INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

Established by the Computer Security Act of 1987
[Amended by the Federal Information Security Management Act of 2002]

MEETING MINUTES

March 1 & 2, 2023
Grand Hyatt Washington
Quarter Penn A Room, 1000 H Street, N.W., Washington, DC 20001
(This was an in-person only event)

Board Members

Steven Lipner, SAFECode, Chair, ISPAB
Brett Baker, Inspector General at the National Archives
Giulia Fanti, Carnegie Mellon University
Jessica Fitzgerald-McKay, National Security Agency
Alex Gantman, Qualcomm
Brian Gattoni, US Federal Reserve Board
Cristin Goodwin, Microsoft
Marc Groman, Groman Consulting
Katie Moussouris, Luta Security

Absent with Regrets:
Arabella Hallawell, WhiteSource
Douglas Maughan, National Science Foundation
Essye Miller, Executive Business Management
Philip Venables, Google

Board Secretariat and NIST staff

Matt Scholl, NIST
Jeff Brewer, DFO, NIST
Jim St. Pierre, NIST
Kevin Stine, NIST
Annie Sokol, Exeter Government Services LLC

** Meeting announcement https://csrc.nist.gov/Events/2023/ispab-march-2023-meeting, and Meeting Agenda can be found https://csrc.nist.gov/Projects/ispab/meetings*

*** Presentations provided by presenters can be found https://csrc.nist.gov/Events/2023/ispab-march-2023-meeting*

**** Footnotes are added to provide relevant or additional information*

Wednesday, March 1, 2023

Welcome and Remarks
Board Introduction and Member Updates on Recent Activity
Review of Schedule and Discussion of Potential Issue Areas

Steve Lipner, Chair, ISPAB, Executive Director, SAFECode

- The Chair opened the meeting at 10:02 a.m. ET and welcomed everyone to the in-person meeting.
- The Chair mentioned that he sent out a note to the board suggesting potential questions and discussion topics for the items on the Board's agenda last week.

- He briefly explained the structure and purpose of the ISPAB [1], and stated that, while the board provides formal input to the NIST, DHS and OMB with board letters, the members' comments and questions during the sessions with speakers also add value.
- For the visitors, he covered Federal Advisory Committee Act (FACA) committee rules including rules for asking questions.
- The Chair welcomed Alex Gantman, a new member of the Board to his first meeting.
- The Chair stated that Chuck Romaine who usually attended the ISPAB as the NIST ITL Director is currently detailed to a management role at NIST. In his absence, Jim St. Pierre is now the Acting ITL Director. He welcomed Jim to the Board.
- Following the introduction, the Board members in attendance are traditionally given the opportunity to introduce themselves and to include any updates on their recent activities.

Board Member Introductions and Updates

Brian Gattoni, US Federal Reserve Board
Brian Gattoni was formerly with CISA and has taken on a new role with the Federal Reserve Board as the Assistant Director for cyber strategy responsible for cybersecurity governance of the Federal Reserve System and not the IT system.

Alex Gantman, Qualcomm
Alex Gantman has been with Qualcomm for over 20 years working in cybersecurity in multiple divisions.

Katie Moussouris, Luta Security
Katie Moussouris is involved in three different Federal advisory boards, two of which (including the ISPAB) meet this week.

Jessica Fitzgerald-McKay, NSA
Jessica Fitzgerald-McKay is the co-lead for NSA's Center for Cybersecurity Standards.

Marc Groman, Groman Consulting
Marc Groman is a Privacy consultant and advisor. He is in the process of reviewing the American Data Privacy and Protection Act (ADPPA), a draft federal privacy law. He is focusing on vague and ambiguous definitions, undefined terms, and the inconsistent and imprecise use of different words to mean the same or similar ideas. Without significant revisions to the text, he is concerned that the enacted ADPPA will be bogged down in courts for years as judges attempt to divine the intent of Congress.

Brett Baker, US National Archives & Records Administration
Brett Baker is the Inspector General at the National Archives. His responsibilities include FISMA reporting which will be covered during the March 2 agenda.

[1] ISPAB - Overview, Charter, and scope and objectives https://csrc.nist.gov/projects/ispab

Giulia Fanti, Carnegie Mellon University
Giulia Fanti is an assistant professor with the Department of Electrical and Computer Engineering of Carnegie Mellon University. Her research includes encrypted proof, machine learning, cryptocurrencies, privacy and anonymity.

Cristin Goodwin, Microsoft
Cristin Goodwin is Associate General Counsel for Cybersecurity and Digital Trust at Microsoft, and she is currently consumed with work on Ukraine response, national resiliency, dealing with the EU draft Cyber Resilience Act, and incident response.

Mandatory Ethics Briefing [2]

US Department of Commerce, OGG Ethics

ISPAB Members are either federal employees or Special Government Employees (SGEs) [FACA]. This ethics [3] briefing is an annual required training that is presented to ISPAB members.

Conflict of interest [4] - members are not to represent their interest or employers', and when a situation arises where there is a conflict of interest, members should rescue themselves. If in doubt, members should contact the presenter.

Misuse of Position [5] - Members shall not use their position in partisan political activities, nor to support any political candidacy, including any side discussion during the Board meeting. Neither government resources nor any confidential government information discussed during board meetings, can be used for the benefit of members' private interest nor shared or released to influence the issuing of any contact. Members should exercise judgment in the use of their roles as board members as part of their credentials for any activity outside the context of the Board.

The rules are applicable across federal agencies. Each agency interprets the policies differently and can stipulate additional conditions. Board members can reach out to the presenter if they have further questions.

[2] https://www.oge.gov/web/oge.nsf/Resources/Summary+of+the+Ethics+Provisions+that+Apply+to+Special+Government+Employees+(SGEs)

[3] https://extapps2.oge.gov/Training/OGETraining.nsf/xsp/.ibmmodres/domino/OpenAttachment/training/ogetraining.nsf/D006291C1FEC02448525869C005BD4B8/Body/EthicsLawsApplicabletoSGEs.pdf

[4] The general prohibition under Section 208 described for non-SGEs and SGEs applies equally to FACA SGEs, as does the provision in subsection (b)(2) of Section 208 for waiver by regulation (when the financial interest is too remote or inconsequential to affect the integrity of an employee's service).

[5] For further information regarding specific misuse concerns about representational activities of SGEs, see OGE Informal Advisory Opinion 00 x 1 (Feb. 15, 2000), at 10-11.

