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

June 23 and 24, 2021

Virtual Meeting Platform: BlueJeans

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

Wednesday, June 23, 2021

Welcome and Opening Remarks

Steve Lipner, Chair, ISPAB, Executive Director, SAFECode

ISPAB Chair Steve Lipner, Executive Director of SAFECode, opened the meeting at 10 a.m. ET.

- New board member Essye Miller, Executive Business Management (EBM), LLC, was recently appointed.
- The Executive Order on Improving the Nation's Cybersecurity (EO 14028), which the President signed in May, is changing the way the U.S. government deals with cybersecurity and software products' security. It will have a big impact on agencies and companies and potentially on industry and the population at large.
- A reminder that the board's deliverable is advice to the non-defense executive branch about emerging issues and practices in security and privacy through motions and letters to government officials. Interaction between board members and speakers can also be a source of advice.

The Chair invited board members to introduce themselves:

- Essye Miller, retired in June, 2020, as Principal Deputy CIO for the Department of Defense (DoD). She spent 35 years as a career civilian with the Army, Air Force, and Office of the Secretary of Defense in CIO and CISO roles.
- Arabella Hallawell, Vice President, Strategy and Communications, NetScout Systems
- Jessica Fitzgerald-McKay, Co-Lead, Center for Cyber Security Standards, National Security Administration (NSA)
- Philip Venables, CISO, Google Cloud
- Douglas Maughan, Head of Office of Convergence Accelerator, National Science Foundation (NSF)

- Marc Groman, Principal, Groman Consulting; Adjunct Professor, Georgetown University Law Center
- Brian Gattoni, CTO, Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security (DHS)

Matt Scholl, Chief of the Computer Security Division in NIST's Information Technology Laboratory (ITL), reviewed the Federal Advisory Committee Act and the board's role in providing consensus advice to the government.

The role of the audience is to observe and listen but not engage with the board or speakers. There is a session scheduled later for open, public dialog with the board.

Kevin Stine, Chief of the Applied Cybersecurity Division, ITL, introduced himself.

Welcome and ITL Update

James St. Pierre, Acting Director, ITL

Update on NIST Leadership

- NIST is in a transitional phase as the new Administration continues to settle in.
- Jim Olthoff is currently performing the non-exclusive functions and duties of the NIST Director. Chuck Romine is serving as acting chief of staff and is expected to return to his role as director of ITL once a new NIST director is confirmed; Eric Lin is acting associate director for lab programs; Stephanie Hooker is acting director of the Material Measurement Lab; and Joannie Chin is acting director of the Engineering Lab.

Update on ITL Initiatives

- The President's FY 2022 Budget Request is increased over the FY20 request. The increase will help fund many priorities, including work on artificial intelligence (AI), quantum computing, and climate change.
- New Executive Orders
  - EO 14028: Improving the Nation's Cybersecurity
    - Consult with stakeholders to identify or develop standards, tools, best practices, and guidelines to enhance software supply chain security
    - Workshop was held June 2-3, 2021
    - Recommend minimum standards for vendors' testing of their software source code and publish guidelines by July 2021
    - Initiate two pilot labeling programs related to secure software development practices and IoT to inform consumers about the security of their products
  - EO 14017: America's Supply Chains
    - Lead agency: Commerce Department
    - Identify risks in semiconductor manufacturing and advanced packaging supply chains
    - Report on supply chains for critical sectors and subsectors of the Information and Communications Technology (ICT) industrial base
    - Partner with federal agencies and private stakeholders to identify and map critical supply chains
  - EO 14005: Ensuring the Future Is Made in All of America by All of America's Workers
    - Charges agencies with partnering with Hollings Manufacturing Extension Partnership (MEP) for supplier scouting
    - Identify U.S. companies that can produce goods, products, and materials in the United States that meet federal procurement needs

