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

July 17 and 18, 2024

Virtual Meeting Platform: Zoom for Government

Board Members	Board Secretariat and NIST Staff
Brett Baker, NARA (absent)	Jeff Brewer, NIST
Giulia Fanti, Carnegie Mellon University	Matthew Scholl, NIST
Jessica Fitzgerald-McKay, NSA	Rodney Petersen, NIST
Alex Gantman, Qualcomm	Kevin Stine, NIST
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	
Phil Venables, Google Cloud (absent)	

Wednesday, July 17, 2024

ISPAB Meeting Notes - Day 1

---

1. Welcome and Opening Remarks

- Time: 10:00 A.M. – 10:30 A.M.
- Speakers:
  - Steve Lipner, Chair, ISPAB
  - Alex Gantman
  - Mike Duffy
  - Marc Groman
  - Cristin Goodwin
  - Board Members (various contributions)
- Details:
  - Steve Lipner, Chair, ISPAB:
    - Opened the meeting by welcoming all participants and initiating a round of introductions.
    - Briefly discussed his recent work on software liability, noting that he had published a paper on the subject, which he promised to share with the board members. He emphasized the importance of this work in the context of ongoing

discussions about cybersecurity and the necessity of establishing clear legal frameworks to govern software liability.
    - Encouraged board members to participate in the day's discussions actively, stressing the importance of their insights in shaping the Board's future recommendations.
- Alex Gantman:
    - Introduced himself as affiliated with Qualcomm and UCSD.
    - Discussed a recent project where he and his colleagues worked on cleaning up and publishing an ebook version of Kerckhoff's military cryptography. He emphasized the importance of making historical cryptographic works accessible to modern cybersecurity professionals better to understand foundational principles like "security through obscurity."
    - Mentioned that he would share the link to the ebook with the board members, seeing it as a valuable resource for those involved in cryptographic research and education. He expressed his belief that understanding these foundational texts is crucial for anyone working in the field of cybersecurity.
- Mike Duffy, Department of Homeland Security:
    - Provided an update on his new responsibilities as acting federal Chief Information Security Officer (CISO), emphasizing the importance of this role in enhancing cybersecurity across federal agencies. He noted that his position involves significant coordination with various federal entities to ensure that cybersecurity policies are consistently implemented.
    - Highlighted his ongoing focus on improving interagency operational alignment and cohesion at CISA, particularly in relation to the day's agenda items, such as the National Vulnerability Database (NVD) and AI security. He emphasized the need for better communication and collaboration across agencies to address the complex challenges posed by modern cybersecurity threats.
    - Acknowledged the challenges that come with his dual role at DHS and OMB, expressing optimism about the progress being made in aligning cybersecurity policies across the federal government. He mentioned that the integration of cybersecurity efforts across different agencies is crucial for the effective implementation of national strategies.
- Marc Groman:
    - Asked Mike Duffy about his new role, confirming that Duffy was now also involved with the Office of Management and Budget (OMB). He pointed out that having someone with operational experience in a policy-making position could help bridge the gap between policy and practice in federal cybersecurity efforts.
    - Mike Duffy responded, affirming that his involvement with OMB provided a valuable perspective that allowed him to align operational needs with policy decisions better. He noted that this dual role has been beneficial in ensuring that the policies developed are practical and implementable across various federal agencies.
    - Highlighted the importance of having a federal CISO who understands both the operational and policy aspects of cybersecurity, which is crucial for the effective implementation of national cybersecurity strategies. Groman suggested that this dual perspective would enable better decision-making at the federal level.
- Cristin Goodwin, Advancing Cyber Law:
    - Discussed her recent work on incident notification reports, particularly in response to new regulations from the Securities and Exchange Commission (SEC) and other regulatory bodies. She detailed the complexities companies face

in navigating different regulatory regimes in the US, especially regarding the sharing and reporting of incidents.
        - Emphasized the ongoing debates over incident notification rules and how they might evolve in the near future, stressing the need for clear and consistent guidelines that would help organizations comply with multiple regulatory requirements. Goodwin also pointed out the potential legal implications of these evolving regulations, noting that companies must be prepared to adapt to new reporting standards.
        - Steve Lipner responded by agreeing on the importance of consistency in regulatory requirements, mentioning that these issues would likely come up later in the meeting when discussing the integration of various frameworks. He suggested that the Board could consider making recommendations on how to streamline these requirements.
    - Other Contributions:
        - Other Board member introductions were provided by Giulia Fanti, Jessica Fitzgerald-McKay, Katie Moussouris, and Brian Gattoni.

2. Welcome and ITL Update

- Time: 10:30 A.M. – 11:00 A.M.
- Speakers:
    - Kevin Stine, Director, Information Technology Laboratory, NIST
    - Cristin Goodwin (question)
    - Marc Groman (question)
- Details:
    - Kevin Stine, Director, Information Technology Laboratory, NIST:
        - Provided an overview of the lab's mission to cultivate trust in IT and metrology, reiterating that recent leadership changes and ongoing projects at NIST have reinforced this mission.
        - Discussed recent leadership changes, including the ongoing search for a new Chief of the Applied Cybersecurity Division and Chief of Staff. He emphasized the importance of these roles in maintaining the lab's momentum and ensuring the successful execution of its initiatives. Stine noted that these leadership positions are critical for driving forward key programs and maintaining organizational stability during a period of significant transition.
        - Highlighted the challenges posed by a $33 million reduction in the FY 2024 R&D budget, explaining how this has created financial pressures that could potentially lead to significant programmatic cuts in the future. He stressed that while the cybersecurity and privacy budget remained stable, other areas within NIST were facing substantial challenges due to these cuts. Stine expressed concern about the potential impact on NIST's ability to meet its objectives, particularly in areas requiring sustained investment. An additional $100 million reduction is anticipated for FY2025.
        - Emphasized the lab's focus on key initiatives such as the National Vulnerability Database (NVD), privacy framework updates, and digital identity guidelines for public benefits programs. He noted that these initiatives are critical to advancing NIST's mission and ensuring that the lab remains at the forefront of addressing emerging cybersecurity challenges.
        - Discussed the integration of various risk management frameworks and profiles, as highlighted during the recent privacy workshop. He pointed out the

importance of aligning these frameworks, such as the Privacy Framework and the Cybersecurity Framework, to provide a cohesive approach to managing privacy and security risks. Stine mentioned that the ongoing integration of these frameworks would help organizations better manage complex cybersecurity challenges.
    - Mentioned a collaborative project on digital identity for public benefits programs, which is being undertaken with the Center for Democracy & Technology (CDT) and Georgetown University. This project aims to develop guidelines and standards to ensure secure and privacy-preserving digital identity solutions for government programs. Stine emphasized that this project is crucial for modernizing public benefits programs and enhancing their security and efficiency.
    - Referred to a guidance document that serves as a companion to the AI Risk Management Framework (AI RMF). This document is intended to help organizations better understand and implement AI-related risk management practices in alignment with the broader NIST frameworks. Stine highlighted the significance of this guidance in addressing the growing concerns about AI's societal impact.
    - Talked about the ongoing work on age estimation/ verification software, a critical platform for secure digital identity verification in federal services. He explained the role of ensuring secure access to government services while also maintaining user privacy. Stine discussed the challenges and opportunities associated with scaling this platform to meet the needs of an increasingly digital government.
    - Mentioned efforts to enhance the NVD's capabilities by integrating new data sources and automation tools, aiming to improve data quality, reduce the backlog, and ensure timely processing of vulnerabilities. He stressed the importance of maintaining high data quality standards to ensure that NVD remains a trusted resource for the cybersecurity community.
    - Stressed the need for sustained funding to support these critical programs, underscoring the risks that budget cuts pose to NIST's ability to maintain and advance its key initiatives. Stine warned that without adequate funding, NIST could face significant challenges in continuing its mission to provide essential cybersecurity and privacy resources to the nation.
- Cristin Goodwin:
    - Asked about the specific challenges NIST faces in maintaining high data quality within the NVD, given the budget cuts and the increasing volume of vulnerabilities reported. She expressed concern about how these constraints might affect NIST's ability to keep the NVD up-to-date and accurate, which is critical for its users.
    - Inquired about the integration of new data sources into the NVD and how this might impact the timeliness of vulnerability information being made available to the public. Goodwin emphasized the importance of timely updates to the NVD, particularly for organizations relying on this data to protect their systems.
    - Kevin Stine responded by acknowledging the challenges posed by the budget cuts, particularly in maintaining the quality and timeliness of data in the NVD. He explained that the integration of new data sources and the use of automation tools were key strategies to address these challenges. Stine reassured Goodwin that while the volume of vulnerabilities is increasing, the team is committed to ensuring that the NVD remains a reliable and timely resource.
- Marc Groman:

- Asked Kevin Stine how the ongoing collaboration with CDT and Georgetown on the digital identity project is progressing and what specific outcomes NIST expects from this partnership. Groman highlighted the importance of secure digital identity solutions for public benefits programs and expressed interest in how NIST's guidelines might influence broader government policies.
- Inquired about the challenges and opportunities associated with age verification software and login.gov, particularly in terms of balancing security and user privacy. Groman suggested that the success of it could serve as a model for other digital identity initiatives within the federal government.
- Kevin Stine responded by explaining that the collaboration with CDT and Georgetown is progressing well, with the project focusing on developing practical guidelines that can be adopted across various public benefits programs. He noted that the project aims to balance security with privacy, ensuring that digital identity solutions are both secure and user-friendly. Regarding Login.gov, Stine mentioned that the platform's scalability and adaptability are critical factors, and NIST is working closely with other agencies to ensure these aspects are addressed effectively.