NIST Information Technology Laboratory (ITL) Update

Jim St. Pierre, Acting ITL Director <presentation provided>

There are lots of changes at NIST – Jim Olthoff is moving on to be the NIST Chief Metrologist, and Chuck Romaine is assuming Jim's role and responsibilities as the Associate Director for Laboratory Programs effective the beginning of February. Jim (the presenter) is now the Acting Information Technology Laboratory Director in Chuck Romine's absence. The Director's priorities focus on critical and emerging technology leadership, e.g., for smart grid, ITL on-going environmental work, standards leadership, manufacturing, mission delivery enhancement, and NIST community (diversity and inclusivity). They all are interesting challenges.

This is an exciting time for the CHIPS Act. At a glance, NIST is involved in the research and development, coordination on research facilities, work with manufacturing, and aligning work on on-going internal programs.

On Artificial Intelligence (AI), NIST is directing attention to cultivating trust in the design, development, use and governance of AI technologies and systems. NIST is working closely with the National Science Foundation (NSF), leading the National AI Advisory Committee, TTC (US-EU Trade and Technology Council[6]) and other stakeholders, with the focused emphasis on public-private partnership and social impact.

Cybersecurity Framework (CSF) – NIST started a journey to update the CSF (V2.0) [7] with the release of a concept paper for comments. The virtual workshop on CSF on February 15, 2023,[8] was attended by over 1500 people from the US and other countries. A follow-up in-person working session on February 22-23, 2023[9], received 100+ attendees.

The draft fourth revision of NIST SP 800-63-4, Digital Identity Guidelines,[10] was released for review with feedback due by March 24, 2022. Several webinars are in planning. FIPS 186-5 Digital Signature Standard (DSS)[11] [supersedes FIPS 186-4] was published on February 3, 2023. This standard specifies a suite of algorithms that can be used to generate a digital signature, and it is related to Special Publication (SP) 800-186[12] Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters that was also published in February 2023. On that note, NIST announced in December 2022 plans to phase out SHA-1 by December 31, 2030, in favor of the more secure SHA-2 and SHA-3 groups of algorithms.

NCCoE is busy with many activities - supply chain assurance, an application profile for hybrid satellite network cybersecurity, a profile for 5G network cybersecurity is out for comment, and projects are under way addressing

[6] https://www.google.com/url?sa=i&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=0CAQQw7AJahcKEwjg1Iu8w_z9AhUAAAAAHQAAAAAQAg&url=https%3A%2F%2Fwww.nist.gov%2Fsystem%2Ffiles%2Fdocuments%2F2022%2F12%2F04%2FJoint_TTC_Roadmap_Dec2022_Final.pdf&psig=AOvVaw2BOG_advJD3JEcsnjIQ2l-&ust=1680020824115582

[7] Update Process for Cybersecurity Framework: https://www.nist.gov/cyberframework/updating-nist-cybersecurity-framework-journey-csf-20

[8] https://www.nist.gov/news-events/events/2023/02/journey-nist-cybersecurity-framework-csf-20-workshop-2

[9] https://www.nist.gov/news-events/events/2023/02/journey-nist-cybersecurity-framework-csf-20-person-working-sessions

[10] https://www.nist.gov/identity-access-management

[11] https://csrc.nist.gov/publications/detail/fips/186/5/final

migration to PQC / PKI replacement, cybersecurity of genomic data, and securing water and wastewater utilities.

Jim St. Pierre described new and emerging areas of interest to include space cybersecurity – working with the Department of Commerce and mapping to CSF; automotive cybersecurity – an initial public-private partnership that is planning upcoming webinars; cybersecurity of genomic data; and privacy enhancing technologies. The efforts seek to help researchers to define what needs to be secured and address the challenges of defining cybersecurity measurement.

In 2022, NIST celebrated 75 years of applied mathematics and statistics, 50 years of cybersecurity research, and 60 years of biometrics research. ITL has launched a website on the NIST cybersecurity program's history and timelines. In taking a walk-through time, NIST Cybersecurity program website[13] demonstrates the range of cybersecurity topics that ITL has worked on.

Before he closed, Jim mentioned that NIST Director Laurie Locascio was elected an AAAS Fellow, and that the NIST Information Technology Image group was recognized for its service and leadership at the 2022 Federal Identity Forum, and that Drs. Kamran Sayrafian and Raghu Kacher were named Fellows of the Washington Academy of Sciences.

Board's discussion

- MD5 (message-digest algorithm) cryptographic function: It is globally relevant and whether NIST is or did research on it. It is noteworthy that NIST is long proven to be a good initiator in collaborating research and information in pursuing work on this topic, e.g., best practices, coordination with CISA, developing standards that can benefit industry, vulnerability notification, expectation, and incident response.
- The Board asked about status on possible work on Cryptography quantifiable clarity, and migration protocol

Updates on Agency Zero Trust Architecture (ZTA) and Software Attestation

Chris DeRusha, Federal Chief Information Security Officer, Office of Management and Budget

Chris DeRusha emphasized the importance of Zero Trust Architecture (ZTA) and that the ZT strategy is the umbrella to post many policies. M-22-09[14] was released publicly in January 2023. This memorandum sets forth a Federal zero trust architecture (ZTA) strategy, requiring agencies to meet specific cybersecurity standards and objectives by the end of Fiscal Year (FY) 2024 to reinforce the Government's defenses against increasingly sophisticated and persistent threat campaigns. The memo sets out strategic goals aligned with CISA's five pillars as an updated and best starting point, and a good basis for benchmarking. It provides fundamentals for implementation, and a performance matrix (Appendix B) as a comprehensive approach to help agencies to resource responsibly.

[12] https://csrc.nist.gov/publications/detail/sp/800-186/final
[13] https://csrc.nist.gov/nist-cyber-history
[14] M-22-09 Moving the U.S. Government Toward Zero Trust Cybersecurity Principles
https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

Budget designated for zero trust is allocated in response to agency requests as a strategy to momentum begin toward doing the appropriate thing. The strategy is about doing the right thing, but how well we appropriate funding will be key in driving progress. The strategy also seeks to drive agencies to start working towards the goals sooner.

Board discussion: In responding to questions about the challenge of pressing agencies to create their programs and the ability to secure the enterprise, a culture challenge exists, but it is necessary to press on maintaining progress to get everyone to implement the strategy. The Board asked if there are any attempts to gather examples and lessons learned. The presenter stated that the focus is on learning in managing cyber risks and getting to a manageable state. There are efforts to gather terms and map them to common definitions to gauge where the agencies are making progress on their investments – measurable in various levels, e.g., system level, to determine the actual state. The presenter reiterated the steps to gather all the terms and search for what we are looking for mapping to determine the appropriate tooling is used. Next step is to have definitions across for mapping and tracking as a performance measurement. Many things can be measurable at system level, annual level, etc. to define the gaps and perpetuity processes. The agencies can figure out the most actualized version used and critical vulnerability risks, and then focus on the hurdles to eliminating the actualized risks that they are facing. The Board observed that it is important to measure outcomes and not efforts. The presenter affirmed that the focus on outcomes is the ultimate goal to breaking down risks.

