenced by various factors such as threat landscape, industry-specific requirements, and internal policies. They highlighted the need for continued research and collaboration with industry partners to identify and refine metrics that can provide a more comprehensive assessment of framework effectiveness while acknowledging the limitations and challenges involved.
  - Suggested that an interesting data point would be to hear from the NIST CISO on their organization's application of the frameworks.
- Cristin Goodwin:
  - Inquired about efforts to integrate MSPs and CSPs into the NIST frameworks, recognizing their critical role in many organizations' cybersecurity strategies. Ensuring the frameworks address the unique considerations of these third-party relationships is essential.
  - Goodwin highlighted a recent court finding about SolarWinds where 10-11 pages were dedicated to analyzing the company's application of the NIST Cybersecurity Framework, noting this level of detailed examination in legal proceedings creates potential disincentives for companies to give themselves accurate assessments if that data could later be subpoenaed and used in court opinions.
    - The panel discussed ongoing efforts to engage MSPs and CSPs in the framework development process, recognizing their crucial role in supporting the cybersecurity needs of many organizations. They highlighted the importance of incorporating guidance and best practices specific to managing third-party risks and ensuring the frameworks provide a consistent approach for evaluating and addressing security concerns in outsourced environments. The speakers also mentioned plans to develop targeted resources and case studies to help organizations effectively implement the frameworks in the context of MSP and CSP relationships.
  - Highlighted the specific challenges small businesses face in adopting NIST's frameworks, such as resource constraints and the need for tailored guidance. Continued development of resources like quick start guides and simplified toolkits is crucial to promoting wider framework usage among smaller organizations.
    - The panel acknowledged the unique challenges faced by small businesses in adopting cybersecurity frameworks, particularly in terms of limited resources and expertise. They emphasized the ongoing efforts to create accessible, streamlined resources tailored to the needs of smaller organizations, such as quick start guides, simplified toolkits, and online training materials. The speakers also highlighted the importance of collaborating with industry associations and local business communities to

raise awareness and promote the adoption of frameworks among small businesses.

- Marc Groman:
    - Discussed the evolution of the Privacy Framework and its relationship to the rapidly changing landscape of privacy legislation worldwide. Ensuring the framework remains aligned with emerging laws and regulations is critical to its ongoing relevance and usefulness.
        - The panel recognized the challenges posed by the constantly evolving privacy legislation landscape and the need for the Privacy Framework to remain aligned with emerging requirements. They discussed ongoing efforts to monitor legislative developments, engage with policymakers and industry stakeholders, and incorporate feedback to ensure the framework provides a flexible and adaptable approach to managing privacy risks. The speakers also highlighted the importance of maintaining a balance between the framework's voluntary nature and its ability to support organizations in meeting their compliance obligations.
    - Explored the intersection between NIST's frameworks and organizations' compliance obligations, emphasizing the importance of harmonizing risk management practices with legal requirements. Balancing the voluntary nature of the frameworks with the need for compliance is an ongoing challenge.
        - The speakers acknowledged the complex relationship between voluntary frameworks and mandatory compliance requirements, noting that organizations often struggle to align their risk management practices with legal obligations. They emphasized the need for continued collaboration between NIST, regulators, and industry stakeholders to promote greater harmonization and provide clear guidance on how the frameworks can support compliance efforts. The panel also discussed the potential benefits of mapping framework controls to specific legal requirements and developing case studies showcasing the successful integration of risk management and compliance activities.
- Steve Lipner:
    - Inquired about the current state of integration between NIST's different frameworks and the roadmap for continued harmonization efforts. Ensuring the frameworks provide a cohesive and complementary approach to risk management is essential to their collective success.
        - The panel discussed the ongoing efforts to align and integrate the various NIST frameworks, recognizing the importance of providing a cohesive and complementary approach to risk management. They highlighted initiatives such as the development of crosswalks and mapping documents, joint working groups focused on harmonization, and the creation of unified taxonomies and terminologies. The speakers also outlined plans for future collaborations, including the development of integrated case studies and guidance documents that demonstrate how the frameworks can be used together to address an organization's holistic risk management needs.

- Discussed common challenges organizations face in implementing the Risk Management Framework, such as the complexity of the control catalog and the resource-intensive nature of the assessment process. Continued refinement of implementation guidance and automation tools is necessary to reduce barriers to adoption.
    - The panel acknowledged the challenges organizations often encounter when implementing the Risk Management Framework, particularly in terms of navigating the extensive control catalog and conducting resource-intensive assessments. They discussed initiatives aimed at simplifying and streamlining the implementation process, such as the development of tailored control baselines, the creation of automated assessment tools, and the provision of more granular implementation guidance. The speakers also emphasized the importance of sharing best practices and lessons learned among the user community to help organizations overcome common hurdles and accelerate framework adoption.
- The panel engaged in a critical examination of framework validation, focusing on a fundamental question: Can we empirically prove that adopting these frameworks actually improves security outcomes?
- Alex Gantman challenged the group to move beyond assumptions, asking how organizations can track and validate whether security interventions genuinely lead to improved outcomes. He suggested that while many believe these frameworks are beneficial, there's a lack of concrete evidence demonstrating their effectiveness.
- The discussion revealed several key challenges:
    - Difficulty in isolating framework adoption as the sole cause of security improvements
    - Lack of standardized methods for measuring security outcome improvements
    - The complex, multi-faceted nature of cybersecurity risk management
- Marc Groman emphasized that frameworks like the Privacy Framework are not compliance checklists, but tools for understanding and managing potential risks. He noted that different organizations might apply the same framework and reach very different security outcomes based on their unique risk tolerances.
- The panel acknowledged that while frameworks provide valuable guidance, empirical validation remains elusive. They proposed several approaches for future research:
    - Developing more rigorous measurement methodologies
    - Creating longitudinal case studies tracking security outcomes
    - Establishing baseline metrics before framework implementation
    - Tracking changes in organizational risk posture and incident response capabilities

5. Software Metrics Presentation

- Time: 2:00 P.M. - 2:45 P.M.

- Speakers:
    - Paul Black, NIST
    - Steve Lipner
    - Alex Gantman
- Details:
    - Paul Black:
        - Opened the presentation by highlighting the fundamental challenges involved in developing meaningful software metrics. He referenced David Flayer's report "Mostly Sunny with a Chance of Cyber Doom," which underscores the difficulties in forecasting breaches and understanding the complex contextual factors influencing software security.
        - Emphasized three fundamental principles for approaching software security and measurement:
            - Limit the role of software: Organizations should carefully constrain software's scope and complexity, focusing only on essential functionality rather than expanding features unnecessarily.
            - Only build software that can be measured: Development should proceed only when clear, effective metrics can be established to validate and verify the software's behavior and security.
            - Accept failure: Acknowledge that failure is an inherent part of software systems and build appropriate resilience and recovery mechanisms accordingly.
        - These principles were presented as crucial guidelines that should inform both development practices and security assessment methodologies. Black emphasized that these form the foundation for developing more secure and manageable software systems.
        - Outlined three categories of useful software metrics: those related to the software development process itself, those focused on characteristics of the software product, and evidence gathered from the software's actual use in production environments. Each category offers valuable insights into different aspects of software security.
        - Provided an overview of various NIST initiatives and research efforts aimed at advancing software metrics. These include the Static Analysis Tool Exposition (SATE), which evaluates the effectiveness of static analysis tools in detecting software weaknesses, and the Software Assurance Reference Dataset (SARD), a comprehensive collection of over half a million test programs in multiple languages designed to support software metrics research.
        - Discussed NIST's work on artificial intelligence techniques for bug detection, highlighting the potential for AI to accelerate the identification of known software weaknesses at scale. The Bugs Framework (BF) project aims to develop a more rigorous and comprehensive taxonomy of software bugs.