3. NIST Cybersecurity and Privacy Update

- Time: 11:15 A.M. – 12:00 P.M.
- Speakers:
  - Matthew Scholl, Chief, Computer Security Division, NIST
  - Rodney Petersen, Director, National Initiative for Cybersecurity Education (NICE), NIST
  - Cristin Goodwin (comments and questions)
  - Marc Groman (comments and questions)
  - Katie Moussouris (comments)
  - Jessica Fitzgerald-McKay (comments)
- Details:
  - Matthew Scholl, Chief, Computer Security Division, NIST:
    - Provided a comprehensive overview of the National Vulnerability Database (NVD), detailing its history, current status, and the challenges ahead. He emphasized the NVD's critical role as a central repository for information on vulnerabilities, serving as a key resource for cybersecurity professionals. Scholl discussed the evolution of the NVD from its origins as a research project to its current status as a vital tool for managing cybersecurity risks.
    - Discussed the collaborative ecosystem that supports NVD, including the roles of Common Vulnerability and Exposure (CVE) numbering authorities, the CVE Board, and the importance of partnerships with organizations like CISA. Scholl highlighted how these collaborations have been instrumental in the evolution and continued success of NVD, noting that the NVD's effectiveness relies heavily on the support and cooperation of these partners.
    - Addressed the ongoing challenge of managing the volume of vulnerabilities reported, outlining the strategies being implemented to reduce the backlog. He explained that while the team is making progress, the high volume of vulnerabilities and the complexity of modern threats make this a continuous challenge. Scholl emphasized the importance of prioritizing vulnerabilities based on their potential impact and the need for timely remediation.
    - Discussed recent improvements to the NVD, including the integration of automation tools that help streamline the processing of vulnerabilities. He also

mentioned efforts to enrich the data within NVD by incorporating additional context and remediation information, making the database more useful for end-users. Scholl stressed that these improvements are part of an ongoing effort to ensure that the NVD remains a trusted and reliable resource for the cybersecurity community.

- Rodney Petersen, Director, National Initiative for Cybersecurity Education (NICE), NIST:
- Provided updates on leadership positions within the Applied Cybersecurity Division, emphasizing the importance of these roles in supporting NIST's broader cybersecurity and privacy objectives. He discussed the ongoing recruitment process for key positions, such as the Chief of the Applied Cybersecurity Division, and expressed confidence that these positions would be filled soon to ensure the division's effectiveness.
- Highlighted the role of NICE in promoting cybersecurity education and workforce development across the United States. Petersen discussed recent initiatives aimed at closing the cybersecurity skills gap and fostering a more diverse and capable cybersecurity workforce. He emphasized the importance of aligning educational programs with industry needs and ensuring that cybersecurity professionals are equipped with the skills necessary to address emerging threats.
- Discussed the work being done at the National Cybersecurity Center of Excellence (NCCoE), focusing on the center's role in developing practical cybersecurity solutions that can be implemented across various industries. Petersen highlighted recent projects related to post-quantum cryptography, emphasizing the importance of preparing for the future challenges posed by quantum computing and ensuring that cryptographic systems are resilient to such threats.
- Mentioned the ongoing development of the Secure Software Development Framework (SSDF), which aims to provide guidance on integrating security into the software development lifecycle. Petersen emphasized that the SSDF is crucial for improving the overall security of software products, particularly in an era where software vulnerabilities are a significant threat to cybersecurity.
- Provided an update on the Cybersecurity Framework (CSF) 2.0 profiles, discussing how these profiles are being developed to address specific sectors and industries. Petersen highlighted that CSF 2.0 is designed to be more flexible and adaptable, allowing organizations to tailor the framework to their unique needs and challenges. He mentioned that the new profiles are expected to enhance the framework's utility across a broader range of use cases.
- Discussed the Federally Funded Research and Development Center (FFRDC) recompete process, explaining that this process is crucial for ensuring that NIST continues to have access to the best research and development resources. Petersen emphasized that the FFRDC plays a vital role in supporting NIST's mission, particularly in areas like cybersecurity research and innovation. He mentioned that the recompete process would help ensure that NIST's partnerships remain strong and effective.
- Mentioned the ongoing efforts to align NICE's educational resources with NIST's broader frameworks, including the Privacy Framework and Cybersecurity Framework. He emphasized the importance of this alignment in ensuring that the next generation of cybersecurity professionals is well-equipped to address emerging threats. Petersen also highlighted the need for ongoing collaboration with educational institutions and industry partners to keep NICE's programs relevant and effective.
- Cristin Goodwin:
    - Added comments on the intersection of privacy and security, particularly in the context of the NVD. She highlighted the broader implications of data governance

in cybersecurity and stressed the need for clear and consistent guidelines that address both privacy and security concerns. Goodwin emphasized the importance of aligning privacy and security frameworks to ensure that organizations can effectively manage both areas without compromising one for the other.
    - Asked about the potential legal implications of emerging cybersecurity threats and how NIST is addressing these issues within the NVD. She expressed concern about the increasing complexity of legal and regulatory requirements and the need for the NVD to help organizations navigate these challenges.
    - Tanya Brewer responded by acknowledging the complexities involved in balancing privacy and security within the NVD. She explained that NIST is actively working to align its frameworks to provide clear guidelines that help organizations navigate these challenges. Brewer also mentioned that the team is exploring ways to incorporate legal and regulatory considerations into the NVD's data structure to better support organizations in meeting their compliance requirements.
- Marc Groman:
    - Raised concerns about the integration of various risk management frameworks and how they apply to both privacy and security. He stressed the need for better alignment across these frameworks to effectively address emerging threats. Groman pointed out that without proper alignment, organizations might struggle to implement these frameworks effectively, leading to gaps in their cybersecurity posture.
    - Highlighted the challenges organizations face in implementing these frameworks, particularly in balancing the need for security with privacy and compliance requirements. Groman emphasized the importance of ongoing collaboration between NIST and industry stakeholders to refine these frameworks and ensure they meet the needs of the broader cybersecurity community.
    - Matthew Scholl responded by agreeing with the need for alignment across frameworks and explaining that NIST is actively working to integrate these frameworks in a way that addresses both privacy and security concerns. He mentioned that emphasized that while budget cuts pose challenges, NIST is prioritizing critical programs and leveraging partnerships to maintain its capabilities.
    - Explained that data quality and timely updates are key challenges, which are being addressed through collaboration with authorized data providers and enhanced automation tools. Feedback from industry stakeholders is crucial in this process, and NIST is committed to ongoing collaboration to refine and improve its frameworks.
- Katie Moussouris:
    - Emphasized the importance of CVE data encompassing more than just base CVSS scores. She clarified that while the CVSS score provided by the NVD is a useful baseline, organizations should be using their own environmental enhancement scores to properly prioritize vulnerabilities based on their specific contexts. Katie further pointed out that relying solely on CVSS scores for prioritization could lead to improper handling of vulnerabilities.
    - Asked about scalability and the ability of NVD to keep up with the volume of CVEs and the timeliness of updates. She mentioned that one of the current drawbacks of the NVD is that it often provides the best estimate of impact at the time a CVE is published, but it doesn’t always get updated with new information as vulnerabilities evolve.