- Diversity, Equity, and Inclusion (DEI)
  - Main purpose is giving all of the staff a strong sense of belonging
  - NIST just hired a new director of DEI, Sesha Moon
  - COACH Study of STEM Promotion Process: They had seen some concerning data showing discrepancies in how women were promoted. The study did not find that to be as significant as they had initially thought, but it identified the need and offered recommendations for improvements. They try to make the promotions process as transparent as possible.
  - ADLP Assignment Study: Disappointing findings regarding the number of women who have faced a chilling climate. Highlighted need to work so that everyone has the same vision for the sense of belonging.
  - Inclusive Language: As a result of a letter ISPAB sent to NIST in 2020, the agency updated the NIST Technical Series Publications Author Instructions. Additionally, the American National Standards Institute is working on gender-responsive standards.
  - Mr. St. Pierre is involved in the steering group for equity and career advancement. They are looking at tools to improve the language used in job postings. They are working on a pilot project to use LinkedIn to draw from a diverse pool of candidates. They are increasing efforts to reach out to diverse universities, Historically Black Colleges and Universities, and more.
  - ITL Diversity Committee – working to maintain both a top-down and bottom-up approach
- Encryption
  - Third Post Quantum Cryptography Standardization Conference held June 7-9, 2021: Seven third-round finalists and eight alternates
  - Fourth Lightweight Cryptography Workshop held October 19-21, 2020
- Trustworthy AI
  - Advisory and Working Groups
    - AI Federal Advisory Committee - currently being established
    - AI Resource Research Task Force – working toward democratization of AI; advance U.S. competitiveness and innovation. ITL AI Program Lead Elham Tabassi was selected to be on the task force.
    - AI Standards Coordination Working Group under Interagency Committee for Standards Policy
  - Reports
    - Proposal for Identifying and Managing Bias in AI – NIST SP 1270
    - AI and User Trust – NISTIR 8332
    - Machine learning (ML) for Access Control Policy Verification – Draft NISTIR 8360
  - Workshops
    - Assessing and Improving AI Trustworthiness, March 3-4, 2021
    - Secure Government Data Sharing, May 21, 26
    - AI In Drug Development, June 31-July 1, 2021 – working with FDA and DARPA
    - NIST AI Measurement and Evaluation Workshop, June 15-17, 2021
- 2022: Celebrating 50 years of cybersecurity research at NIST

Discussion

- Ms. Fitzgerald-McKay asked if there will be any updated studies on diversity based on work transitions during the pandemic, such as more telework to broaden hiring pools.

  Mr. St. Pierre said there are no current plans, but it is a good idea for the future. Part of the feeling is that they've done a lot of studies and it's time to start working on the findings. It was relatively easy for everyone to move to telework. It's much harder to go back to in-person because it's happening in phases. A plan is due July 19 to make sure people who continue teleworking are not left out and their career is not affected.

- The Chair asked if there is a sense that the new normal won't be like the old normal in terms of physical presence. What is the timeframe for more people returning to the office?

  Mr. St. Pierre said that it is an evolving situation. By July 19 they must submit a plan, and then the return to the office will phase in. For now, 25 percent of the staff is allowed on campus. There used to be 72 hours before you could work in a space somebody else had been in. Some of those approvals have changed over time. They are looking at shift work, among other things. It represents a real change in philosophy throughout the federal government that we should lean in on telework. If people can be effective and efficient, then that should be a way of operation. How do we make sure that the serendipity – people running into each other in the halls and coming up with a great idea – continues?

The Chair recessed the meeting for a 20-minute break.

NIST Cybersecurity and Privacy Update

Matthew Scholl, ITL; Kevin Stine, ITL

Executive Order on Improving the Nation's Cybersecurity (EO 14028), Section 4

- NIST's direct tasks and deliverables
  - Day 30, June 11, 2021: Solicit input from stakeholders (4b)
  - Day 45, June 26, 2021: Publish definition of "critical software"
  - Day 60, July 11, 2021: Publish guidance outlining security measures for critical software (4i); Publish guidelines recommending minimum standards for vendor testing of software source code (4r)
  - Day 180, November 8, 2021: Publish preliminary guidelines for enhancing software source code security
  - Day 270, February 6, 2022: Issue guidance identifying practices that enhance security of software source code (4e); Initiate pilot programs identifying IoT cyber and secure software development practices or criteria for consumer labeling programs (4s, 4t, 4u)
  - Day 360, May 8, 2022: Publish additional guidelines, including review/update procedures (4d)
  - Day 365, May 13, 2022: Review and submit summary report of pilot programs (4w)
- NIST guidelines, standards, and resources will be drawn on to support other areas of the EO, including Section 3 (modernizing federal government's cybersecurity in areas like Zero Trust and cloud migration, multi-factor authentication, and encryption); Section 6 (standardizing federal government's playbook for cybersecurity incident response); and Section 8 (log management activities)
- There will be updates to key publications in those areas.
- These are the specific deliverables, but NIST also will continue to enhance the resources that are produced to ensure they are helpful over the long haul.

Ransomware

- High-profile incidents in last several months
- Continue to look at existing guidelines, best practices, and standards
- New Resources Issued Recently: 1) Tips & Tactics for Ransomware Protection and Recovery; 2) Cybersecurity Framework Profile for Ransomware Risk Mitigation – preliminary draft of profile to highlight how the categories and subcategories can be viewed through the lens of ransomware

protection, response, and recovery – to serve as input for workshop in July focusing on challenges and practical approaches to recovering from ransomware and other destructive events.