    - Discussed the goal of the Bugs Framework research to develop a taxonomy of software bugs, similar to how the periodic table categorizes chemical elements. The intent is to identify the fundamental "atoms" of software weaknesses and failures.
    - Emphasized the importance of collaboration in advancing software metrics, citing NIST's ongoing partnership with the National Security Agency (NSA) to develop robust datasets for software analysis. These datasets, covering languages like C, C++, Java, and Python, provide a foundation for evaluating and comparing different software analysis techniques.
    - Presented examples of federal government initiatives and industry-led efforts focused on software metrics. The Department of Homeland Security's Software Assurance Metrics and Tool Evaluation (SAMATE) program and the CISQ Consortium for IT Software Quality were highlighted as key collaborations driving progress in this area.

Discussion Participants:

- Steve Lipner:
  - Inquired about the level of engagement and participation from static analysis tool vendors in NIST's SATE program. Understanding the extent to which these vendors are leveraging NIST's datasets and contributing to the development of evaluation methodologies is crucial to assessing the program's impact.
    - Paul Black acknowledged that static analysis tool vendors actively participate in the SATE program and utilize the datasets provided by NIST. He explained that these vendors often use the datasets to evaluate and improve their tools, comparing their performance against other participants. Black highlighted that while some vendors may express frustration with the limitations of the datasets, overall, they recognize the value of having a standardized benchmark and actively contribute to the program's development. He mentioned that NIST regularly solicits feedback from vendors to identify areas for improvement and collaborates with them to refine the evaluation methodologies. Black emphasized that the SATE program has become an important resource for the static analysis community, promoting transparency, fostering innovation, and driving the development of more effective tools.
  - Raised the question of dataset representativeness, emphasizing the importance of ensuring that the software programs used in metrics research accurately reflect the characteristics and complexities of real-world codebases. Striking a balance between controlled test cases and realistic software samples is an ongoing challenge.
    - Paul Black acknowledged the challenge of ensuring dataset representativeness in software metrics research. He explained that NIST strives to create datasets that balance the need for controlled test cases with the inclusion of realistic software samples. Black mentioned that the

SATE program incorporates a diverse range of software programs, including open-source projects, industrial codebases, and synthetic test cases designed to cover specific vulnerability classes. He recognized that achieving perfect representativeness is difficult, as real-world codebases often contain unique characteristics and complexities that are hard to replicate in a controlled setting. However, Black emphasized that NIST continuously works to expand and diversify its datasets, collaborating with industry partners and academic institutions to identify and include relevant software samples. He also highlighted the importance of transparency in documenting the limitations and biases of the datasets, allowing researchers and users to interpret the results in the appropriate context.

  - The Bugs Framework, in contrast, is specifically designed to be a structured taxonomy. It aims to:
    - Factor out common underlying characteristics of weaknesses.
    - Create clear relationships between different types of bugs.
    - Provide a systematic way to classify and analyze vulnerabilities.
    - Enable better understanding of root causes and relationships between different types of bugs.
  - This structured approach allows for more precise categorization and analysis of software weaknesses compared to CWE's more loosely organized collection of vulnerabilities.
    - Black emphasized that this fundamental difference in organization makes the Bugs Framework more suitable for systematic analysis and classification of software weaknesses. The difference between the Bugs Framework and the CWE is that CWE is not a structured taxonomy while the framework is intended to be.
- Alex Gantman:
  - Asked about historical approaches to software security testing and how they compare to the metrics-driven techniques being explored by NIST. Understanding the evolution of software assurance practices provides valuable context for evaluating the potential impact of new metrics and tools.
    - Paul Black provided an overview of the historical approaches to software security testing and how they have evolved over time. He explained that traditional methods often relied on manual code reviews, penetration testing, and ad-hoc testing techniques. These approaches, while valuable, were often time-consuming, resource-intensive, and dependent on the expertise of individual testers. Black contrasted these historical methods with the metrics-driven techniques being explored by NIST, which leverage automated tools, standardized datasets, and quantitative measurements to assess software security. He highlighted the potential benefits of metrics-driven approaches, such as increased efficiency, scalability, and the ability to identify trends and patterns across large codebases. Black also emphasized the importance of combining metrics-driven techniques with human expertise and judgment, as automated tools may not capture all relevant security issues. He acknowledged that while

metrics-driven approaches represent a significant advancement in software assurance, they should be viewed as complementary to, rather than a replacement for, traditional testing methods.

- Discussed the importance of metrics focused on the software development process itself, such as measures of developer training, code review practices, and security testing coverage. These process-oriented metrics can provide leading indicators of software security and help organizations proactively manage risk.
    - Paul Black agreed with Alex Gantman's emphasis on the importance of process-oriented metrics in software security. He acknowledged that while much of the focus in software metrics research has been on the technical characteristics of the code itself, the development process plays a crucial role in determining the overall security of the software. Black discussed the value of metrics such as developer training levels, the thoroughness of code review practices, and the coverage of security testing activities. He explained that these process-oriented metrics can serve as leading indicators of software security, helping organizations identify potential risks and vulnerabilities early in the development lifecycle. Black also highlighted the importance of establishing baseline measurements for these process metrics and tracking their evolution over time to assess the effectiveness of security initiatives and drive continuous improvement. He mentioned that NIST is actively exploring ways to incorporate process-oriented metrics into its software assurance research and is collaborating with industry partners to develop standardized frameworks and best practices for measuring and improving software development processes from a security perspective.

6. How to Measure and Communicate What Matters in Cybersecurity Risk and Board Questions

- Time: 2:45 P.M. -- 3:30 P.M.
- Speakers:
    - Richard Seiersen, Chief Technology Risk Officer, Qualys
    - Cristin Goodwin
    - Alex Gantman
    - Giulia Fanti
    - Steve Lipner
    - Matthew Scholl
- Details:
    - Richard Seiersen:
        - Opened the presentation by sharing his personal experience working as the CISO for a cloud-native company that had recently gone public. He described inheriting a security team that had been significantly reduced in size and faced pressure from the CEO to prioritize brand and reputation risk.