- Jessica Fitzgerald-McKay:
  - Stressed the importance of NIST's role in international standards, particularly in the context of global security and privacy. She noted that NIST's participation in international standards meetings is crucial for ensuring vendor and global interoperability. Jessica emphasized that U.S. industry would be deeply concerned if NIST were to step back from its leadership role in this area, as other nations, like China, might step in to fill the void, potentially undermining global security efforts.
  - Suggested that the board consider formalizing a statement to support NIST's continued involvement in international standards, aligning with the broader goals of the National Cybersecurity Strategy.

4. US National Cybersecurity Strategy Implementation Plan Update / Board Q&A

- Time: 1:00 P.M. – 1:45 P.M.
- Speakers:
  - Nick Leiserson, Office of the National Cyber Director, Executive Office of the President
  - Steve Lipner (facilitating discussion)
  - Board Members (various contributions)
  - Cristin Goodwin (questions and comments)
  - Marc Groman (questions and comments)
  - Katie Moussouris (questions and comments)
  - Alex Gantman (questions and comments)
  - Mike Duffy (questions and comments)
- Details:
  - Nick Leiserson, Office of the National Cyber Director, Executive Office of the President:
  - Provided an in-depth update on the US National Cybersecurity Strategy, focusing on its key objectives, including the 10-year vision for national cybersecurity. Leiserson explained that this long-term vision aims to create a more resilient and secure digital ecosystem, with a particular emphasis on integrating cybersecurity efforts across federal, state, and local levels.
  - Discussed the integration of the Department of Defense (DoD) strategy with the broader National Cybersecurity Strategy. Leiserson highlighted how this integration is essential for ensuring that military and civilian cybersecurity efforts are aligned and mutually reinforcing, particularly in areas such as critical infrastructure protection and defense against nation-state threats.
  - Highlighted the over 100 initiatives that have been launched under the National Cybersecurity Strategy, emphasizing that these initiatives are designed to address a wide range of cybersecurity challenges, from improving threat detection and response capabilities to enhancing cybersecurity education and workforce development.
  - Mentioned the addition of six new Sector Risk Management Agencies (SRMAs), explaining that these agencies will play a critical role in overseeing and enhancing the security of key sectors such as energy, financial services, and transportation. Leiserson noted that these additions are part of a broader effort to strengthen the nation's ability to protect critical infrastructure from cyber threats.
  - Discussed the v2 National Cybersecurity Strategy Implementation Plan, which outlines the steps that will be taken to achieve the strategy's goals. Leiserson explained that this updated plan includes new initiatives and refined priorities based on lessons learned from the initial implementation phase. He emphasized that the v2 plan is designed to be more

agile and responsive to the rapidly evolving threat landscape. Where v1 involved academics heavily, v2 now works to include more private sector.

- Addressed the Cyber Safety Review Board (CSRB) recommendations, specifically focusing on two key areas: the diversion of juveniles involved in cybercrime and the resilience of open-source software (OSS). Leiserson explained that the CSRB has recommended new programs aimed at diverting juveniles from cybercrime by offering them alternative pathways in cybersecurity education and employment. He also discussed the importance of strengthening the resilience of OSS, given its widespread use and the critical role it plays in the digital infrastructure.
- Emphasized the importance of interagency collaboration, with the Office of the National Cyber Director playing a central role in coordinating these efforts across various federal agencies. Leiserson discussed how this coordination is essential to ensuring that the national strategy is effectively implemented and that all relevant stakeholders are aligned in their efforts.
- Highlighted specific initiatives under the strategy, including efforts to improve the security of critical infrastructure sectors such as energy, transportation, and healthcare. He noted that these sectors are particularly vulnerable to cyberattacks and that securing them is a top priority for the Administration.
- Acknowledged the challenges in implementing the strategy, particularly in terms of resource allocation and the need for continuous innovation to stay ahead of evolving cyber threats. Leiserson stressed the importance of fostering a culture of innovation within the federal government and working closely with the private sector to develop new technologies and approaches to cybersecurity.
- Discussed the role of the private sector in the national strategy, emphasizing the need for strong public-private partnerships to effectively combat cybersecurity threats. He highlighted ongoing efforts to strengthen these partnerships and ensure that private sector stakeholders are fully engaged in the national strategy.
- Outlined the next steps in the strategy's implementation, including upcoming initiatives and milestones. Leiserson emphasized that the Administration is committed to regularly reviewing and updating the strategy to ensure it remains effective in addressing the dynamic nature of cybersecurity threats.
- Cristin Goodwin:
    - Asked about the specific measures being taken to ensure that the strategy's objectives are met, particularly in the context of critical infrastructure protection. She expressed concern about the challenges of securing critical infrastructure and inquired about the role of regulatory agencies in enforcing the strategy's guidelines.
    - Inquired about the engagement of private sector stakeholders in the strategy, particularly how small and medium-sized enterprises (SMEs) are being supported in their cybersecurity efforts. Goodwin highlighted the challenges SMEs face in implementing robust cybersecurity measures and the need for tailored support from the federal government.
    - Nick Leiserson responded by explaining that the strategy includes specific initiatives aimed at securing critical infrastructure, including enhanced collaboration with regulatory agencies to ensure that the necessary guidelines are enforced. He also mentioned that the strategy recognizes the unique challenges faced by SMEs and includes measures to provide them with the resources and support they need to improve their cybersecurity posture.
- Marc Groman:

- Asked about the potential impact of the strategy on federal agencies' operational capabilities, particularly in terms of resource allocation and interagency collaboration. He emphasized the importance of ensuring that federal agencies have the necessary resources and support to implement the strategy effectively.
- Inquired about the role of innovation in the strategy, particularly how the federal government is fostering innovation in cybersecurity practices and technologies. Groman suggested that encouraging innovation is essential for staying ahead of emerging threats and maintaining the security of critical infrastructure.
- Nick Leiserson responded by acknowledging the challenges of resource allocation but emphasized that the strategy is designed to optimize the use of available resources through enhanced interagency collaboration. He also highlighted ongoing initiatives to foster innovation, including partnerships with the private sector and academia to develop cutting-edge cybersecurity technologies.

- Board Members:
  - Various board members provided feedback on the strategy, discussing the potential impacts on their respective areas of expertise. Several members highlighted the need for better alignment between the national strategy and existing frameworks such as the NIST Cybersecurity Framework.
  - Board members also discussed the challenges of implementing the strategy at the organizational level, particularly in terms of resource constraints and the complexity of aligning various cybersecurity initiatives. They emphasized the importance of ongoing collaboration between the federal government and industry stakeholders to ensure the success of the strategy.
- Cristin Goodwin:
  - Raised a question about how the six new Sector Risk Management Agencies (SRMAs) would coordinate with existing agencies and whether there would be any overlap in responsibilities. She expressed concern about potential duplication of efforts and the need for clear roles and responsibilities to ensure efficiency.
  - Nick Leiserson responded by explaining that the new SRMAs were carefully chosen to address gaps in sector-specific risk management. He reassured Goodwin that each SRMA had been assigned clear roles to complement the existing agencies, with an emphasis on collaboration and avoiding overlap.
- Alex Gantman:
  - Asked about how the outcomes of the cybersecurity strategy will be measured, emphasizing the difficulty but not the impossibility of doing so. He compared the challenge to outcome measurement in fields like healthcare and crime, which also deal with adaptive adversaries.
  - Nick Leiserson acknowledged the challenge of measuring outcomes in cybersecurity, noting that while there is a strong desire to measure success through outcomes, there aren't many effective metrics currently in place. He highlighted the complexities in measuring impacts, especially when considering the shifting tactics of adversaries. Leiserson discussed the potential risks of focusing solely on metrics like reducing the number of CVEs, as it might lead to unintended consequences such as downgrading reports or discouraging disclosure. He mentioned that they are exploring concepts of success that go beyond just counting CVEs, including incentivizing better security practices and patch adoption.
- Katie Moussouris:

        - Expressed concerns about using the number of CVEs as a metric for success, suggesting that this could create perverse incentives, such as downgrading the severity of vulnerabilities to meet targets. She proposed that a more meaningful measure might be to compare the number of CVEs in the first six months after a software release with the number for older releases, as this could provide insight into whether security is improving over time.
        - Nick Leiserson responded by acknowledging these concerns and noted that they are considering various ways to measure success that account for these complexities. He reiterated the importance of looking at the broader picture and ensuring that any metrics used to evaluate the strategy's success do not lead to negative outcomes.
    - Marc Groman:
        - Commented that the demand for ROI could potentially halt every US government program, expressing that he doesn't know how to measure outcomes in an appropriate way. Groman highlighted the inherent difficulty in establishing concrete metrics for cybersecurity due to the many mitigating or contributing factors involved. Despite these challenges, he emphasized the importance of continuing efforts and not letting the lack of clear metrics halt progress in implementing the cybersecurity strategy.
    - Mike Duffy:
        - Commented on the need for sustained support and resources to implement the cybersecurity strategy effectively, particularly in light of the new responsibilities being placed on NIST. He mentioned that the Administration had recently released a priority document for FY26 and asked how these priorities align with the strategy's implementation.
        - Nick Leiserson responded by explaining that resourcing is a major focus for the Office of the National Cyber Director and that they are working closely with agencies like NIST to ensure they have the support needed to fulfill their expanded roles. He noted that the recent priorities memorandum for FY26 is part of this effort to align budget allocations with the goals of the cybersecurity strategy.
    - Katie Moussouris:
        - Also asked about resources for open-source software (OSS) security and the shared responsibility model. She noted that OSS plays a critical role in the nation's digital infrastructure yet often lacks the resources needed to ensure its security.
        - Nick Leiserson responded by acknowledging that this is an area of concern and that there are still many unknowns about how to best support OSS security. He emphasized that this is an ongoing discussion within the Administration, and they are actively seeking input on how to address these challenges.