M-22-18[15] Enhancing the Securing of the Software Supply Chain through Secure Software Development Practices released on September 14, 2022, is based on Executive Order (EO) 14028, Improving the Nation's Cybersecurity (May 12, 2021), using OMB authority to direct requirements per NIST guidance – NIST SP 800-218 and the NIST Software Supply Chain Security Guidance[16]. The memo was socialized, and a document based on feedback received will be released and announced via Federal Register Notice. The Board commented that releasing a document is simple but getting effective assurance may not be as simple. While the focus is on gathering data to track progress, documenting procedures cannot fully provide evidence of assurance.

The Board asked about the report on the Commonly Exploited Vulnerabilities and of the approximately 1.2 – 1.4M unpatched endpoints, many of which are due to under-resource and non-compliance. The presenter pointed to stronger authentication/password and to follow the discussed process and tracking of risks. The session ended with no extended discussion on this topic.

[15] M-22-18 https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf
[16] https://www.nist.gov/system/files/documents/2022/02/04/software-supply-chain-security-guidance-under-EO-14028-section-4e.pdf

The US Government National Cybersecurity Strategy [17] [18] [19] [20]

Drenan E. Dudley, Assistant NCD for Budget Review and Assessment, Office of the National Cyber Director (ONCD)

The presenter left Capitol Hill and joined ONCD six months ago to work on federal network security under Chris Inglis. ONCD is maximizing inter-agency coordination and supporting the private sector, to establish security in cyberspace. We have a lot of legislation and hold a huge amount of information. The cybersecurity Executive Orders (Eos) have mandated many strategy documents. Strategies are tools, and can help in designing systems that are defensible, resilient, and aligned with our values. There are lots of investments in cyber, but we need to invest in a good strategy that is resilient. With resilience, when defenses fail, the consequences are not catastrophic, and recovery is seamless and swift. Cyber incidents should not have systemic real-world impacts. Technology is shaped by the rest of our society as we rebalance the responsibility for managing cyber risks. ONCD is in collaboration with private industry and agencies, and we have received hundreds of contributions and are taking time to internalize the conversation. We need to rethink who makes us secure and expect some leadership from industry including cloud service providers and other internet companies along with developers of software, manufacturers of hardware and other key players. Risk is often pushed down to the smaller companies. We need to think about long term investment and solutions, and not be tempted to focus on short term, easy quick fixes.

In evaluating the long-term benefits, we depend on information availability to enable decision making. In determining how to set aside investment for federal network security, federal agencies must determine what they need before basing decisions on what is known. How we can be more secure and where are things more fragile are questions that will take time to answer before we have a vision of functions, to flesh out details without being reactive as we make decisions about spending. An implementation plan will be provided to agencies in the coming months to help alignment in adopting the National Cybersecurity Strategy. It will be the agencies' responsibilities to implement the plan. Apart from asset management, having the right people on hand to address and align the plan with appropriate resources will help to keep from simply doing quick fixes. There is a constant discussion about problems that result from operation not being controlled by agencies' CISOs but by others. The implementation plan should set the directions to ensure that the budget reflects the priorities of both the implementor and CISO. Priorities are identified and justified to ensure they are met. The implementation plan will provide clarity for the agencies to enforce their implementation. A workforce strategy is in the works for release.

Board discussion: The Board commented that people cost vs. other costs and that there are a number of ways that people function, e.g., contract. As a cautionary condition, every grant or program needs to consider if cyber

[17] Fact Sheet https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/

[18] National Cybersecurity Strategy chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[19] discussion on the Strategy with remarks from Acting National Cyber Director Kemba Walden and Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger, March 2, 2023 (2-3:00 PM) at CSIS https://www.csis.org/events/biden-harris-administrations-national-cybersecurity-strategy https://www.youtube.com/watch?v=6Fwtvcf2A2c

[20] Briefing at CSIS https://www.youtube.com/watch?v=6Fwtvcf2A2c

security is included in the consideration but is not a requirement. The Board asked whether there is an estimate of a total cost for investment as each agency's effort varies and can result in different total expenditure/cost. In addition, agencies often struggle to fulfill their allocation within the assigned cycle and meeting the acquisition process.

M 22-16 Administration Cybersecurity Priorities for the FY 2024 Budget[21]

Drenan E. Dudley, Assistant NCD for Budget Review and Assessment, Office of the National Cyber Director (ONCD)[22]

It is relevant to begin with the budget process for federal government. There are many policy councils, and each has its own role. Proposals are discussed between the National Security Council and other councils. We are in the cycle, developing a budget for almost two years in the future. Federal agencies should now be thinking about budgets for 2025. Currently, the agencies are spending money that was planned three years ago. In essence, agencies are spending money while they do not have full knowledge and understanding between the cycle of approval and budget initiation. In crafting a proposed allocation, agencies are to include funding requests for the year, but OMB needs to consider further details to ensure that they balance the budget rollout.

The memorandum will provide instructions to begin the hard work of implementation. The government needs to stay coordinated and put funding and investment where it should be and be accountable to the goals prescribed. A partnership between ONCD and OMB will set up agencies to think about cybersecurity. Agencies have a role to play and should be sure to request funding to ensure everything is implemented accordingly – keeping pace with people, skill set needed, and resources. The FY2024 budget will be released next month and the FY2025 memo is planned for released April/June this year. The presenter is willing to return in future meeting to provide updates on this topic.

Board discussion: The Board noted that people cost versus other costs varies as there are many ways people function, e.g., under contract. The presenter responded that agencies need to consider cyber for each grant or program as a cautionary condition. On whether ONCD has in mind a total cost for investment, each agency's effort varies resulting in varied total cost. Many agencies struggle to fulfill the allocation within the cycle assigned as well as meeting the acquisition process. The Board found the information helpful and informative.