    - Presented a case study involving the discovery of 2 trillion records of PII data stored in AWS S3 buckets with weak security controls. Through discussions with the company's CPO, CTO, GC, and CFO, he helped them understand the true extent of their risk exposure and the need for additional cyber insurance coverage.
    - Emphasized the importance of quantifying cyber risk in financial terms that resonate with business stakeholders. By translating technical risks into potential loss scenarios, CISOs can more effectively communicate the business impact of cybersecurity investments.
    - Introduced a framework for measuring an organization's attack surface across on-premises, cloud, and operational technology environments. This framework incorporates threat intelligence, asset criticality, and compensating controls to provide a comprehensive view of an organization's risk posture.
    - Stressed the distinction between implementing security controls and achieving meaningful risk reduction. Effective cybersecurity programs must prioritize investments based on their demonstrable impact on mitigating the most significant risks to the business.

Discussion Participants:

- Cristin Goodwin:
  - Asked about the challenges companies face in adopting a risk quantification approach to cybersecurity and how to overcome internal resistance to change. Transitioning from compliance-based to risk-based security programs requires a significant shift in mindset and culture.
    - Richard Seiersen acknowledged the challenges organizations face when adopting a risk quantification approach, emphasizing the need for a collaborative effort involving security, finance, and business stakeholders. He stressed the importance of starting with small, manageable steps and demonstrating the value of risk quantification through pilot projects and incremental successes. By engaging stakeholders in the process and highlighting the benefits of data-driven decision-making, CISOs can gradually build support for a more risk-focused approach to cybersecurity management.
  - Discussed the importance of aligning security metrics with business objectives and communicating the value of cybersecurity in terms that resonate with executive leadership. CISOs must develop the language and skills to translate technical risks into strategic priorities.
    - Richard Seiersen strongly agreed with the need to align security metrics with business objectives and effectively communicate the value of cybersecurity to executive leadership. He emphasized the role of CISOs as translators, bridging the gap between technical risks and strategic priorities. By developing a deep understanding of the organization's goals, industry landscape, and risk appetite, CISOs can craft compelling

narratives that demonstrate how cybersecurity investments directly support business outcomes. Seiersen also highlighted the importance of using financial terms and metrics that resonate with executives, such as return on investment (ROI) and net present value (NPV), to articulate the business case for cybersecurity initiatives.

- Alex Gantman:
  - Raised the question of how to effectively measure the outcomes of cybersecurity investments and demonstrate their impact on reducing risk. Traditional security metrics often focus on activity rather than results, making it difficult to assess the true value of security programs.
    - Richard Seiersen acknowledged the challenges in measuring the outcomes of cybersecurity investments and the limitations of traditional activity-based metrics. He emphasized the need to shift focus towards risk-based metrics that directly tie to business objectives and demonstrate the impact of security programs on reducing potential losses. Seiersen suggested leveraging techniques such as Monte Carlo simulations and scenario analysis to quantify the likelihood and financial impact of cyber incidents, enabling organizations to prioritize investments based on their risk reduction potential. He also stressed the importance of establishing baseline measurements and tracking progress over time to assess the effectiveness of security controls and initiatives.
  - Explored the potential for leveraging economic models and data analytics to quantify the financial impact of cyber incidents and inform investment decisions. Developing more sophisticated approaches to risk quantification is essential to optimizing cybersecurity resource allocation.
    - Richard Seiersen expressed enthusiasm for the application of economic models and data analytics in quantifying the financial impact of cyber incidents and informing investment decisions. He discussed the value of leveraging techniques such as the loss distribution approach (LDA) and extreme value theory (EVT) to model the frequency and severity of potential losses, enabling organizations to make more informed decisions about risk transfer and retention strategies. Seiersen also highlighted the importance of collecting and analyzing historical incident data, as well as incorporating external threat intelligence and industry benchmarks, to refine risk models and improve their predictive power. By adopting a more data-driven approach to risk quantification, organizations can optimize their cybersecurity resource allocation and ensure that investments are aligned with the most significant areas of risk.
- Katie Moussouris:
  - Expressed concerns about the challenges of implementing risk quantification at scale and the potential for unintended consequences. Overreliance on quantitative metrics may lead to a false sense of precision and underestimation of the inherent uncertainty in cyber risk assessment.
    - Richard Seiersen acknowledged the valid concerns raised by Katie Moussouris regarding the challenges of implementing risk quantification

at scale and the potential pitfalls of overreliance on quantitative metrics. He emphasized the importance of recognizing the inherent uncertainty in cyber risk assessment and the need to incorporate qualitative factors and expert judgment alongside quantitative analysis. Seiersen stressed that risk quantification should be viewed as a decision-support tool rather than a silver bullet and that organizations must remain aware of the limitations and assumptions underlying their risk models. He also highlighted the importance of regularly validating and updating risk models based on new data and evolving threat landscapes to ensure their ongoing relevance and accuracy.

  - Emphasized the need to consider the broader system dynamics and interdependencies that influence an organization's risk posture. Focusing too narrowly on individual metrics may obscure important contextual factors and lead to suboptimal decision-making.
    - Richard Seiersen strongly agreed with the importance of considering the broader system dynamics and interdependencies that shape an organization's risk posture. He emphasized that effective risk management requires a holistic view of the interconnected nature of technology, people, and processes, and the potential cascading effects of security incidents across the enterprise. Seiersen discussed the value of techniques such as system dynamics modeling and network analysis to identify key risk drivers and understand the complex relationships between different components of the organization's cybersecurity ecosystem. By taking a more systemic approach to risk assessment and decision-making, organizations can avoid the pitfalls of focusing too narrowly on individual metrics and ensure that their cybersecurity strategies are resilient and adaptable to changing circumstances.
- Steve Lipner:
  - Inquired about the evidence supporting the effectiveness of secure-by-design principles in reducing cyber risk. While intuitively appealing, empirical data on the impact of proactive security measures is often limited.
    - Richard Seiersen acknowledged the current limitations in empirical data supporting the effectiveness of secure-by-design principles in reducing cyber risk. He emphasized that while the concept is intuitively appealing and aligns with best practices in software development and system architecture, quantifying the specific impact of proactive security measures remains challenging. Seiersen discussed the need for more rigorous research and case studies to establish a stronger evidence base for the value of secure-by-design approaches. He also highlighted the importance of organizations tracking and measuring the outcomes of their own secure-by-design initiatives, such as the reduction in vulnerabilities, incidents, and remediation costs, to build a body of empirical data that can support the broader adoption of these principles.
  - Discussed the role of architectural decisions and design trade-offs in shaping an organization's risk profile. CISOs must collaborate closely with IT and business

leaders to ensure that security considerations are integrated into the early stages of system design and development.