5. NIST National Vulnerability Database (NVD) and Vulnerabilities / Board Q&A

- Time: 2:00 P.M. - 3:00 P.M.
- Speakers:
    - Tanya Brewer, Program Manager, National Vulnerability Database, NIST
    - Steve Lipner (facilitating discussion)
    - Katie Moussouris (comments and questions)
    - Giulia Fanti (questions and comments)
    - Board Members (various contributions)

- Details:
    - Tanya Brewer, Program Manager, National Vulnerability Database, NIST:
        - Provided a detailed overview of the current status of the National Vulnerability Database (NVD), highlighting the improvements made in managing the volume of vulnerabilities reported. She noted that NVD is now better equipped to handle this workload thanks to enhanced capacity and improved processes. She mentioned some specifics: 14 TB of data downloaded from NVD per day, 22 people USG and contractor, and reduced 3 federal employees doing analysis per day turning out around 10 new CVEs per day.
        - Discussed the challenges of maintaining data quality within the NVD, emphasizing the importance of accurate and timely vulnerability information. Brewer explained that the team is continuously working to improve the quality of the data within NVD, particularly as new vulnerabilities and threats emerge. She highlighted the ongoing efforts to ensure that the NVD remains a trusted and reliable resource for the cybersecurity community.
        - Highlighted the collaborative efforts between NIST and other agencies, particularly CISA, in enriching the data available in NVD. Brewer mentioned the integration of the Authorized Data Provider (ADP) program, which adds valuable context and remediation information to the vulnerability records, making the database more useful for cybersecurity professionals.
        - Outlined future plans for the NVD, including efforts to sustain and expand its capabilities. Brewer discussed ongoing initiatives to enhance the NVD's infrastructure and user interface, making it more accessible and efficient for end-users. She also mentioned the team's exploration of new technologies and methodologies to further improve the NVD's performance. Brewer emphasized that these improvements are essential for maintaining the NVD's status as a leading resource in the cybersecurity community.
        - Emphasized the need for sustained funding to support these efforts, noting that continued investment in the NVD is critical to maintaining its status as a trusted resource in the cybersecurity community.
        - Addressed a common question regarding the use of AI to perform all analysis tasks related to the NVD. Brewer explained that the description field in CVEs is often unstructured and lacks standardization, making it difficult for AI to process the information effectively. She emphasized that current AI technology struggled with the quality of data available in the CVE descriptions, achieving only about 68% confidence in generating CVSS scores from these descriptions.
        - Discussed the ongoing development of a vulnerability ontology (Vulntology), which aims to standardize the language and descriptions of vulnerabilities. This project, which had been on the back burner for some time, is now gaining prominence. The Vulntology will allow for more precise and consistent descriptions of vulnerabilities, facilitating better communication across systems and potentially improving the effectiveness of AI tools in the future.
        - Introduced the CPE applicability statement tool, which is designed to help streamline the creation of CPE match strings. Brewer explained that creating these strings currently consumes a significant portion of analysis time, and the new tool will help automate this process, allowing for faster and more accurate data handling.
        - Outlined the short-term plans for the NVD, including dealing with the backlog of CVEs and overhauling the internal analysis console, which has not been thoroughly updated in over five years. Brewer mentioned that they plan to

implement improvements to make the console more efficient and user-friendly, allowing analysts to process data more quickly and effectively.
    - Added that NIST plans to overhaul all of the CPE specifications, which have not been updated in over a decade. Brewer explained that this overhaul is necessary to ensure that CPE data is more effectively integrated with modern tools She also discussed the future goal of allowing third parties to provide bulk CPE data directly into the NVD, which would significantly enhance the scalability and efficiency of data processing.
    - Discussed potential future collaborations with industry and academia to improve NVD processes and incorporate advanced AI technologies. Brewer mentioned that companies like Google are interested in using large language models to analyze CVE data, and NIST is considering forming a consortium to facilitate such collaborations. However, she emphasized the importance of not becoming dependent on external resources, advocating for a model that encourages collaboration without sacrificing NVD's internal capabilities.
    - Noted that current staffing levels have not yet returned to their state in 2021, indicating a gradual rebuilding phase but acknowledging that the team is not as large as it was a few years ago.
    - Discussed the impact of staffing levels on the NVD's ability to manage the increasing volume of vulnerabilities. She emphasized that while there has been some recovery, the staffing is not adequate to handle the growth in vulnerabilities without additional resources.
- Giulia Fanti:
    - Asked for clarification on the earlier efforts to use AI for CVSS scoring and the challenges faced. She inquired about the specific inputs and outputs used during these AI experiments and the factors that contributed to the relatively low confidence scores.
    - Tanya Brewer responded by explaining that the AI efforts focused on using CVE description fields to generate CVSS scores, but the unstructured nature of the data made it difficult for AI to achieve high accuracy. She mentioned that the AI could not match the analysts' confidence levels due to missing contextual information that is often found outside the description fields.
    - Fanti suggested that recent advances in AI, particularly in foundation models and retrieval-augmented generation, could potentially improve the accuracy of such tools, especially if they incorporate external data sources.
- Katie Moussouris:
    - Raised concerns about staffing levels and resource allocation at NVD, suggesting the board consider recommending an increase to support NVD's expanding requirements. She also commented on the importance of maintaining NVD as a robust and independent resource, emphasizing collaboration over dependency on external resources. She inquired about the challenges Brewer's team faces in ensuring that vulnerability data is promptly added to the database and whether there are any plans to automate parts of the data entry process to improve efficiency.
    - Asked about the integration of new data sources into the NVD and how these might impact the quality and relevance of the data available. Goodwin highlighted the importance of continuously enriching the NVD to ensure that it remains a valuable resource for cybersecurity professionals.
    - Tanya Brewer responded by acknowledging the challenges of maintaining timely updates, especially with the increasing volume of vulnerabilities. She explained

that the team is exploring automation tools to streamline the data entry process, which would help ensure that the database is updated more efficiently. Brewer also mentioned that the integration of new data sources is being carefully managed to maintain the quality and relevance of the NVD's data.

- Steve Lipner:
  - Inquired about the role of CWE (Common Weakness Enumeration) entries in the NVD, how these entries are managed and utilized within the database and the involvement of CNAs (CVE Numbering Authorities) in proposing CWE entries, seeking clarity on how often this occurs and how these proposals are integrated into the NVD.
  - Tanya Brewer explained that CNAs propose CWE entries in about a quarter of cases, highlighting that these authorities contribute a significant portion of CWE entries in the NVD.
  - Detailed the auditing process conducted by NIST to ensure the accuracy and relevance of CWE entries proposed by CNAs. She emphasized that this process is critical to maintain the integrity and utility of the data within the NVD.
  - Stressed the importance of CWE entries in categorizing and understanding vulnerabilities effectively. She noted that these entries provide essential insights into the nature and implications of security weaknesses.