[21] M-22-16 Administration Cybersecurity Priorities for the FY 2024 Budget chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.whitehouse.gov/wp-content/uploads/2022/07/M-22-16.pdf

[22] https://www.whitehouse.gov/oncd/briefing-room/2022/08/30/office-of-the-national-cyber-director-announces-appointments-made-since-its-establishment/

NIST Risk Management Framework Overview

Vicky Pillitteri, NIST <presentation provided>

[this presentation replaced the initial agenda topic, *CISA Federal Agency Incident Reporting Requirements, Successes and Challenges* – Brian Dewyngaert, CISA]

The presenter explained that Risk Management Framework is federal agency guidance for security programs. NIST publications are used by federal agencies. The key driver for RMF is FISMA (Federal Information Security Management Act of 2002)[23]. SP 800-37 Rev. 2[24] (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy was developed by the Joint Task Force Transformation Initiative Working Group. SP 800-37 is mandated by OMB A-130[25] "Managing Federal Information as a Strategic Resource," that requires executive agencies within the federal government to: 1) Plan for security; 2) Ensure that appropriate officials are assigned security responsibility; 3) Periodically review the security controls in their systems; and 4) Authorize system processing prior to operations and, periodically. The publication provides a process that can be used across all federal agencies and provided commonalities for federal agencies to implementing security controls.

An overview on RMF – RMF provides a structured, yet flexible process for managing cybersecurity and privacy risk. The first revision aimed to transform the traditional Certification and Accreditation (C&A) process into the Risk Management Framework (RMF), and the second version addressed privacy controls in a more central manner and added a preparatory step. This publication is high level and holistic. It is flexible in addressing cybersecurity and privacy, and applicable to all types of systems and organizations. The Risk Management Framework has seven steps – Categorize, Select, Implement, Assess, Authorize, Monitor, and Prepare.

The process includes 6-steps[26] of essential activities to prepare the organization to manage security and privacy risks – categorize, select, implement, assess, authorize, monitor, and prepare. The steps are based on the process. Each step is supported by other NIST publications. The presenter asked the Board for feedback, ideas, and suggestions to update and align with other policy activities. There are always opportunities for improvement on RMF and NIST publications. It is also important and necessary for NIST to better communicate and explain RMF to both technical and non-technical audiences.

Future revisions of NIST SP 800-53 – NIST provides various mapping, assumptions, and guidance to help guide and inform the control selection process. In addition, the development of overlays to facilitate control baseline customization, develop the Security Control Overlay Repository (SCOR), and roll out spreadsheet format in Open Security Assessment Language (OSCAL) format. These developments support the intent to

[23] NIST CSRS / NIST RMF (FISMA) https://csrc.nist.gov/projects/risk-management/fisma-background
[24] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf
[25] https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf
[26] https://www.nist.gov/system/files/documents/2018/03/28/vickie_nist_risk_management_framework_overview-hpc.pdf

gather suggestions for new controls, improve on existing controls, and simultaneously provide updates in response to comments received and to preview planned changes in next revision.

Board discussion: In the context of the RMF, documenting verifies the effectiveness of the controls and reinforces assessment, but documentation is a different perspective than assessment. In security assessment, documentation is a relevant part of the assessment as part of the record. It is noted that assessment is internally focused and a measurement of output, and not for external focus. The Board posted a question if there is any opportunity to use the RMF to analyze a cybersecurity incidence. RMF does not include a timeline, and the framework tackles assessment of work stream where each system deviates.

Public Comment – No request from public comment was received.

Day 1 Board Review

- AI – update from the last presentation to ISPAB, e.g., next steps and progress
- CSF 2.0 - did not address a) vulnerability disclosure handling, b) how to incorporate informative references, c) how to keep updating and mapping to CSF, d) guidance to connect as a gateway.

Matt Scholl reminded the Chair of outstanding topics:

- Draft letter to CSRB approved during the last ISPAB meeting, October 2022
- Known Exploited Vulnerabilities (KEV), CISA [27]

Meeting Recessed

The Board recessed at 3:55 p.m., EDT, March 1, 2023

[27] https://www.cisa.gov/known-exploited-vulnerabilities

Day 2 - Thursday, March 2, 2023

The Chair called to session at 10:01 a.m. EDT.

NIST Update

Kevin Stine, Chief of the Applied Cybersecurity Division (ACD), NIST
Matthew Scholl, Chief of Computer Security Division (CSD), NIST

Kevin Stine began his presentation with the announcement that the National Cybersecurity Strategy was released early this morning. Some high-level aspects of the strategy were covered during Day 1 of this meeting (see footnote # 16, 17, 18 & 19).

The Cybersecurity Framework (CSF) V2.0 Concept paper describes options for evolution of the CSF and many comments were submitted. The V2.0 virtual workshop[28] held on February 15, 2023, recorded over 1500 attendees from the US and many other countries. An in-person two-day workshop29 followed on February 22-23, 2023, with another workshop planned in the fall. Feedback received concentrated on governance and functions. NIST learned many things from past years' feedback, especially from private industry.

The continuing work on CSF will leverage the privacy framework and AI risk management framework. A lot of discussion focuses on privacy risk assessment framework and privacy enhancement framework with emphasis on variances, leadership role, recuring different values and basic input for privacy guidance. It is planned to be available for public comments shortly. NIST organized a spy test challenge between US and UK, and the winner will be announced in the coming months.

Supply Chain was another topic where NIST ACD had been actively involved in establishing the CSF and functions, gathering feedback on informative references, creating guidance on the framework, making changes to the framework core, reordering functions, and mapping to rules and regulations. There is still much more to do in setting a platform for awareness and measurement. NIST is still working on a few priorities such as 1) how to use the framework at national level, 2) how to achieve a greater ROI, and alignment with SP 800-37 RMF.

Matt Scholl reported on the work in cryptography and quantum design. CSD is targeting to releasing standards for public comments by early 2024. CSD is dealing with some issues that have arisen including a reported side channel attack on one of the post-quantum algorithms that has been the subject of some mischaracterization. The real issues in implementation and mapping. There is no specific concern with lightweight with the performance fit effectively with 112 bits and 128 bits latency.

Work is continuing on the CHIPS Act research (see Day 1 ITL Updates).

SP 800-63-4[30] Digital Identity Guidelines was published in December 2022 with comments due to close on March 24, 2023. The document provides an update on authentication including the real-world implications of online risk. The guidelines present the process and technical requirements for meeting digital identity management assurance levels for identity proofing, authentication, and federation, including requirements for security and privacy as well as considerations for fostering equity and the usability of digital identity solutions and technology. NIST is

[28] https://www.nist.gov/news-events/events/2023/02/journey-nist-cybersecurity-framework-csf-20-workshop-2
[29] https://www.nist.gov/cyberframework/updating-nist-cybersecurity-framework-journey-csf-20
[30] https://csrc.nist.gov/publications/detail/sp/800-63/4/draft

specifically interested in comments on and recommendations for identity proofing and enrollment (especially on non-biometric options), risk management, authentication and lifecycle management, federation and assertions.