- Richard Seiersen strongly emphasized the critical role of architectural decisions and design trade-offs in shaping an organization's overall risk profile. He discussed the importance of CISOs collaborating closely with IT and business leaders to ensure that security considerations are integrated into the earliest stages of system design and development rather than being bolted on as an afterthought. Seiersen highlighted the value of threat modeling, security architecture reviews, and risk-based design principles in identifying and mitigating potential vulnerabilities and attack vectors. He also stressed the need for CISOs to be involved in key technology and business decisions, such as vendor selection, cloud migration, and digital transformation initiatives, to ensure that security risks are adequately addressed and aligned with the organization's overall risk appetite. By fostering a culture of collaboration and shared responsibility for cybersecurity, organizations can develop more resilient and secure systems that effectively balance business objectives with risk management imperatives.

- Giulia Fanti:
  - Raised questions about the use of scores in cybersecurity metrics. She highlighted significant challenges in score computation, including:
    - Inconsistent methodologies across organizations
    - Lack of comparability between different scoring systems
    - Problematic practices of mixing categorical and numeric variables
  - Richard Seiersen acknowledged these concerns, explaining that scores are a persistent 'war doctrine' in cybersecurity. He emphasized that while scores inevitably lose information during aggregation, a well-designed scoring system should:
    - Serve as an index of related heuristics.
    - Maintain consistency when comparing similar entities.
    - Provide meaningful differentiation between distinct risk scenarios.
    - Adapt to complex factors like hybrid assets, vulnerability stacks, and temporal changes security.

7. Public Comment, Summary of Day 1, and Board Discussions

- Time: 3:30 P.M. -- 4:15 P.M.
- Speakers:
  - Steve Lipner, Chair
- Details:
  - Public Comment: Joseph Guirreri provided substantive input on several key areas:
    - Infrastructure vulnerability concerns
      - Current state of critical infrastructure security

    - Emerging threats and challenges
    - Need for systematic improvements
  - CrowdStrike Incident Analysis
    - Root cause examination
    - Broader implications for industry
    - Lessons learned and recommendations.
  - Software Development Practices
    - Current reliance on customer-found errors
    - Need for improved reliability standards
    - Recommendations for enhanced quality assurance

- The Board engaged in open discussion, reflecting on the insights and themes that emerged during the day's presentations and identifying potential areas for further exploration and recommendations.
- Steve Lipner adjourned the meeting for the day, noting that the Board would reconvene the following morning to continue their discussions and hear additional presentations on cybersecurity topics of interest.

Thursday, November 7th, 2024

ISPAB Meeting Notes - Day 2

---

1. Face Recognition Verification Test Program and Board Q&A / Discussions

- Time: 10:00 A.M. -- 10:45 A.M.
- Speakers:
  - Patrick Grother, Chief, Information Access Division, ITL, NIST
  - Alex Gantman
  - Giulia Fanti
- Details:
  - Patrick Grother, Chief, Information Access Division, ITL, NIST:
    - Explained that the face recognition industry is largely incapable of estimating errors in their systems due to a lack of access to large-scale, diverse databases. Acquiring such databases would be prohibitively expensive for individual companies.
    - Noted that while some companies operating in diverse cities may be able to recruit more diverse datasets, these are still limited to thousands or tens of thousands of photos. In contrast, NIST provides an open, ongoing benchmark with a much larger and more diverse data set.

- Highlighted that face recognition technology has advanced significantly over the past decade. On a fixed dataset, mean absolute errors have reduced from around 4 years a decade ago to 2.7 years today, largely due to advancements in AI and neural network-based algorithms.
- Presented an overview of NIST's comprehensive biometrics evaluation programs, including the Face Recognition Vendor Test (FRVT), Face Recognition Technology Evaluation (FRTE), and Facial Age Test and Evaluation (FATE). These programs support NIST's broader biometrics work that spans fingerprints, tattoos, voice recognition, and DNA testing protocols.
- Highlighted significant improvements in face recognition accuracy, with error rates dropping from 28% to 0.2% for certain tasks over the past decade. Noted particularly strong performance in age estimation, achieving accuracy of +/-1.4 years for subjects aged 14-30.
- Detailed NIST's role in providing essential testing infrastructure for the biometrics industry through its vendor testing program. Explained that most companies lack access to sufficiently large, diverse datasets needed for comprehensive testing, typically having only thousands to tens of thousands of photos even in diverse cities.
- Described the rigorous controls around NIST's sequestered datasets, including physical security measures, strict submission protocols limiting vendors to updates every four months, and controls preventing network access or side effects from submitted code. Emphasized that only aggregated results are published to protect dataset privacy.
- Discussed the issue of variance in age estimates when running face recognition on video clips. Algorithms from all vendors exhibit fluctuations in age estimates across frames, which is undesirable. The face recognition community has made strides in addressing this, building algorithms that are more resilient to factors like illumination, expression, and head orientation. More work is needed in this area.
- Emphasized that face recognition now largely succeeds within a certain "capture envelope" - i.e., frontal portrait photos under controlled conditions. Performance degrades when images fall outside this envelope due to extreme pose, blur, occlusion, or other factors.
- Identified problematic behavior of algorithms when processing very low-resolution images. Due to neural network architecture limitations, when input images are smaller than the network's input layer size, interpolation issues arise leading to anomalous results, including very high false positive rates. While some algorithms exhibit this unwelcome property, more responsible developers have implemented analysis to detect low-quality images with insufficient signal and avoid assigning high match likelihood scores in these cases.
- Discussed demographic differences in false match rates, with some algorithms developed in certain regions showing significantly higher false match rates on images from other demographics - e.g., a 60x higher false

match rate on West African women compared to Eastern European women. Improvements have been made but many developers likely remain unaware of these performance variations.

Discussion Participants:

- Alex Gantman:
    - Inquired about potential confounding factors like the time period in which photos were taken, noting that facial expressions and styles change over time, which could impact the accuracy of models trained on older data. Also asked about the impact of the social conditions in which the photo subjects lived, suggesting this could affect perceived age.
        - Patrick Grother agreed with Alex Gantman's observations, acknowledging that various factors such as the time period, cultural and societal changes, and individual circumstances can indeed influence the accuracy of facial recognition models. He noted that there could be variations in facial expressions, hairstyles, and other characteristics across different eras, which may impact the performance of algorithms trained on older data when applied to more recent images. Grother also concurred that the social conditions and life experiences of the individuals in the photos could affect their perceived age, as factors like stress, lifestyle, and environmental exposures can contribute to variations in facial aging patterns. He emphasized the importance of considering these confounding factors when evaluating the accuracy and generalizability of facial recognition algorithms and the need for diverse and representative datasets that span different time periods and demographic groups to mitigate potential biases.
- Giulia Fanti:
    - Asked if the sequestered datasets used by NIST are private and if there are any risks associated with external parties potentially learning about the data through the benchmarks and metrics published. Suggested that if algorithms are designed adversarially, aggregate statistics could potentially leak information about individuals in the dataset.
        - Patrick Grother assured Giulia Fanti that the sequestered datasets used by NIST are indeed private and subject to strict access controls and data protection measures. He explained that the datasets are stored in secure, physically protected rooms with limited access and that NIST adheres to data-sharing agreements that prohibit the dissemination of the data to external parties. Grother acknowledged the potential risks associated with adversarial algorithms attempting to infer information about individuals from aggregate statistics but emphasized that NIST takes precautions to mitigate these risks by publishing only aggregated results over large sample sizes and ensuring that no personally identifiable information is released. He also mentioned that NIST continually assesses and updates its