6. Assessing Risk and Impacts of AI (ARIA) Program / Board Q&A

- Time: 3:15 P.M. – 4:00 P.M.
- Speakers:
  - Reva Schwartz, Principal Investigator, AI Risk Management, NIST
  - Cristin Goodwin (comments and questions)
  - Marc Groman (comments and questions)
  - Giulia Fanti (comments and questions)
  - Alex Gantman (comments and questions)
- Details:
  - Reva Schwartz, Principal Investigator, AI Risk Management, NIST:
    - Introduced the ARIA program, which focuses on assessing the societal risks and impacts of AI systems. Schwartz explained that the program aims to go beyond traditional technical assessments of AI by considering the broader social, ethical, and economic implications of AI technologies in real-world settings. She emphasized that this approach is essential for understanding the full impact of AI on society.
    - Discussed the importance of a multidisciplinary approach in the ARIA program, combining insights from various fields to provide a comprehensive understanding of AI's impact on society. Schwartz emphasized that this approach is necessary for addressing the complex challenges posed by AI, particularly as these technologies become more integrated into everyday life.
    - Introduced three levels of testing within the ARIA program aimed at assessing AI risks and impacts: Model Testing: Verifies that AI models perform as specified; Red Teaming: Involves targeted stress tests on AI systems to identify potential risks and adverse outcomes; Field Testing: Measures the actual impacts of AI systems in scenarios that approximate real-world usage, determining both positive and negative outcomes.
    - Provided examples of ongoing research within the ARIA program, highlighting the need for stakeholder engagement and the inclusion of diverse perspectives to

ensure that the research addresses the most pressing concerns related to AI. Schwartz discussed how the program is working to engage with a broad range of stakeholders, including industry, academia, and government, to inform its research and ensure its relevance.
    - Described the use of specifically designed proxy scenarios that replicate potential real-world implications of AI technologies without exposing participants to harmful content. These scenarios allow for safe, ethical testing while still providing valuable insights into how AI systems operate and impact users in realistic settings.
    - Emphasized the importance of these methodologies in developing a comprehensive risk assessment framework that captures the nuanced effects of AI across various applications and environments.
    - Discussed the program's future direction, including plans to expand research efforts and deepen collaborations with experts from different disciplines. Schwartz emphasized the importance of continued investment in AI research and the need for policies that reflect the complexities of AI's impact on society. She noted that the ARIA program is committed to providing actionable insights that can guide the development of responsible AI policies and practices.
    - Referred to the companion guidance document for the AI Risk Management Framework (AI RMF), which provides practical advice for organizations looking to implement AI-related risk management practices. Schwartz highlighted the significance of this document in helping organizations navigate the challenges of AI and ensure that their practices align with broader NIST frameworks. She emphasized that this guidance is crucial for organizations looking to integrate AI technologies into their operations responsibly.
- Cristin Goodwin:
    - Added comments on the ethical considerations associated with AI, particularly in the context of privacy and data protection. She highlighted the importance of developing AI systems that respect individual rights and comply with privacy regulations, suggesting that the ARIA program could play a key role in shaping the ethical frameworks for AI development.
    - Asked about the role of the ARIA program in influencing AI policy at the federal level, particularly in light of recent developments in AI governance. Goodwin inquired about the program's engagement with policymakers and how its research findings are being used to inform AI-related regulations.
    - Reva Schwartz responded by explaining that the ARIA program is actively involved in providing insights and recommendations to policymakers. She noted that the program's research is designed to inform the development of AI-related policies that are both effective and ethically sound. Schwartz emphasized that the ARIA program is committed to ensuring that its findings contribute to the creation of responsible AI governance frameworks.
- Marc Groman:
    - Contributed to the discussion by emphasizing the need for a balanced approach to AI regulation that considers both innovation and the potential risks associated with AI technologies. He pointed out that overly restrictive regulations could stifle innovation, while insufficient regulation could lead to significant societal harm. Groman suggested that the ARIA program could help strike this balance by providing evidence-based insights that guide policy development.
    - Inquired about the specific challenges Schwartz's team faces in conducting multidisciplinary research on AI and how they are addressing these challenges.

Groman emphasized the importance of integrating diverse perspectives into AI research to ensure that the resulting policies are both effective and equitable.
        - Reva Schwartz responded by acknowledging the challenges of conducting multidisciplinary research, particularly in balancing the various perspectives involved. She explained that the ARIA program is committed to fostering collaboration among experts from different fields to ensure that the research addresses all relevant aspects of AI's impact. Schwartz noted that this approach has been instrumental in developing a comprehensive understanding of AI's societal implications.
        - Discussed the objective of metrics in AI assessment, emphasizing that metrics should be designed to incentivize desired behaviors and outcomes. He highlighted the need for quantitative metrics to properly assess risks and the impact of AI systems.
        - Raised concerns about the practical implementation of AI assessments and the correct approximation of risk, noting that the "something" that might happen (the risk) needs to be clearly defined.
    - Giulia Fanti:
        - Asked about the definition of AI and what counts as AI under the program, specifically questioning whether rule-based systems are included. She expressed concern that the definition might be too broad and include systems not traditionally considered AI.
        - Discussed how the role of data in AI evaluation is critical, especially proprietary training data, which impacts privacy and copyright risks. She pointed out the challenges in assessing risks without access to the actual training data.
    - Alex Gantman:
        - Spoke about the challenges of measuring outcomes in cybersecurity and AI, stressing the need for cultural metrics that align with the operational culture of organizations. He highlighted the difficulty organizations face when security measures conflict with operational priorities.
        - Discussed the broader implications of not knowing whether the interventions or measures taken are genuinely beneficial due to a lack of precise measurement tools.

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

- Time: 4:00 P.M. – 4:15 P.M.
- Speakers:
    - Steve Lipner
    - Cristin Goodwin (comments)
    - Marc Groman (comments)
    - Board Members (brief contributions)
- Details:
    - Steve Lipner:
        - Opened the floor for public comments, although no comments were recorded during the session. He then provided a summary of the day's discussions, reflecting on the progress made in each session.
        - Highlighted the key takeaways from Kevin Stine's update on NIST's budget challenges and leadership changes, emphasizing the importance of these issues in the broader context of NIST's mission.

        - Summarized the discussions on the National Vulnerability Database (NVD), noting the critical role the database plays in national cybersecurity and the ongoing efforts to enhance its capabilities.
        - Reflected on the insights gained from the session on the ARIA program, emphasizing the importance of understanding AI's societal impacts and the need for continued research in this area.
    - Cristin Goodwin:
        - Commented on the importance of continued collaboration between NIST and industry stakeholders to address the challenges discussed during the day. She emphasized the need for a coordinated approach to cybersecurity and AI governance, suggesting that the Board could play a key role in facilitating this collaboration.
        - Highlighted the importance of addressing the ethical implications of AI and suggested that the Board consider these issues in its future discussions. Goodwin noted that the ARIA program's research could provide valuable insights for developing ethical frameworks for AI.
        - Steve Lipner responded by agreeing that the Board should continue to focus on facilitating collaboration between NIST and industry stakeholders. He emphasized that the Board's role in shaping ethical AI governance would be crucial in the coming years.
    - Marc Groman:
        - Echoed Goodwin's comments, emphasizing the need for a unified approach to addressing the challenges discussed during the day. He suggested that the Board should focus on developing recommendations that integrate both technical and ethical considerations in cybersecurity and AI governance.
        - Added that the Board should consider the broader implications of AI and cybersecurity on public trust, suggesting that this could be a focus for future meetings. Groman emphasized the importance of building and maintaining public trust in AI technologies and cybersecurity practices.
        - Steve Lipner agreed with Groman's suggestion, noting that public trust is a critical component of successful AI and cybersecurity initiatives. He mentioned that this topic could be explored further in the next board meeting.
    - Board Members:
        - Several board members provided brief comments, agreeing on the importance of the issues discussed and the need for continued collaboration. They emphasized the importance of integrating the insights gained from the day's discussions into the Board's future recommendations.

8. Day Review and Meeting Recessed

- Time: 4:15 P.M. – 4:30 P.M.
- Speakers:
    - Steve Lipner
- Details:
    - Steve Lipner:
        - Concluded the day's meeting by thanking all participants for their contributions. He summarized the key points discussed throughout the day, emphasizing the importance of continuing the work on the NVD, AI, and other critical areas of cybersecurity and privacy.

- Expressed confidence in the Board's ability to address the challenges identified during the sessions and looked forward to further progress in the upcoming meetings. Lipner noted that the insights gained during the day would be crucial for shaping the Board's future recommendations.
- Recessed the meeting, noting that the Board would reconvene the following day to continue their discussions. He encouraged board members to reflect on the day's discussions and come prepared to build on the progress made during the next session.