NIST's on-going work covers identity PIV credentials for non-federal and state governments and that the credentials are trackable. It also covers containers for security stack capabilities, hardware, off-premises cloud services used for security, increased capabilities to make hardware secure and how tools can be used by designers and developing guidance on fraudulent identity tools and their impact on authentication[31]. On the topic of mobile driving license, mapping is critical to avoid a burden on industry to adhere to too many different frameworks.

Annual FISMA Reporting Requirements

Khalid Hasan, Assistant Inspector General for the Information Technology (IT), Office of the Inspector General (OIG) <*Presentation provided*>

The presenter gave a brief introduction of his role and explained the two groups of Inspectors General (IG). The IGs have sought to improve collaboration between the IGs and agencies. The new IG FISMA reporting process seeks to harmonize the challenges that agencies are facing in meeting the criteria. The IG FISMA Reporting process is explained as "the Office of Management and Budget (OMB) consults with the Department of Homeland Security (DHS), CIGIE, and other parties on the development of annual FISMA reporting guidance for IGs whereby the CIGIE (Council of the Inspectors General on Integrity and Efficiency) FISMA metrics working group coordinates with federal partners. The IG FISMA results are reported in DHS's CyberScope application. In 2021, the SCRM (Supply Chain Risk Management) domain was added and ERM (Enterprise Risk Management) CSRM (cyber security risk management) was clarified. The components of IG FISMA evaluations are:

- Identify (Risk management and supply chain risk management
- Protect (configuration management, identity and access, data protection and privacy, and security training
- Detect (information security continuous monitoring)
- Respond (incident response)
- Recover (contingency planning)

There are five levels in the IG FISMA Maturity model and OMB has defined Level 4 (quantitative and qualitative metrics are used to monitor effectiveness of processes) as being effective.

The new IG FISMA reporting process, FY 2022-20, outlines the guidance for implementing the requirements outlined in M-22-05[32] and M23-03[33], and emanating from EO 14028, and resulting in new FY2023 IG evaluation areas focusing on:

[31] https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-president-bidens-sweeping-pandemic-anti-fraud-proposal-going-after-systemic-fraud-taking-on-identity-theft-helping-victims/

[32] M-22-05 FISMA Guidance on IG Reporting for FY22
"OMB will select a core group of metrics, representing a combination of Administration priorities and other highly valuable controls, that must be evaluated annually. The remainder of the standards and controls will be evaluated in metrics on a two-year cycle based on a calendar agreed to by CIGIE, the CISO Council, OMB, and CISA."

[33] FISMA Guidance on IG Reporting for FY23
"OMB selected a core group of metrics, representing a combination of Administration priorities and other highly valuable controls, that must be evaluated annually. The remainder of the standards and controls will continue to be

- Reporting of government furnished equipment via the DHS' Continuous Diagnostics and Mitigation (CDM) program
- Asset visibility and vulnerability detection
- Security measures for EO critical software
- Software producer self-attestations
- Audit logging for privileged accounts
- Endpoint detection and response

The core IG metrics include five functions: Identify, protect, detect, respond and recover, and description of core metrics area for each function.

The IG FISMA Capstone report included historical analysis of IG FISMA data, where it demonstrated effectiveness decreased with the evolution of the FISMA reporting. The presentation concluded with next steps to a three-year continuous evaluation cycle that should provide key data to identify improvements and target profiles that may help IGs to better evaluate effectiveness while considering agency specific factors. It was noted that a challenge remains in finding the right balance amongst compliance, risk management, and effectiveness.

Board Discussion: The Board is interested in tracking correlation of the agencies' scores and its history, and results in protecting government data. The Board is also interested in the effectiveness of the scoring system and in how important is gathering the feedback is to improving agencies' performance.

Enduring Security Framework (ESF) Supply Chain Risk Management Guidance Briefing [34] [35] [36] [37]

Valecia Maclin, General Manager Engineering, Customer Security and Trust, Microsoft
Carol Lee, NSA

The Enduring Security Framework (ESF), a public-private cross-sector working group led by NSA and CISA that provides cybersecurity guidance to address high priority threats to the nation's critical infrastructure. The ESF work on supply chain risk management was motivated by the evolution of supply chain and events that led to the SolarWinds attack to create a set of industry- and government-evaluated best practices focused on the needs of

evaluated in metrics on a 2-year cycle based on a calendar agreed to by CIGIE, the CISO Council, OMB, and CISA. These changes do not in any way limit the scope of IG authority to evaluate information systems on an as-needed or ad-hoc basis."

[34] https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/Cybersecurity-Partnerships/ESF/ The ESF is a cross-sector working group that operates under the auspices of Critical Infrastructure Partnership Advisory Council (CIPAC) to address threats and risks to the security and stability of U.S. national security systems. It is comprised of experts from the U.S. government as well as representatives from the Information Technology, Communications, and the Defense Industrial Base sectors. The ESF is charged with bringing together representatives from private and public sectors to work on intelligence-driven, shared cybersecurity challenges.

[35] CISA, NSA, and ODNI Release Part One of Guidance on Securing the Software Supply Chain (Customers) https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3221208/esf-partners-nsa-and-cisa-release-software-supply-chain-guidance-for-customers/

[36] ICT Supply Chain Risk Management Task Force https://www.cisa.gov/resources-tools/groups/ict-supply-chain-risk-management-task-force

[37] Securing the Software Supply Chain – Recommended Practices Guide for Developers https://www.cisa.gov/sites/default/files/publications/ESF_SECURING_THE_SOFTWARE_SUPPLY_CHAIN_DEVELOPERS.PDF August 2022

software stakeholders. The guidance is meant as principles for operational guidance and aims to make sure it does not replicate other work. It heavily emphasizes public-private partnership. The objective is to think about the environment with many open source components and what change in operational guidance is relevant. ESF work aligns with NIST and NIST publications. To-date, ESF has published three documents relating to supply chain, namely:

- ESF: Securing the Software Supply Chain for Customers (see footnote #34), October 2022 (39 pages)
- Securing the Software Supply Chain: Recommended Practices Guide for Suppliers[38], September 2022 (45 pages)
- Securing the Software Supply Chain for Developers (see footnote #36), August 2022 (64 pages)

ESF: Securing the Software Supply Chain for Customers – Prevention is often seen as the responsibility of the software developer, as they are required to securely develop and deliver code, verify third party components, and harden the build environment. If a software package injected with malicious code proliferates to multiple consumers, it is much more difficult to confine; it may cause an exponentially greater impact compared to when a single customer is the target of a cyberattack. Because of this, the customer also holds a critical responsibility in ensuring the security and integrity of software; not only do they acquire the software, but they are also responsible for deploying it. Security is not just for the developers and suppliers, it's for customers too.