Operational Technology (OT) Cybersecurity

- Recent high-visibility incidents have affected OT environments and caused business disruptions and service delivery disruptions.
- At the end of May, a pre-draft call for comments closed on the planned update to SP 800-82. A draft for public comment will be available later this year.

Control System Cybersecurity

- Recently issued more appealing resources that include fundamental steps an organization can take to protect control systems and steps to manage cybersecurity risk - blasted out in a number of different ways, including on LinkedIn.

Visually Appealing Resources

- On a broader scale, with resources like tips, tactics, and quick hits, NIST is trying to incorporate resources that are more visually appealing and engaging in order to reach different audiences and increase impact.

Discussion

- Ms. Fitzgerald-McKay asked whether there is any overlap in the guidance on industrial control systems and the guidance on ransomware.

  Mr. Stine said that the two sets of guidance refer to each other. Updates to SP 800-82 will likely include guidance specifically for ransomware and other destructive events.

- Mr. Groman asked about cross-referencing guidance for ransomware. What are the triggers for notification in a ransomware attack? When do you need to tell someone their data is compromised or not available? The privacy community should start thinking about this guidance.

  Mr. Stine said that they are taking a hard look at guidelines around incident response. The emphasis on privacy at NIST – and broadly – has grown.

- The Chair asked whether NIST has any role in the creation of the Cyber Safety Review Board.

  Mr. Stine said they have no direct role in standup of the board, but they will contribute where they can with an eye toward (1) what they can learn through its standup and the execution of its responsibilities to improve standards and guidelines and (2) contributing resources to help improve the way the board functions.

  The Chair said NIST ought to be a high-priority consumer of the lessons learned via that board.

- The Chair asked about the role of ISA/IEC 62443 as a standard for OT. It would be interesting if NIST had a view on that and made a recommendation.

  Mr. Stine said that standard is one of the base informative references in the Cybersecurity Framework. They have worked with the community to map the Framework and the standard to reflect control system practices. As SP 800-82 is updated, the same type of mapping and alignment will be done. Additionally, they might provide input into future versions of ISA/IEC 62443.

- Mr. Scholl added, with regard to overlap in guidance on ransomware and guidance on OT, that when they issued the document as a pre-draft, the team asked six specific questions about industrial control security. One question was about ensuring that updates to control system threats and any recommended practices to address those threat models were included. Part of the intent was around ransomware and ensuring there are adequate controls that address the OT space.

Post Quantum Cryptography (PQC)

- Timeline
  - 2015: NIST Workshop on PQC
  - 2016: NIST report on PQC – NISTIR 8105
  - 2016: NIST announces "competition-like" process
  - 2017: Deadline for submissions
  - 2018: First NIST PQC Standardization Conference
  - 2019: Announced 26 algorithms moving to the Second Round
    First Round Report – NISTIR 8240
  - 2019: Second NIST PQC Standardization Conference
  - 2020: Announced Third Round seven finalists and eight alternate candidates
    Second Round Report – NISTIR 8309
  - 2021: Third NIST PQC Standardization Conference
  - 2022-2023: Release draft standards and call for public comment
- There is a lot of discussion commercially about post-quantum cryptography and the post-quantum transition. How can lessons learned from previous, less-than-fully-successful transitions be used?
- Starting some joint work with DHS, leveraging their reach into state, local, tribal, and territorial regions to spread the word.
- The word "quantum" is being used almost on a hype scale – purchased "quantum" dishwashing tablets recently.
- Will be working on ensuring that we design the new sets of algorithms to use on classic machines and also help people understand what this all means and how to be prepared for it.
- Draft project description for crypto migrations project and seeking public comment through July 7. Will stand up a cryptographic applications Community of Interest to begin developing migration playbooks, tools, and resources. Help organizations start inventories and data collection to plan out what the migration will look like when the time comes.

Discussion

- Mr. Venables said he is finding that a lot of organizations are not looking further up the stack to consequences to other protocols and applications that have made fixed assumptions about key sizes and signature sizes – where they are going to need to change high-level protocols and application code. People need to think about changing not just the crypto but also all the things that have made assumptions about key sizes, signature sizes, and other things.

  Mr. Scholl said some companies, including Google, have done some pilot work on communication protocols, as have some international partners. People in the European Union are doing some TLS [Transport Layer Security] testing. There will be disruption in protocols, standards, and certificates, which will drive a hybrid life for a while.

- Mr. Venables asked whether sector-specific agencies, such as the Department of Energy and Department of Treasury, have this on their agenda. There are a lot of things in critical infrastructure where the higher-level communication protocols make assumptions about things like signature sizes, certificates, and key lengths.