Thursday, July 18, 2024

ISPAB Meeting Notes - Day 2

1. DHS Vulnerability Support; KEVs/Vulnrichment/CVE / Board Q&A

- Time: 10:00 A.M. – 11:15 A.M.
- Speakers:
  - Lindsey Cerkovnik, CISA
  - Sandra Radesky, CISA
  - Alex Gantman (questions and comments)
  - Marc Groman (questions and comments)
  - Katie Moussouris (questions and comments)
  - Steve Lipner (facilitating discussion)
  - Board Members (various contributions)
- Details:
  - Lindsey Cerkovnik, CISA:
    - Provided an overview of DHS's Vulnerability Support program, focusing on the KEVs (Known Exploited Vulnerabilities) and the ongoing efforts in Vulnrichment and CVE (Common Vulnerabilities and Exposures).
    - Explained the importance of the KEV catalog in helping organizations prioritize remediation efforts based on the active exploitation of vulnerabilities. Emphasized that the KEV catalog is a critical tool in national cybersecurity, aiding both public and private sectors to focus on the most pressing threats.
    - Discussed the collaboration between CISA and NIST to enrich vulnerability data and ensure that it is comprehensive, accurate, and useful for cybersecurity professionals. Highlighted the role of Vulnrichment in enhancing the CVE data, making it more actionable for end-users.
    - Outlined the process of how vulnerabilities are identified, enriched, and added to the KEV catalog. Stressed the importance of maintaining up-to-date and accurate information to support effective vulnerability management across organizations.
    - Highlighted the milestone achievement of having enriched 240,000 vulnerabilities to date, underscoring the scale and impact of CISA’s Vulnrichment efforts on national cybersecurity.
  - Sandra Radesky, CISA:

- Expanded on Lindsey Cerkovnik's discussion by providing technical details about the enrichment process used for CVEs. Explained how CISA collaborates with vendors and other stakeholders to gather additional context and remediation information for vulnerabilities, which is then integrated into the CVE records.
- Mentioned the challenges of managing a large volume of vulnerabilities and ensuring that the most critical ones are prioritized. Discussed the use of SSVC (Stakeholder-Specific Vulnerability Categorization) as a tool to help prioritize vulnerabilities based on their potential impact on specific stakeholders.
- Highlighted ongoing efforts to improve the quality and timeliness of vulnerability data, including the automation of some aspects of the enrichment process. Emphasized the importance of collaboration with industry partners to enhance the accuracy and relevance of the data.
- Concluded by discussing future plans for Vulnrichment, including expanding the program and incorporating feedback from users to make the data more useful and accessible.
- Noted that only three organizations consistently submit CPE data 100% of the time, indicating a gap in data quality and consistency across different CNAs

- Alex Gantman:
  - Asked about the visibility that vendors have into the data used to classify a vulnerability as a KEV. Expressed concern that vendors might not be fully aware of the criteria used by CISA to determine the inclusion of a vulnerability in the KEV catalog, which could impact their ability to respond effectively.
  - Inquired whether there were plans to provide vendors with more detailed information about the exploitation of vulnerabilities to help them make more informed decisions about mitigation strategies.
  - Sandra Radesky responded by explaining that CISA engages with vendors throughout the process of adding a vulnerability to the KEV catalog. Acknowledged that communication gaps might exist and assured Gantman that CISA is committed to improving communication with vendors to ensure they are fully informed. Mentioned that efforts are underway to provide more detailed and timely information to vendors, which should help close the gap Gantman referred to.
- Marc Groman:
  - Raised a question about the overall process of enriching CVE data and how it is coordinated between CISA, NIST, and other stakeholders. Sought clarification on whether the enrichment process is standardized or if it varies depending on the source of the data.
  - Lindsey Cerkovnik responded by outlining the different steps involved in the enrichment process, explaining that while there is a general framework, the specifics can vary depending on the type of data being enriched and the sources involved. Emphasized that the goal is always to ensure that the enriched data is as accurate and actionable as possible.
  - Matthew Scholl responded in response to a query about the capacity and resources at NIST, Matt clarified that NIST's NVD team comprises 8 analysts and 2 developers, supported by a budget of approximately $7.5 to $8 million. Discussed the challenge of maintaining a high standard across the 390 CNAs involved, pointing out the considerable variation in the quality of CVE submissions which impacts the overall efficacy of the NVD system
- Katie Moussouris:

- Asked about the resources available to CISA for managing the Vulnrichment process, particularly in terms of staffing and funding. Expressed concern about whether CISA has sufficient resources to handle the growing volume of vulnerabilities.
- Sandra Radesky responded by acknowledging that resource constraints are a challenge but emphasized that CISA is continuously working to optimize its processes to manage the workload effectively. Mentioned that additional resources have been allocated to the Vulnrichment team, and CISA is exploring ways to automate the process further to reduce the manual burden.
- Expressed concerns about the pressures CNAs face, including vendors frequently downgrading the severity of vulnerabilities and bug bounty platforms sometimes upgrading them. Emphasized the need for more rigorous oversight to balance the severity ratings and ensure they accurately reflect the risk.
- Lindsey Cerkovnik clarified in Response to Katie and acknowledged the issues Katie raised about CNAs, emphasizing that CISA is currently prioritizing completeness in its data handling, but also recognizes the need to address accuracy and timeliness to enhance the overall quality of CVE data.
- Several board members, including Cristin Goodwin and Marc Groman, expressed their appreciation for the detailed presentation and highlighted the need for ongoing collaboration between CISA, NIST, and other stakeholders to ensure the success of the Vulnrichment program.
- Cristin Goodwin suggested that the Board consider recommending additional resources for CISA to enhance its vulnerability management capabilities, particularly in light of the increasing volume of vulnerabilities and the critical role of the KEV catalog in national security.

2. Identity Management and SP 800-63 / Board Q&A

- Time: 11:30 A.M. – 12:15 P.M.
- Speakers:
  - Ryan Galluzzo, NIST
  - Steve Lipner (facilitating discussion)
  - Marc Groman (comments and questions)
  - Jessica Fitzgerald-McKay (comments and questions)
  - Giulia Fanti (comments and questions)
  - Board Members (various contributions)
- Details:
  - Ryan Galluzzo, NIST:
    - Presented an update on NIST's work on Identity Management and the latest developments in SP 800-63, focusing on the new revisions and how they address emerging challenges in digital identity verification and authentication.
    - Explained the core tenets of SP 800-63, including the emphasis on equitable access, privacy, and security in digital identity systems. Galluzzo discussed the importance of balancing these factors to ensure that digital identity solutions are both secure and accessible to all users.
    - Highlighted specific updates in the latest revision, including new guidance on phishing-resistant authentication and the integration of emerging technologies such as mobile digital wallets. He emphasized that these updates are designed to address the evolving threat landscape and the increasing reliance on digital identity solutions in both the public and private sectors.

- Discussed the feedback received during the public comment period for the latest revision of SP 800-63, noting that NIST received a wide range of comments from various stakeholders, including government agencies, industry representatives, and civil society organizations. Galluzzo mentioned that this feedback has been instrumental in shaping the final version of the document.

- Marc Groman:
  - Added to Goodwin's sentiments, adding that the Board should also consider the role of education and outreach in promoting the adoption of SP 800-63. He suggested that NIST could benefit from additional resources to support these efforts, particularly in sectors that may be less familiar with the guidelines.
  - Inquired about the role of public-private partnerships in the implementation of SP 800-63 and how NIST is engaging with private-sector stakeholders to ensure that the guidelines are practical and effective.
  - Ryan Galluzzo responded by highlighting the importance of public-private partnerships in the development and implementation of SP 800-63. He mentioned that NIST has been actively engaging with private sector stakeholders throughout the revision process and is committed to ensuring that the guidelines are both practical and effective for all users.
  - Expressed concerns about the evolving threat landscape, specifically noting the rise in state-sponsored and highly resourced threat actors who have gained new capabilities over the past few years. He questioned the adequacy of current security measures to counter these threats as digital identity systems are increasingly adopted by various organizations, including state and local governments
  - Ryan Galluzzo responded, noting that NIST is focused on creating robust profiles and implementation guidance that cater specifically to the needs of various public benefit programs, ensuring that digital access remains secure and equitable. Galluzzo also emphasized the ongoing efforts to involve state agencies in discussions about security enhancements and the need for continuous investment in their infrastructures to protect against sophisticated threats.
- Giulia Fanti:
  - Questioned the applicability of mobile driver's licenses and other forms of digital identity to non-drivers, stressing the importance of equitable access to digital identification options.
  - Expressed concern over the metrics for automated document authentication technologies, particularly the high false acceptance rates, and how these could affect equity, especially in terms of false positives and negatives.
  - Ryan Galluzzo responded by affirming the inclusive approach of NIST's guidelines, which are designed to cater to various forms of digital IDs beyond just driver's licenses. He acknowledged the need for continuous improvement in authentication technologies to ensure they meet the required security standards while being equitable and accessible.
- Jessica Fitzgerald-McKay:
  - Inquired about the scope and status of the NCCOE's ongoing project related to identity management. She expressed interest in understanding whether this project was an extension of existing efforts like the mobile driver's license initiative or a new framework to support identity requirements across different NIST projects
  - Ryan Galluzzo clarified that the NCCOE's intention behind its efforts is to establish a core infrastructure that supports various identity-related requirements

without having to rebuild foundational elements for each project. This infrastructure aims to provide a stable set of tools and products that can accommodate the exploration of new hypotheses in identity technologies.