This document discusses resiliency, best practices, and third party maintenance. It is also a guidance leverage on best practices for software . Customers should be diligent about deployment, operation of supply chain, and paying close attention to potential threats. Also included in the document are informative details on procurement such as requirements, gaps, and specifically a call out to customers to define requirements for security by design and detailed scenarios for attention. Customers need to have a clear understanding of defined functions and roles, information for maintenance and upgrade, product evaluation as part of acquisition, and assessment. During Phase I of the ESF work on SCRM, they covered SBOM, tamper threats, testing, configuration, integration, upgrade, and end of life.

Securing the Software Supply Chain: Recommended Practices Guide for Suppliers – until all stakeholders seek to mitigate concerns specific to their area of responsibility, the software supply chain cycle will be vulnerable and at risk for potential compromise. The document advises organizations to prepare their environment and to protect software. They should develop policies and procedures to identify threats, create binary code, and updating code when designing software. The assessment and acceptance of risk will be covered in the guidance for developers.

Securing the Software Supply Chain for Developers – There are five sections in this document offering guidance on developing secure code, verifying third party components, hardening the build environment, and delivering the code. Until all DevOps are DevSecOps, the software development lifecycle will be at risk. Every recommendation on training developers focuses on mitigation, delivering solid safe code, testing, and protecting software, protecting the repository, a how-to integration of building, testing, building environment, and delivering software. The appendices include A: Crosswalk between Scenarios and SSDF; B: Dependencies; C: Supply chain levels for software artifacts (SLSA); and D: Artifacts and checklist.

These publications aim to promote awareness for all stakeholders – customers, suppliers, and developers. Thus, they are strongly motivated to produce a simple, consumable frameworks in the hope of bringing practices into

[38] https://media.defense.gov/2022/Oct/31/2003105368/-1/-1/0/SECURING_THE_SOFTWARE_SUPPLY_CHAIN_SUPPLIERS.PDF

focuses together in a holistic way with possibilities to expand the documents in the future. ESF is a public-private cross-sector working group and will continue to work with sectors, consortia, and government. ESF is looking to work on complementary documents.

Board discussion: The Board raised the question whether the adoption of these publications is mandated. Is there a roll out for implementation? The presenters do not think there is any intent to mandate. ESF is chartered by the Department of Defense, Department of Homeland Security, Office of the Director of National Intelligence, and the IT, Communications and Defense Industrial Base Sector Coordinating Councils. The focus in Phase I was setting the foundation, and support to manage the mission. In response to the Board query of whether the documents are meant for developers or for compliance, the plan for Phase 2 is to address actionable ways of securing software.

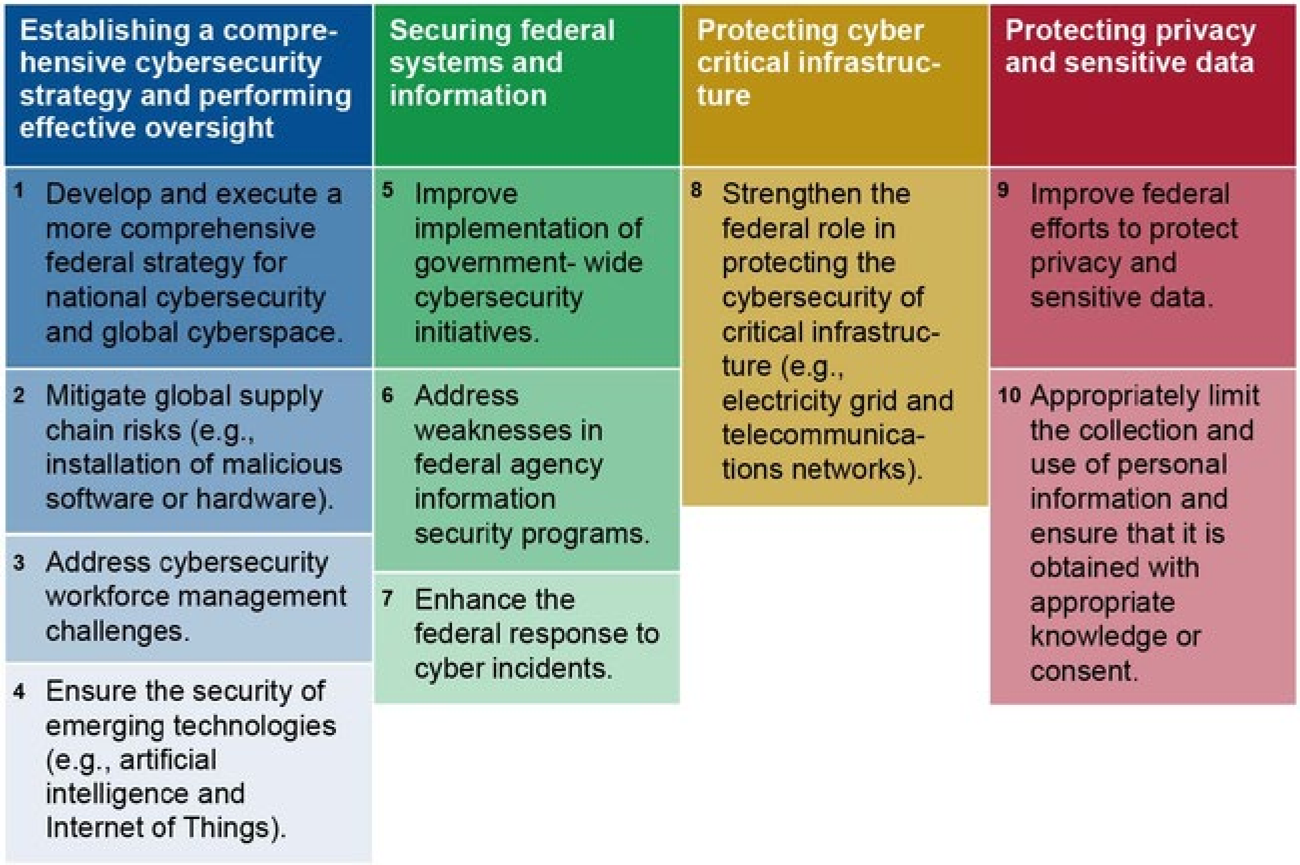
GAO Findings in report GAO 23-106415[39] *& 106428*[40] *Challenges in Establishing a Comprehensive Cybersecurity Strategy and Performing Effective Oversight*

Marisol Crus-Cain, Director, Information Technology and Cybersecurity, GAO <provided handouts to ISPAB>

US Government Accountability Office (GAO) developed a high-risk list, and information security was added to the list in 1997. It was updated to include advancements in technology – PII, critical infrastructure concerns, comprehensive national strategy, and oversight. The motivation for developing the series is the concerns for serious risk to human safety, national security, the environment, and the economy.