        data protection practices addressing emerging threats and maintain the privacy and security of the datasets.
  - Inquired about any limits NIST places on how frequently organizations can update their algorithms for the benchmark to prevent overfitting.
    - Patrick Grother confirmed that NIST does impose limits on the frequency with which organizations can update their algorithms for the benchmark as a measure to prevent overfitting and ensure the integrity of the evaluation process. He explained that participants are typically allowed to submit algorithm updates once every four months, striking a balance between providing opportunities for improvement and preventing excessive fine-tuning to the specific datasets used in the benchmark. Grother emphasized that this policy helps maintain a level playing field among participants and ensures that the benchmark results reflect the general performance of the algorithms rather than their ability to overfit a particular set of test data. He also noted that NIST continuously monitors the submission process and may adjust the frequency limits as needed to adapt to changes in the technology landscape and maintain the robustness of the benchmark.

2. NIST Cybersecurity and Privacy Update and Board Q&A / Discussions

- Time: 10:45 A.M. -- 11:30 A.M.
- Speakers:
  - Matthew Scholl, Division Chief, Computer Security Division (CSD), NIST
  - Julie Chua, Division Chief, Applied Cybersecurity Division (ACD), NIST
  - Marc Groman
  - Cristin Goodwin
  - Jessica Fitzgerald-McKay
  - Steve Lipner
  - Essye Miller
- Details:
  - Matthew Scholl:
    - Provided an update on post-quantum cryptography (PQC) standardization efforts, noting the recent finalization of the first 3 PQC algorithms in August 2022. Emphasized that significant work remains in areas like transition guidance, identifying quantum-vulnerable algorithms, and establishing deprecation timelines.
    - Discussed NIST's ongoing collaboration with standards bodies like the IETF to ensure the new PQC standards are properly referenced for broad international adoption. Highlighted the role of the Board's previous standards recommendation letter in allowing NIST to prioritize this standards engagement.
    - Outlined plans to publish draft transition timelines for migrating to post-quantum algorithms by November 19th, 2024, as required by the National Security Memorandum 10 (NSM-10). The draft will propose timelines for accepted use, deprecation, and legacy use of different algorithms.

    - Announced an upcoming PQC workshop in February 2025 to discuss key establishment, additional guidance beyond the FIPS standards, hybrid implementations, and potential future key establishment methods.
    - Touched on the issue of "cryptographic agility" and the need for a clearer definition of this concept. Noted plans for NIST to publish a paper and host a workshop on crypto agility in 2025 aiming to identify the properties of "agile" algorithms and consider agility in future algorithm selection.
    - Provided additional details about NIST's ongoing work with Special Publications 800-171 and 800-172, which provide security guidance for controlled unclassified information (CUI). These documents, originally created to standardize security requirements for data shared outside government with commercial partners, have seen significant adoption. The Department of Defense has incorporated these publications into their Cybersecurity Maturity Model Certification (CMMC) program, extending their influence across the defense industrial base and supply chain. Scholl mentioned that NIST will be releasing an update to SP 800-172 prior to the Thanksgiving break, incorporating feedback from implementing agencies, the National Archives and Records Administration (NARA), and industry partners.
    - Noted NIST's recent seat on the Common Vulnerabilities and Exposures (CVE) board, which will allow them to play a more active role in vulnerability tracking and management. The organization is currently working to catch up on the existing CVE backlog,
  - Julie Chua:
    - Provided an update on NIST's involvement in 5G security standards development through participation in 3GPP security working groups. The goal is to ensure NIST's cybersecurity guidelines are considered in standards discussions.
    - Highlighted the NCCoE's 5G security project focused on demonstrating the use of existing cybersecurity capabilities to protect 5G systems. Noted the recent release of a series of white papers sharing findings from the NCCoE 5G testbed.
    - Discussed the status of supply chain security efforts, including the relaunch of the DevSecOps project to demonstrate use cases for the Secure Software Development Framework (SSDF). Acknowledged previous delays but expressed optimism about the project's renewed progress.
      - Scholl highlighted NIST's continued work in hardware security, emphasizing collaborations with the Chips Office and Material Science Office. The team is developing cybersecurity framework profiles for several critical hardware-related use cases, including:
        - Security assessment of hardware fabrication environments
        - Supply chain security for hardware delivery.
        - Research into hardware design characteristics
        - Developing protections against IP theft, reverse engineering, and gray market activities

        - The research focuses on advanced techniques such as:
            - Side-channel attack analysis
            - Secret leakage detection
            - Best practices for preventing hardware-level security vulnerabilities.
        - Blockchain technology is being explored as a potential tool for enhancing supply chain traceability, though specific details of this research were not extensively discussed.
    - Shared an update on the NCCoE's Mobile Driver's License project, which is expanding to explore use cases in the financial sector. Highlighted the diversity of collaborators engaged, including government agencies, tech companies, and existing partners at the state and bank level.

Discussion Participants:

- Marc Groman:
    - Asked for clarification on the scope of NIST's authority to mandate post-quantum algorithm adoption timelines for federal agencies versus the private sector.
        - Matthew Scholl confirmed that NIST has the authority to set mandatory standards and timelines for post-quantum algorithm adoption within the federal government, specifically for non-classified systems, while NSA handles requirements for classified systems. He explained that NIST's role is to establish the internal U.S. government policy for encryption on non-classified systems, and agencies are obligated to comply with these mandates. However, Scholl clarified that NIST does not have the same authority to enforce adoption timelines in the private sector, although many companies voluntarily follow NIST's guidance and best practices. He mentioned that other regulatory bodies, such as the FTC, HHS, and industry-specific authorities, often defer to NIST's standards when setting their own requirements for the private sector.
- Cristin Goodwin:
    - Inquired whether NIST's 5G security efforts consider deployments in China and the intersection with U.S. initiatives.
        - Julie Chua acknowledged the importance of considering global deployments and the potential impact of 5G security efforts in other countries, including China, on U.S. initiatives. She explained that while NIST's primary focus is on 5G security within the United States, they recognize the interconnected nature of telecommunications networks and the need to address potential risks arising from deployments in other regions. Chua mentioned that NIST collaborates with international partners and participates in global standards bodies to promote alignment and address common security challenges. However, she clarified that the specific scope of NIST's 5G security projects, such as the NCCoE testbed, may not directly incorporate deployments in China, but the insights gained

from these efforts can inform broader discussions on mitigating risks associated with global 5G implementations.