3. NSA AI Security Center (AISC) / Board Q&A

- Time: 1:15 P.M. – 2:30 P.M.
- Speakers:
  - Dr. Tyson Brooks, AISC Tech Director, NSA
  - Steve Lipner (facilitating discussion)
  - Jessica Fitzgerald-McKay (response)
  - Essye Miller (comments and questions)
  - Marc Groman (comments and questions)
  - Mike Duffy (comments and questions)
  - Giulia Fanti (comments and questions)
- Details:
  - Dr. Tyson Brooks, AISC Tech Director, NSA:
    - Provided an overview of the NSA's AI Security Center (AISC) and its role in advancing the security and ethical use of AI technologies within the national security community. Brooks emphasized that AI security is a top priority for the NSA, given the potential for AI technologies to be both a tool and a target in cyber warfare.
    - Discussed the current initiatives within AISC, including research on AI-driven cyber defense systems and the development of ethical frameworks for AI deployment in military and intelligence operations. He highlighted the importance of these initiatives in ensuring that AI technologies are both secure and aligned with national security objectives.
    - Mentioned the ongoing collaboration between AISC and other government agencies, as well as academic institutions, to advance AI research and ensure that the latest advancements are integrated into national security strategies. Brooks emphasized the need for a multidisciplinary approach to AI security, involving experts from various fields to address the complex challenges posed by AI technologies.
    - Provided technical insights into the work being done at AISC, focusing on the development of AI-driven tools for threat detection and response. Brooks explained that these tools are designed to enhance the NSA's capabilities in identifying and mitigating cyber threats in real time, leveraging the power of AI to process and analyze vast amounts of data.
    - Discussed the challenges of ensuring the security and reliability of AI systems, particularly in high-stakes environments like national security. Brooks emphasized that the NSA is committed to developing AI systems that are both effective and resilient, capable of withstanding sophisticated cyberattacks.
    - Highlighted the importance of ethical considerations in AI development, noting that AISC is actively working on creating ethical guidelines for the use of AI in military and intelligence operations. Brooks stressed that these guidelines are crucial for maintaining public trust and ensuring that AI technologies are used responsibly.
  - Essye Miller:
    - Asked about the role of AISC in shaping national AI policy, particularly in the context of cybersecurity and defense. She inquired whether AISC is involved in

providing recommendations to policymakers on the ethical and security implications of AI technologies.
        - Dr. Tyson Brooks responded by explaining that AISC plays a key role in advising policymakers on AI-related issues, particularly those related to national security. He mentioned that AISC's research and insights are regularly shared with policymakers to help inform decisions on AI governance and regulation.
        - Asked about AISC's engagement with industry consortiums focused on content authenticity and deep fakes. She inquired whether the NSA's AI Security Center (AISC) is involved with groups working on combating deep fake technologies. Dr. Tyson Brooks confirmed their involvement, indicating that their researchers are deeply integrated into nearly every consortium addressing deep fake technologies.
    - Marc Groman:
        - Raised concerns about the potential risks of AI technologies being used in cyber warfare, particularly the possibility of AI systems being manipulated or compromised by adversaries. He asked what steps AISC is taking to mitigate these risks and ensure that AI systems remain secure and reliable.
        - Dr. Tyson Brooks and Jessica Fitzgerald-McKay responded by outlining the various security measures being implemented at AISC to protect AI systems from cyberattacks. They mentioned that the NSA is investing heavily in research on AI security, including the development of techniques for detecting and mitigating AI-specific threats. They emphasized that the security of AI systems is a top priority for AISC and that the center is committed to staying ahead of emerging threats.
    - Mike Duffy:
        - Discussed the importance of unified and holistic approaches to AI security across various federal entities. He emphasized the need for better collaboration and alignment of guidance and standards to ensure comprehensive and accessible support for all stakeholders in AI security.
        - Questioned how the NSA's AI Security Center could enhance coordination with other federal efforts and how the board might recommend improving these collaborative processes.
        - Expressed interest in the AISC's specific audience and its collaboration potential. He asked about AISC's focus, whether it is primarily directed towards the Defense Industrial Base (DIB), the Intelligence Community (IC), or broader sectors. Mike Duffy also suggested exploring how AISC's work could be integrated with other federal efforts to enhance the alignment of AI security initiatives across different governmental agencies.
    - Giulia Fanti:
        - Questioned the extent of AISC's work beyond large language models to simpler deployed AI systems. Dr. Tyson Brooks acknowledged that AISC also focuses on these simpler systems, though details remain classified. He highlighted that while much of AISC's work remains under classified settings, they are beginning to engage more with unclassified, national security systems through their presence in the Cybersecurity Collaboration Center.

4. US National CET Standards Strategy / Board Q&A

- Time: 2:30 P.M. – 3:15 P.M.
- Speakers:

- Jayne Morrow, NIST
- Steve Lipner (facilitating discussion)
- Cristin Goodwin (questions and comments)
- Katie Moussouris (questions and comments)
- Jessica Fitzgerald-McKay (questions and comments)

Details:

- Jayne Morrow, NIST:
  - Presented a detailed overview of the US National Critical and Emerging Technologies (CET) Standards Strategy, focusing on its extensive scope that includes AI/ML, networking, digital ID, quantum, and semiconductors. Morrow discussed the development of a 5-year implementation roadmap aimed at enhancing collaborative efforts among academia, industry, NGOs, the US government, and foreign governments. She emphasized the need for the standards to evolve to meet the challenges of current and future technologies, ensuring robust national security and maintaining a leadership position in global innovation.
  - Explained the creation of the implementation roadmap, which seeks to foster greater collaboration and integration of diverse inputs from multiple sectors. This roadmap is designed to guide the strategic alignment of standards with technological advancements, ensuring they are adaptive and comprehensive.
  - Highlighted visa wait times as a significant barrier to international participation in standards development. Morrow advocated for policy reforms to streamline visa processes to enable greater and more effective global collaboration. She emphasized the critical role of international experts in enriching the U.S. standards setting process and contributing to technological initiatives.
  - Stressed the strategic importance of the CET Standards Strategy in addressing global technological challenges and maintaining national security. Morrow called for proactive engagement with industry stakeholders to align the standards with the real-world applications and needs of the cybersecurity workforce, underscoring the need for continuous adaptation and responsiveness to the dynamic tech landscape.
- Cristin Goodwin:
  - Addressed the national security implications of the CET Standards Strategy, particularly highlighting the challenge posed by the PRC's proactive involvement in standards committees. She raised concerns about the potential for foreign governments, notably the PRC, to influence critical standards, which could impact global technology regulations and U.S. strategic interests. Goodwin sought insights on strategic discussions that might be necessary to counteract these influences and asked how the board could support NIST's strategic objectives in this complex geopolitical landscape.
- Katie Moussouris:
  - Discussed the financial barriers that prevent smaller entities from participating in standards development. She noted that while consortia provide a platform for collaboration, the "pay to play" nature often excludes vital, innovative players due to high costs. Moussouris emphasized the role of NIST in reducing these barriers and suggested that government-supported frameworks could enable more inclusive participation across a broader range of stakeholders, thereby enhancing the diversity and richness of the standard-setting process.
- Jessica Fitzgerald-McKay:
  - Expressed concerns about the risks associated with insufficient NIST participation in international standards bodies, particularly given budget constraints that limit NIST's

engagement capabilities. She stressed the importance of NIST's active involvement in shaping international standards, which have direct impacts on national security and privacy. Fitzgerald-McKay advocated for increased coordination within the U.S. government to ensure that NIST and other agencies could contribute more effectively to international standards development. She highlighted the need for a unified approach to maximize the impact and efficiency of U.S. participation in global standards settings.