In 2018, GAO reported that the federal government needed to address four major cybersecurity challenges: (1) establishing a comprehensive cybersecurity strategy and performing effective oversight, (2) securing federal systems and information, (3) protecting cyber critical infrastructure, and (4) protecting privacy and sensitive data. Within these four challenges are 10 actions critical to successfully dealing with the serious cybersecurity threats facing the nation (see the figure identifying the four challenges and 10 actions) [41].

[39] https://www.gao.gov/products/gao-23-106415
[40] https://www.gao.gov/assets/gao-23-106428.pdf,
[41] https://www.gao.gov/products/gao-21-288



Establishing a comprehensive cybersecurity strategy and performing effective oversight	Securing federal systems and information	Protecting cyber critical infrastructure	Protecting privacy and sensitive data
1 Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace.	5 Improve implementation of government- wide cybersecurity initiatives.	8 Strengthen the federal role in protecting the cybersecurity of critical infrastructure (e.g., electricity grid and telecommunications networks).	9 Improve federal efforts to protect privacy and sensitive data.
2 Mitigate global supply chain risks (e.g., installation of malicious software or hardware).	6 Address weaknesses in federal agency information security programs.		10 Appropriately limit the collection and use of personal information and ensure that it is obtained with appropriate knowledge or consent.
3 Address cybersecurity workforce management challenges.	7 Enhance the federal response to cyber incidents.		
4 Ensure the security of emerging technologies (e.g., artificial intelligence and Internet of Things).			

Source: GAO analysis. | GAO-21-288

Since 2010, GAO has provided over 4000 recommendations to agencies, over 670 of which were made since the last update in 2021. In December 2022, GAO noted more than 880 recommendations had not been fully implemented. GAO has made efforts in pressing the US government to establish a comprehensive National Cyber Strategy and to address missing elements in the National Cybersecurity Strategy. These efforts resulted in the White House establishing National Cybersecurity Strategy in 2018 and the implementation plan in 2019, and the appointment of the office of National Cyber Director in 2021. SCRM is recognized as a major issue and GAO has made recommendation to 23 agencies to fully implement the foundational SCRM practices, but none of the agencies that GAO reviewed has yet implemented those practices.

Board Discussion: The Board recognized that it can be challenging for agencies to prioritize GAO recommendations in consideration of a variety of recommendations, (e.g., from CISA and OMB as well as GAO) even though GAO audits agencies' actions on the recommendations.

Challenges in Securing Federal Systems and Information (Green color in the figure above) – GAO has made 335 recommendations via public reports since 2010, and about 190 (56%) had not been implemented when reviewed in December 2022. As extracted from the handout, The CISA Act of 2018 established CISA to advance the mission of protecting federal civilian agencies' networks from cyber threats and to enhance the security of the nation's critical infrastructure. The act assigned five key cybersecurity responsibilities to CISA. To implement the identified challenge, CISA undertook a three phased initiative aimed at unifying the agency, reorganized offices and functions previously under NPPD. CIP stakeholders reported challenges in coordination with CISA due to a lack of clarity of the new structure and agency's involvement in development of guidance. The GAO's publication includes recommendations for agencies with expected dates for completion of certain tasks and for overall completion of all recommendations; to develop plans for performance measures; and a strategy for workforce planning. GAO reviewed the interaction between agencies, collaboration with the White House, CISA, and FBI. The status of recommendations noted lesson learned: evidence collection was limited; information sharing was difficult due to issues of assessing classified materials. GAO derived these suggested practices – aligning technology investments with operational priorities, improving public-private engagement, improving threat intelligence acquisition sharing and use among federal agencies. There is no recommendation specific to public-private engagement

Challenges in protecting cyber critical infrastructure (CIP) (Gold/yellow in the figure above) – GAO findings noted that Department of Energy did not address all cyber risks to the grid's distribution system , and the US power grid remains vulnerable. GAO recommends that agencies and industry coordinate to fully address cybersecurity risks while developing plans to implement the National Cybersecurity Strategy. DHS and DOJ need to enhance coordination against ransomware attacks. The findings also recognized that there are many best practices, but they are not mandated. CISA, FBI and Secret Service provide valuable assistance in preventing and responding to ransomware attacks. Challenges were identified related to awareness, outreach and communications, and schools and hospitals are increasingly being attacked. GAO recommends that DHS and DOJ should address challenges and incorporate key collaboration practices and deliver ransomware assistance to SLTTS.

Due to time constraints, the Presenter moved on to talk about privacy. GAO recognized the gaps in incorporating privacy into risk management strategies, coordinating with other key agency functions, and developing privacy policies. The gaps exist in policies for ensuring privacy compliance and role-based training for handling PII. GAO provided 237 recommendations and 140 (59%) were not implemented. The Board asked whether GAO cross checked available guidance to discover any policy recommendations that are not working and thereby not implemented. GAO are aware of certain issues and why the corresponding recommendations were not implemented. GAO cannot affirm that there are no issues when cross checked to SP 800-53.

Agency CISO Activities / Challenges / Success in Prioritizing, Planning and Resourcing Cybersecurity Requirements

Steven Hernandez, CISO, US Department of Education

The Presenter began by discussing the challenges on cybersecurity requirements compliance – there are over 170 high level requirements and over 200 requirements specific to SP 800-53. Additionally, there are hundreds to thousands of requirements on other topics such as workforce and supply chain. There are challenges in changing the ways to deploy systems.

Workforce is a huge challenge to US Department of Education (DOE) especially on policies that are human focused rather than. financially focused – in finding talent and skillsets and getting the right partners in protecting information. The government pay scale and recruitment are not competitive and the current employee expectation of remote and hybrid working environment further impacts recruiting. Although the Scholarship for Service program is helpful, agencies need to have employee positions to hire people who seek to pay back their service commitment.