- Jessica Fitzgerald-McKay:
    - Acknowledged the positive collaboration between NSA and NIST representatives in 3GPP security standards work. Asked if NIST had any plans to engage at the SA plenary level above the working groups, where security proposals often face challenges. Offered the Board's support in expanding NIST's participation.
        - Julie Chua expressed appreciation for the positive feedback on the collaboration between NSA and NIST representatives in 3GPP security standards work. Regarding engagement at the SA plenary level, Chua acknowledged the importance of addressing security challenges at higher levels of the standards process. She mentioned that while NIST's current focus has been on participating in the security working groups, they are open to exploring opportunities for engagement at the SA plenary level. Chua thanked Jessica Fitzgerald-McKay for the offer of support from the Board and agreed to discuss potential avenues for expanding NIST's participation in the future. She emphasized the value of collaboration and leveraging the collective expertise of the cybersecurity community to drive meaningful progress in 5G security standards.
- Steve Lipner:
    - Asked if NIST's 5G work incorporates implementation security issues beyond protocol specifications, such as supply chain, secure design, and software security.
        - Julie Chua confirmed that NIST's 5G security efforts extend beyond protocol specifications and encompass a range of implementation security considerations. She explained that the NCCoE's 5G security project aims to address the security of the underlying IT components and systems that support 5G networks, including supply chain risk management, secure software development practices, and the integration of security controls across the 5G architecture. Chua mentioned that the project's recently released white paper series provides insights into the application of NIST's cybersecurity and privacy frameworks to 5G implementations, covering topics such as zero trust, identity management, and software assurance. She emphasized the importance of a holistic approach to 5G security that considers the entire ecosystem, from hardware and software components to operational processes and human factors.
- Essye Miller:
    - Suggested that CMMC (Cybersecurity Maturity Model Certification) is an important topic for the Board to revisit, as well as FedRAMP, to understand how these efforts intersect with NIST frameworks.
        - Matthew Scholl agreed with Essye Miller's suggestion that CMMC and FedRAMP are important topics for the Board to revisit, given their intersection with NIST frameworks and their impact on cybersecurity practices across the federal government and its supply chain. He acknowledged that both programs have undergone significant changes and

updates in recent years, and it would be valuable for the Board to receive a comprehensive briefing on their current status and alignment with NIST's efforts. Scholl mentioned that NIST has been collaborating with the Department of Defense and the General Services Administration to ensure consistency between CMMC, FedRAMP, and the NIST frameworks, particularly in areas such as control mapping, assessment procedures, and continuous monitoring requirements. He welcomed the opportunity to arrange a dedicated session on these topics at a future ISPAB meeting to facilitate a deeper understanding of the synergies and challenges in harmonizing these programs with NIST's ongoing work in cybersecurity and privacy.

3. Secure By Design Pledge Metrics and CISA Advisory Report and Board Q&A / Discussions

- Time: 11:30 A.M. -- 12:15 P.M.
- Speakers:
    - Matthew Kehoe, Director, Information Security, Apple, Inc.
    - Katie Moussouris
    - Alex Gantman
    - Steve Lipner
- Details:
    - Matthew Kehoe, Director, Information Security, Apple, Inc.:
        - Presented findings and recommendations from the October 11th CISA Cybersecurity Advisory Subcommittee report on secure-by-design practices.
        - Discussed the subcommittee's goal of studying the economics of the software industry to identify actions CISA could take to incentivize the adoption of secure-by-design principles.
        - Shared key findings from interviews with public and private sector entities, including:
            - An estimated 20% of typical application code bases are related to security features but are often written by non-security experts.
            - Venture capital markets view secure development practices as a financial barrier for startups.
            - The majority of open-source work is done by unpaid hobbyists, with many considering quitting due to maintenance burdens.
        - Outlined the subcommittee's 3 recommendations to CISA:
            - Conduct a study to quantify the financial and customer experience impacts of companies that have survived and recovered from large-scale security incidents.
            - Further, study whether fixing vulnerabilities early in the software development lifecycle can be proven cost-effective.
            - Design a framework for standardized, actionable security impact assessments focused on critical infrastructure.

        - Shared data from Apple's supplier ecosystem, highlighting the challenges faced by small and medium-sized businesses in implementing cybersecurity due to cost, awareness, and resource constraints.
        - Emphasized the need for clear, direct, and easy-to-understand security guidance to drive meaningful outcomes, particularly for smaller organizations.

Discussion Participants:

- Katie Moussouris:
    - Asked about efforts to make critical security features like multi-factor authentication (MFA) a default offering to reduce cost barriers for adoption.
        - Matthew Kehoe acknowledged the importance of making critical security features like MFA a default offering to reduce cost barriers and encourage widespread adoption. He agreed that the current practice of treating security as a value-added feature or a premium offering can hinder the implementation of essential security controls, particularly for smaller organizations with limited budgets. Kehoe mentioned that the subcommittee discussed the concept of shifting the liability for security to the software and service providers, ensuring that baseline security features are included as part of the standard offering. He cited examples of major cloud service providers announcing plans to enable MFA by default for their customers, demonstrating a positive trend toward making security an integral part of the product rather than an optional add-on.
    - Highlighted the importance of specifying more secure forms of MFA beyond SMS-based methods, drawing on findings from the Cyber Safety Review Board.
        - Matthew Kehoe concurred with Katie Moussouris' emphasis on specifying more secure forms of MFA beyond SMS-based methods, acknowledging the findings from the Cyber Safety Review Board. He recognized that while SMS-based MFA is still widely used, it has been shown to be vulnerable to various attacks, such as SIM swapping and SMS interception. Kehoe mentioned that the subcommittee's discussions on MFA adoption should include clear guidance on recommended authentication methods, such as hardware tokens, mobile apps with secure key storage, and biometric factors. He expressed the importance of educating organizations and users about the limitations of SMS-based MFA and providing them with practical alternatives that offer stronger security guarantees.
- Alex Gantman:
    - Commended the approach of questioning assumptions about the link between security outcomes and economic outcomes for companies.
        - Matthew Kehoe appreciated Alex Gantman's positive feedback on the subcommittee's approach of questioning assumptions about the link between security outcomes and economic outcomes for companies. He acknowledged that the prevailing narrative often suggests a direct

correlation between investing in security and achieving better financial results, but the empirical evidence to support this claim is limited. Kehoe mentioned that the subcommittee's research aimed to challenge these assumptions and provide a more nuanced understanding of the relationship between security practices and business outcomes. By critically examining the available data and case studies, the subcommittee hopes to identify the specific conditions and contexts in which secure practices translate into measurable economic benefits, as well as the potential limitations and trade-offs involved.