5. Final Board Reviews, Recommendations, and Discussions

- Time: 3:30 P.M. – 4:30 P.M.
- Speakers:
    - Steve Lipner, Chair, ISPAB
    - Board Members (various contributions)
    - Mathew Scholl (NIST)
    - Alex Gantman
    - Cristin Goodwin
    - Katie Moussouris
    - Giulia Fanti
    - Jessica Fitzgerald-McKay
    - Mike Duffy
- Details:

- Steve Lipner:
    - Led the final session of the day, summarizing key points from previous discussions and facilitating a broader review of the Board's recommendations and next steps.
    - Emphasized the need to translate the day's insights into actionable recommendations, with a focus on international standards, AI governance, NVD challenges, and security metrology.
    - Encouraged board members to reflect on how to support ongoing efforts in cybersecurity and privacy through well-crafted letters and follow-up discussions.
- Board Members:
    - International Standards:
        - Jessica Fitzgerald-McKay highlighted the risks associated with insufficient U.S. participation in international standards development. She stressed the importance of NIST's involvement, despite budget constraints, and advocated for the board to recommend that NIST's participation in international standards setting remain a priority. Steve Lipner supported this recommendation, and Matthew Scholl noted that such a recommendation would be helpful for resource prioritization within NIST.
        - The Board agreed to move forward with drafting a letter emphasizing the importance of engaging in international standards setting, including securing resources for NIST participation and coordination across the U.S. government (USG).
    - AI Security and Privacy Frameworks:
        - Giulia Fanti raised concerns about the premature development of AI security and privacy standards, especially given the uncertainties around AI's capabilities and vulnerabilities. Mike Duffy added that there is a need to ensure coordination between NIST, NSA, and CISA to develop harmonized AI security frameworks.

        - The Board agreed that coordination of AI security and privacy frameworks across the government is critical and that a recommendation or letter should address the importance of a unified approach to these challenges.
    - NVD Challenges and Recommendations:
        - Steve Lipner and Katie Moussouris discussed the challenges posed by the National Vulnerability Database (NVD), particularly regarding the completeness and quality of CVE submissions. Moussouris emphasized the need for training for CNAs to ensure that vulnerability data is accurate and comprehensive. Steve Lipner noted the tension between scalability and quality in addressing NVD gaps.
        - The Board agreed to move forward with a letter recommending the prioritization of resources to address these challenges, as well as exploring new technical and organizational approaches to improve NVD's effectiveness.
    - Security Metrology:
        - Alex Gantman and other board members discussed the need for a follow-up discussion on security metrology, specifically how outcomes (as opposed to outputs) can be better measured. The importance of creating frameworks to measure security outcomes, and the need for NIST to address these challenges, was emphasized.
        - The Board requested a deeper dive into security metrology at a future meeting, with potential discussions involving outside stakeholders such as DOJ or FBI to talk about real-world data collection.
    - Other Contributions:
        - Cristin Goodwin suggested that the Board should focus more on the intersection of cybersecurity and AI in future meetings, given the growing relevance of AI technologies in both national security and commercial settings. She also emphasized the need for ethical considerations in AI governance.
        - Katie Moussouris highlighted the need for increased support for CNAs in generating quality vulnerability data, while noting that financial and structural barriers limit participation in vulnerability management processes.
        - The Board discussed the potential for public-private partnerships and international collaboration to further enhance cybersecurity capabilities and standards development, with Cristin Goodwin and Steve Lipner emphasizing the importance of these collaborations for advancing global cybersecurity efforts.

Key Action Items:

1. Draft letters on:
    - The importance of engaging in international standards setting, including securing resources for NIST participation and improving USG coordination.
    - Coordinating AI security and privacy frameworks across NIST, NSA, CISA, and other government agencies.
    - Addressing the challenges posed by the NVD, including improving the quality of vulnerability submissions and exploring new approaches to close existing gaps.
2. Follow-up discussion on security metrology, with a focus on measuring security outcomes and the potential involvement of external experts (e.g., DOJ or FBI).
3. Plan future meetings to address cybersecurity and AI governance, public-private partnerships, and other emerging topics.

Next Meeting

- To be conducted November 6-7, 2024. The meeting will be held virtually.

A motion was made and seconded to adjourn the meeting. The Chair thanked everyone for their participation and adjourned the meeting.

ISPAB – July 17 and 18, 2024		
Last name	First name	Affiliation
Board members		
Fanti	Giulia	Carnegie Mellon University
Fitzgerald-McKay	Jessica	NSA
Gantman	Alex	Qualcomm
Gattoni	Brian	Federal Reserve Board
Goodwin	Cristin	Advancing Cyber
Groman	Marc	Privacy Consulting
Duffy	Mike	CISA - DHS
Lipner	Steve	SafeCode
Miller	Essye	Executive Business Management
Moussouris	Katie	Luta Security
Nist staff		
Brewer	Jeff	NIST
Scholl	Matt	NIST
Petersen	Rodney	NIST
Stine	Kevin	NIST
Speakers		
Lipner	Steve	Board Chair / SAFECode
Stine	Kevin	NIST
Scholl	Matt	NIST
Petersen	Rodney	NIST
Leiserson	Nick	ONCD
Brewer	Tanya	NIST
Schwartz	Reva	NIST
Gazlay	Jay	CISA - DHS
Cerkovnik	Lindsey	CISA - DHS
Donovan	Kevin	CISA - DHS
Radesky	Sandra	CISA - DHS
Galluzzo	Ryan	NIST
Mammen	Tahira	NSA
Brooks	Dr. Tyson	NSA
Morrow	Jane	NIST
Registered attendees		
Srividya	Ananthakrishna	NIST
Chad	Boutin	NIST
Tanya	Brewer	Speaker (NIST)
Jeff	Brewer	NIST
Tyson	Brooks	Speaker (NSA)
Jordan	Burris	Socure
Robert	Byers	NIST
Laura	Calloway	NIST
Nelbin	Castro	iCloud

Safira	Castro	IBM
Lindsey	Cerkovnik	Speaker (CISA)
Boutin	Chad	NIST
Yolanda	Cuervo López	Proton
Anne	Dames	IBM
Sandra	Darkson	University of New Hampshire
Kevin	Donovan	Cisa
Justin	Doubleday	Federal News Network
Harry	Doyle	HD Healthcare
Said	El Hamdani	Lockheed Martin
Sara	Friedman	Inside Washington Publishers
Roger	Gaffey	IBM
Ryan	Galluzzo	Speaker (NIST)
Jay	Gazlay	CISA
Joseph	Guirreri	Cyberalus
Bill	Gulledge	American Chemistry Council
Mat	Heyman	Impresa Management Solutions
Zachary	Howell	Hill East Group
Katie	Ignaszewski	IBM
Karen	Kaya	CrowdStrike
Jason	Kerben	State Dept.
Jennifer	Kerber	Socure
Sara	Kerman	NIST
Alaina	Kuehne	ISL Education Lending
Naomi	Lefkovitz	NIST
Nick	Leiserson	Speaker (NCD.EOP)
Tom	Leithauser	Wolters Kluwer
Jacob	Livesay	Inside Washington Publishers
Kirk	Lurie	HII
Devin	Lynch	Executive office of the President
Sudeep	Maharana	
Tahira	Mammen	NSA
Art	Manion	Analygence
Jordan	Marozine	The Barber Studio
Lisa	Marth	NIST
Sean	McGinnis	HII
Jane	Morrow	Speaker (NIST)
Patrick	Nwadiani	Secure Aid Security Group
Madison	Oliver	GitHub
Rodney	Petersen	NIST
Raheel	Qamar	Treasury
Sandra	Radesky	Speaker (CISA)
Arshitha L	Reddy	

Christine	Richards	NIST
Kamie	Roberts	NIST
Chris	Robinson	Intel
Nelson	Ross	HII
Vincent	Ross	EPA
Renault	Ross	Globalnsc
Matthew	Scholl	NIST
Reva	Schwartz	Speaker (NIST)
Stew	Scott	Atlantic Council
Nichole	Seabron	National Association of State Credit Union Supervisors
Annie	Sokol	HII
Scott	Stankus	NIST
Yalonda	Stanley	
Alexander	Stein	NIST
Ed	Stoner	Analygence
Harry	Toor	
Brianna	Townsend	CISA
Rosa	Underwood	GSA
Desiree	Vanderloop	CrowdStrike
Tim	Warren	Warren Communications News
Rick	Weber	Inside Washington Publishers
Peter	Weinberger	Google

Certified and approved by

Steven B. Lipner
Chair
Information Security and Privacy Advisory Board