The US government does not own its entire network and systems, and therefore, workers need to have experience in handling different and sometimes difficult department environments. DOE is using cloud services 100% and relies on cloud service providers to support the government cloud. Many cloud service providers are not meeting government security requirements, and many resist acquiring FedRAMP certification of their services. In view of the EO 14028 requirement for zero trust for example, SaaS is difficult to secure.

Moving on to budget and funding, it is difficult to manage resources and budget while operating under constant continuing resolutions with no authority for new initiatives or modernization. It is a constant challenge to catch up with new budget approval and simultaneously to prioritize scheduling of backlog. The Presenter has to strategize on submitting proposals to meet budget and modernization criteria, while mapping to EO 14028 and include quantitative and qualitative impact to qualify for getting payback for spending under investment programs.

There was no time for board discussion due to overrun of the agenda schedule.

Software Bill of Materials (SBOM) Activities for the Federal Agencies [42] [43]

Allan Friedman, Cybersecurity and Infrastructure Security Agency (CISA)

The Presenter stated that implementation of SBOM should not be an issue. The goal is to create a data layer using the applicable tooling. There are two data formats, but they are not compatible with each other. Users will need to coordinate across formats to build in interoperability and recognize that SBOM is applicable differently in cloud computing. CISA is focusing on software maintenance and open source. EO 14028[44], Section 4 offers the relevant information such as purchasing, value of SBOM, what one should know when acquiring software, and what data ought to be available internally. While SBOM is being developed and not completely mature, it is helpful to organizations. As we are integrating and mapping to new tools for asset management, care should be taken in translating data and not to reinvent the wheel with building new tools. CISA is also looking into customization for particular applications, e.g., 5G to get more sophisticated scenarios.

M-22-18 Enhancing the Security of the Software Supply Chain through Secure Software Development Practices released on September 14, 2022, provides information on adaptation. CISA is coordinating directly with federal agencies, including the DOD CIO Working Group, on testing, and with IETF and CSA (Cloud Security Alliance) on developing standards. Simultaneously, CISA is promoting various resources as guidance and awareness. NIST Software Security Vulnerability Management[45] is cross-referenced.

CISA is working with the Open Source Community on tooling. There are multiple identifier formats that need to be updated on the Vulnerability Exploitability eXchange (VEX). There are at least eight data formats supported by many organizations, and the consideration of cloud computing. It is important to start the conversation early and integrate asset management and enabling automation. In a few more years, we may see more secure federal networks and more mature SBOM repositories.

[42] https://www.cisa.gov/topics/cybersecurity-best-practices/executive-order-improving-nations-cybersecurity
[43] https://www.cisa.gov/sbom
[44] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
[45] https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-security-supply-chains-0

The Presenter was unable to stay beyond the stipulated schedule, so there was no board discussion at the end of the presentation.

Final Board Reviews, Recommendations and Discussions

Steve Lipner, ISPAB Chair

CSRB = The Chair began with a discussion on the draft letter in support of CSRB. Ms. Moussouris circulated a draft letter in support of CSRB (see extracted minutes from October below) to the Board members for review. The Chair asked if the board would approve the letter or needed time to review and confirm/comment via email. Ms. Goodwin would like to have more time to review the draft. Mr. Gattoni voiced his concern that the CSRB document was released with the knowledge that not all information and fact finding were sufficiently complete for analysis. In consideration that CSRB is not directed by Congress and the board's unique role to look at incident response and briefings on best practices, the Chair tasked Mr. Groman and Ms. Moussouris to provide a redline edited of the draft letter for board's review. No timeline for updating the draft was specified.

- Action: The Chair requested Mr. Groman and Ms. Moussouris to provide a redline edited draft letter in support of CSRB for circulation after the meeting.

SBOM = While SBOMs cannot be used to directly prevent software attacks, the information they provide is extremely useful for identifying and mitigating potential vectors of attack, such as vulnerabilities in components. Attackers seek out vulnerable components and attack them. Adherence to the SBOM mandate but not considering attackers or measuring compliance will not be effective as a protection mechanism.

The question for the Board to consider, and ideally for the government to measure, is whether the use of SBOMs is good and appropriate. SBOM is subject to suppliers/vendors producing the information. The information can be helpful, but does it benefit investigation when an incident occurs and recovery that follows. It also depends on the person conducting the analysis of the damage and determining the remedy. Does SBOM help in vulnerability management and to what extent? The Board discussed the rationale and action on the SBOM presentation, and agreed to draft a letter on these questions, especially measuring outcomes.

- Action: Giulia Fanti is to draft a letter to NIST requesting for a formulated list of matrices to be circulated to the Board for review.

Topic(s) for Future Meetings

- A presentation relating to testing and maturity assessment.

Board Discussion Topics/Actions

- AI – update from the last presentation to ISPAB, e.g., next step and progress
- CSF 2.0 - did not address a) vulnerability disclosure handling, b) how to incorporate informative references, c) how to keep updating and mapping to CSF, d) guidance to connect as a gateway.
- Known Exploited Vulnerabilities (KEV), CISA
- Discussion on outcomes vs. effort
- Budget/funding as a motivation (National Cybersecurity Strategy – Implementation Plan)

- Rating on improvement, measurement, assessment or testing
- Software assurance
- OPM failure to protect data

Next Meeting - July 12 & 13, 2023[46]

Adjournment

The Chair thanked everyone for their participation and adjourned the meeting at 4:17 p.m., EDT, March 2, 2023.

[46] https://csrc.nist.gov/Projects/ispab/meetings

ANNEX A

List of Participants

LAST	FIRST	AFFILIATION	ROLE
Brewer	Jeff	NIST	DFO/Staff
Scholl	Matt	NIST	DFO/Presenter/Staff
Crus-Cain	Marisol	GAO	Presenter
DeRusha	Chris	OMB	Presenter
Dudley	Drenan E.	ONCD	Presenter
Friedman	Allan	CISA	Presenter
Hasan	Khalid	OIG	Presenter
Hernandez	Steven	Dept of Education	Presenter
Lee	Carol	NSA	Presenter/Visitor
Maclin	Valecia	Microsoft	Presenter
Pillitteri	Vicky	NIST	Presenter
St. Pierre	Jim	NIST	Presenter
Stine	Kevin	NIST	Presenter
Sokol	Annie	Exeter Government	Staff
Brown	Megan	Wiley Rein LLP	visitor
Fakir	Alice	IBM	visitor
Friedman	Sara	Inside Cybersecurity	visitor
Kaya	Karen	CrowdStrike	visitor
Kerben	Jason	DoS	visitor
Stoller	Travis	Wiley Rein LLP	visitor
Taylor Moore	Debbie	IBM	visitor
Wildenauer	Leopold	ITI	visitor