  - Inquired about plans to validate the effectiveness of secure-by-design principles in leading to positive security outcomes, emphasizing the need for empirical evidence beyond belief.
    - Matthew Kehoe acknowledged the importance of validating the effectiveness of secure-by-design principles in leading to positive security outcomes and the need for empirical evidence to support these claims. He mentioned that while the subcommittee's initial research focused on understanding the economic drivers and barriers to adopting secure-by-design practices, there is a clear need for further studies to assess the impact of these principles on actual security outcomes. Kehoe outlined potential plans to collaborate with industry partners and academic institutions to conduct targeted case studies and collect quantitative data on the relationship between secure-by-design practices and various security metrics, such as vulnerability reduction, incident response time, and overall risk posture. He emphasized the value of establishing a strong evidence base to guide the development and refinement of secure-by-design guidelines and promote their wider adoption across the industry.
- Steve Lipner:
  - Shared anecdotal experience with the high cost of remediating insecure architectural decisions discovered late in the development process.
    - Matthew Kehoe resonated with Steve Lipner's anecdotal experience regarding the high cost of remediating insecure architectural decisions discovered late in the development process. He acknowledged that this is a common challenge faced by many organizations, where security considerations are often an afterthought or addressed only in the later stages of the software development lifecycle. Kehoe mentioned that the subcommittee's research highlighted similar examples where the failure to incorporate security early in the design phase resulted in significant technical debt, increased remediation costs, and delayed time-to-market. He emphasized the importance of shifting security "to the left" and integrating secure-by-design principles from the outset of a project to avoid costly rework and mitigate potential risks.
  - Expressed hope that the subcommittee's recommended studies on the impact and cost-effectiveness of secure design practices would be carried out to provide valuable insights.

- Matthew Kehoe shared Steve Lipner's hope that the subcommittee's recommended studies on the impact and cost-effectiveness of secure design practices would be carried out to provide valuable insights. He reiterated the subcommittee's commitment to driving evidence-based decision-making and providing actionable guidance to organizations seeking to implement secure-by-design principles. Kehoe mentioned that the proposed studies, including the long-term analysis of the financial and customer experience impacts of security incidents and the investigation of the cost-effectiveness of fixing vulnerabilities early in the development process, are critical to building a compelling case for secure-by-design adoption. He expressed optimism that the findings from these studies would help inform industry best practices, standards development, and policy discussions around software security and resilience.

4. Overview of NIST SP 800-55 Performance Metrics Guide and Board Q&A / Discussions

   [Note: The scheduled CWE presentation by Kent Landfield had to be canceled]

- Time: 1:15 P.M. -- 2:45 P.M.
- Speakers:
  - Katherine Schroeder, NIST
  - Cristin Goodwin
  - Katie Moussouris
  - Alex Gantman
  - Essye Miller
  - Marc Groman
  - Giulia Fanti
  - Steve Lipner
- Details:
  - Katherine Schroeder:
    - Provided an overview of the history and evolution of NIST Special Publication 800-55, Performance Measurement Guide for Information Security.
    - Explained the decision to split the new revision into two volumes to separate statistical concepts from guidance on implementing and maintaining measurement programs.
    - Emphasized the importance of clarifying terminology, particularly the distinction between measurement (obtaining quantitative values) and assessment (evaluating against defined criteria).
    - Outlined the three types of assessments: qualitative (non-numerical), semi-quantitative (numerical but context-dependent), and quantitative (numerical and context-independent).
    - Encouraged organizations to move towards quantitative assessments, when possible, to improve precision and reduce bias.

        - Introduced a four-tier model for measurement types: implementation, effectiveness, efficiency, and impact.
        - Discussed the challenges organizations face in determining what and how to measure, highlighting the need for baselines and consistent metrics over time.
        - Shared plans for a forthcoming community of interest to facilitate discussion and collaboration among practitioners in the measurement and metrics space.
        - Outlined future work on the Program Review for Information Security Assistance (PRISMA) and the development of case studies and worked examples to support the adoption of SP 800-55 guidance.

Discussion Participants:

- Cristin Goodwin:
    - Inquired about who the target audience and intended customers for SP 800-55 are, particularly whether federal agencies would utilize the guidance.
        - Katherine Schroeder explained they've focused it at the CISO level and upward direction, as this group translates raw data into meaningful insights for leadership. She noted that while originally written primarily for federal audiences, they've tried to broaden it for wider applicability given the evolution of their audience over the past 20 years.
    - Asked about who constitutes the target community for the planned community of interest.
        - Schroeder shared that they regularly receive emails from newly appointed metrics program leaders across organizations seeking guidance on where to start, demonstrating clear interest and need for this type of support.
- Katie Moussouris:
    - Noted there are only two people on the metrics team and suggested the Board could potentially recommend additional resources.
        - Schroeder confirmed this would be helpful, explaining they had hoped to hire more people earlier in the year but were unable to due to budgetary constraints.
    - Requested information about a prioritized list of projects that would benefit from increased staffing to support potential Board recommendations.
        - Schroeder indicated they could put together such a list, noting they had already discussed internally what those priorities might look like.
- Steve Lipner:
    - Expressed concern that the guidance was too abstract and questioned whether there were specific measures recommended for medium-sized organizations trying to assess their security.
        - Schroeder explained this was an intentional choice to avoid organizations just following a checklist rather than considering their unique needs, though acknowledged this creates challenges for organizations just starting out.

    - Suggested exploring whether case studies or NCCOE worked examples could provide more concrete direction.
        - Schroeder agreed this could be valuable and noted there had been interest from industry partners in developing consensus recommendations about best-starting points for organizations.
- Giulia Fanti:
    - Raised a question about whether federal agencies are currently tracking outcome-level metrics, suggesting it might be useful to start with better-resourced organizations as a model. She also proposed developing a taxonomy of different types of harm and understanding how to measure each type.
        - Alex Gantman responded that measuring harm for federal agencies might actually be harder than for the private sector because national security impacts are more difficult to quantify than economic impacts.
        - Marc Groman countered that this challenge increasingly applies to private sector organizations as well, given their role in national security through their data holdings.
- Marc Groman:
    - Emphasized the need to be precise about what exactly is being measured, noting that the measurement discussion becomes fuzzy quickly without clear objectives.
    - Highlighted NIST's limited role in putting out standards, noting they cannot issue regulations or requirements.
    - Stressed how changing metrics requirements frequently undermines the ability to conduct trend analysis and assess performance over time.
        - Shared personal experience from his time as agency CPO about the frustration and burden of constantly changing metrics without clear evidence they were having positive effects.
- Alex Gantman:
    - Stressed the importance of measuring outcomes rather than just implementation efforts.
    - Argued for the need to validate whether security interventions actually lead to improved outcomes.
    - Drew parallels to public health metrics, suggesting that even with many confounding factors, it's possible to measure whether things are improving at a population level.
        - This sparked discussion about the challenges of measuring security improvements versus measuring compliance with specific practices.
- Essye Miller:
    - Questioned what specific problems they were trying to solve with metrics, drawing from her experience inside government departments.
    - Emphasized the importance of focusing on metrics that matter to mission execution and business interruption.
    - Raised concerns about whether basic cybersecurity measures would meaningfully impact operational missions.
        - This led to a broader discussion about aligning metrics with organizational objectives and mission priorities.

5. Board Work; Recommendations; Next Meeting Planning

- Time: 2:45 P.M. -- 3:30 P.M.
- Speakers:
    - Steve Lipner, Chair
    - Matthew Scholl, NIST
    - Essye Miller
    - Alex Gantman
    - Cristin Goodwin
    - Katie Moussouris
    - Marc Groman
    - Giulia Fanti
- Details:

The Board engaged in an open discussion to reflect on the insights and themes that emerged during the two-day meeting and identify potential areas for further exploration and recommendations.

Steve Lipner provided a recap of the metrics-focused sessions, highlighting:

- The frameworks session provided insight into what government agencies are being told to do.
- The loss of the FISMA metrics presentation was unfortunate, given its relevance.
- Paul Black's presentation offered component-focused metrics for software.
- Rich Seiersen's discussion emphasized measuring overall problems rather than components.
- The need for better data about where harms are occurring.
- The importance of a more rigorous root cause analysis of incidents

Board Members:

- Marc Groman:
    - Emphasized the need for precision in what exactly is being measured, noting that different aspects of measurement don't always map to each other.
    - Highlighted NIST's limited role in putting out standards and avoiding picking winners and losers.
    - Stressed how changing metrics requirements frequently undermines the ability to conduct trend analysis.
    - Drew from his experience at OMB regarding the importance of having evidence before mandating specific requirements.
- Alex Gantman:
    - Stressed the importance of measuring outcomes rather than just implementation efforts.
    - Advocated for validating whether security interventions actually lead to improved outcomes.

  - Drew parallels to public health metrics, suggesting that even with many confounding factors, it's possible to measure whether things are improving at a population level.
  - Expressed interest in following up on CISA's secure by design work in 6-12 months.
- Cristin Goodwin:
  - Highlighted the underserved community of MSPs and CSPs
  - Identified the gap between small businesses and large enterprises.
  - Emphasized the need for metrics appropriate to different organizational sizes.
  - Raised concerns about small businesses transferring risk management to service providers without understanding the implications.
- Katie Moussouris:
  - Discussed system dynamics at play in the industry and individual organizations' maturity journeys.
  - Highlighted challenges with market dynamics and security outcomes
  - Referenced a study showing patch prioritization by CVSS score versus random selection had similar outcomes.
  - Suggested metrics might be measuring the wrong things.
- Giulia Fanti:
  - Questioned whether federal agencies are currently tracking outcome-level metrics.
  - Suggested starting with better-resourced organizations as a model.
  - Proposed developing a taxonomy of different types of harms and methods for measuring each.
- Essye Miller:
  - Questioned what specific problems they were trying to solve with metrics.
  - Drew from her department experience to emphasize focus on mission interruption costs.
  - Raised concerns about whether basic cybersecurity measures meaningfully impact operational missions.

Matthew Scholl indicated that he and Jeff would work on compiling a summary of conclusions to capture the actions and thoughts discussed. This summary would be distributed to board members to ensure they had correctly captured the next steps and activities, noting this would not be formal minutes but rather a compilation of key takeaways and action items for review and feedback.

Key Action Items:

1. Alex Gantman, Cristin Goodwin, and Marc Groman to collaborate on drafting a document summarizing the Board's observations and potential recommendations related to cybersecurity metrics and measurement.
2. Request for additional resources for NIST's metrics staff
3. Consider NCCOE follow-up use case implementing SP 800-55
4. Future discussion of CMMC and FedRAMP

5. Follow-up on CISA's secure by design studies and recommendations.

Steve Lipner adjourned the meeting, noting that while the agenda had been somewhat dynamic, the engagement and discussion had been productive.

- Meeting Wrap-Up:
  - Review of key discussion points
  - Identification of action items
  - Planning for next meeting
  - Administrative announcements

Next Steps:

- Distribution of meeting minutes
- Follow-up on action items
- Preparation for March 2025 meeting
- Coordination of working group activities

Next Meeting:

- To be conducted in March 2025
- Format to be determined based on budgetary considerations following the resolution of the continuing resolution in December.
- Planning for an in-person meeting, pending funding availability.

ISPAB – November 6 and 7, 2024			
Last name	First name	Affiliation	Day
Board members			
Baker	Brett	NARA	
Fanti	Giulia	Carnegie Mellon University	
Fitzgerald-McKay	Jessica	NSA	
Gantman	Alex	Qualcomm	
Goodwin	Cristin	Advancing Cyber	
Groman	Marc	Privacy Consulting	
Duffy	Mike	CISA - DHS	
Lipner	Steve	SafeCode	

Miller	Essye	Executive Business Management	
Moussouris	Katie	Luta Security	
Venables	Philip	Google Cloud	
		NIST Staff	
Bojanova	Irena	NIST	Day 1 & Day 2
Boutin	Chad	NIST	Day 1 & Day 2
Calloway	Laura	NIST	Day 1 & Day 2
Dickson	Jessica	NIST	Day 1 & Day 2
Kerman	Sara	NIST	Day 1 & Day 2
Mahn	Amy	NIST	Day 1 & Day 2
McWhite	Rebecca	NIST	Day 1
Reidy	Kari	NIST	Day 1
Roberts	Kamie	NIST	Day 1
Santos	Danielle	NIST	Day 1
Sedgewick	Adam	NIST	Day 1 & Day 2
St. Pierre	James	NIST	Day 1 & Day 2
Takamura	Ed	NIST	Day 1 & Day 2
Trinh	Hung	NIST	Day 2
		Registered Attendees	
Marin	Alejandro		Day 1 & 2
Ann	Sara	Atlantic Council	Day 2
Danker	Jamie	Venable LLP (law firm)	Day 2
Doubleday	Justin	Federal News Network	Day 1 & Day 2
Eggers	Matthew	US Chamber of Commerce	Day 1 & Day 2
Friedman	Sara	IWP News	Day 2
Guirreri	Joseph		Day 1 & Day 2
Heyman	Mat		Day 1 & Day 2
Huang	Kuan-Tsae		Day 1
Ignaszewski	Katie	IBM	Day 2
Kerben	Jason	Department of State	Day 1 & Day 2
Leithauser	Tom	ANSI	Day 2
Livesay	Jacob	IWP News	Day 1 & Day 2
Lurie	Kirk	Electrosoft	Day 1 & Day 2
McRae	Jason	NIH	Day 2
McWhorter	Kiki		Day 1
Merkel	Warren	ANSI	Day 2
Moorer	Ceasha		Day 2
Mulberry	Karen	IEEE	Day 1 & Day 2
Ross	Nelson	Electrosoft	Day 1 & Day 2
Scott	Stew	Atlantic Council	Day 1

Sokol	Annie	Electrosoft	Day 1 & Day 2
Tupitza	Charlie	Global Resilience Federation	Day 1
Wai	Z.		Day 2
Weinberger	Peter		Day 1 & Day 2
Wunderly	Brooke	Defense Logistics Agency	Day 1
Williams	Derrick		Day 2

Certified and approved by

Steven B. Lipner
Chair
Information Security and Privacy Advisory Board