  Mr. Scholl said it is interesting he mentioned the Energy Department and Treasury Department. The Department of Treasury is leaning forward on this. They have had discussions with them and with different Federal Reserves that want to be ready for the backbone communication protocols that handle bank transfer communications. Some of the agencies were trying to hold back a little bit because specific algorithms have not been selected and parameters have not been defined. Energy is also leaning forward.

Mr. Venables said that on one level it is good that organizations may be holding back to get more certainty about what the changes will be, but it also may be a signal that they're not adequately thinking about crypto agility. We should be transitioning to an environment where it is easier to make future transitions. The only way to do this is in a crypto-agile way as opposed to just hardcoding a new set of things.

Mr. Scholl said that is a great point. There will be more than one replacement algorithm. They will be of different constructs to provide resilience against a quantum capability we aren't yet aware of. They want to continue cryptoanalysis and development even on the alternates that might not make it into the standardization document so that there is a large pool of potential replacements for the future.

- PQC Evaluation Criteria
  - Security – against both classical and quantum attacks
  - Performance – measured on a variety of classical platforms
  - Other Properties – drop-in replacements; perfect forward secrecy; resistance to side-channel attacks; simplicity and flexibility; misuse resistance; any factors that could hinder adoption
- Intellectual Property (IP) Consideration
  - There are some algorithms with IP claims. Two organizations have stated they have some IP coverage through patents of some of the mathematics. One organization put out a statement saying there will be no IP issues for the patents if implementation of a post-quantum selection is conducted – it can be done freely and with full use. The second organization has not gone as far but made a public declaration of free, reasonable, and non-discriminatory use. For-profit companies above a certain size will have a licensing structure. For small, academic research, it will be free. They also said they do not intend to necessarily pursue organizations that might be in violation.
  - ITL would like feedback from the board about whether the IP claims would be a hindrance to adoption and use of an algorithm.
- They are on track to finalize standards by 2023, at the latest, with parameters, and then finalize in 2024 – still believe they will be within an acceptable range for the transition.

Discussion

- The Chair said that the multiplicity of algorithms plus the transition and backward compatibility considerations raise the risk of people messing up implementations. They could wind up with strong RSA [public key cryptosystem], strong post quantum algorithms but also an opportunity for engineering foul-ups and built-in vulnerabilities. Is there anything to do to mitigate that or articulate best practices for implementers?

  Mr. Scholl said misuse resistance is a strong consideration. He will bring it up with staff. They have published a reference to the two Internet Engineering Task Force (IETF) standards for hash-based signatures, which can be implemented incorrectly if not done carefully. That can be a big issue if you don't maintain state on the hashes. They suspect they will have to operate in some hybrid modes for a while.

- Ms. Fitzgerald-McKay asked whether any special consideration is being given to how algorithms will perform in IoT devices.

Mr. Scholl said yes and no. If an IoT device or an OT device currently has the capacity to handle an elliptic curve KM or [inaudible] or RSA, it should be able to handle the recommendation for post-quantum. They are a little concerned about the [inaudible] key size increase. They are also concerned about people who have hardcoded into silicon or into code the implementations, especially in places that are not easy to get to. They talk with NASA a lot to ask what they will be sending up and when and for how long.

- Ms. Miller asked whether agencies are developing systems with an eye to this transition.

  Mr. Scholl said initial conversations centered on setting up the infrastructure planning so that agencies will be ready. They had discussions about marrying budget cycles with implementation timelines so they are prepared for changing infrastructures when needed. The conversations have been less about the technology and more about programmatic and budgetary process.

Awareness, Training, Education and Workforce Development

- National Initiative for Cybersecurity Education (NICE) Strategic Plan: Report to Congress includes Strategic Plan and broader awareness activities across NIST. Plan has a number of goals, and working groups are working on implementation plans for each goal.
- Annual NICE Conference was rescheduled to June of 2022.
- Virtual NICE Symposium will be held in November, 2021, and will focus on cybersecurity workforce as part of the coordinated efforts toward supply chain risk management
- Workforce dimensions of cybersecurity – and increasingly, privacy – intersect with a lot of different areas, including OT and supply chain risk management.
- NICE Framework Competencies: A series of workshops is planned. A workshop coming up in August will focus on competencies and work roles for OT and control systems. A workshop at the end of September will focus on security awareness training.
- Cybersecurity Awareness
  - Federal Information Systems Security Educators' Association (FISSEA): Fall FISSEA Forum at the end of September will kick off Cybersecurity Awareness Month and recognize Cybersecurity Career Awareness Week, which will be held this year October 18-23.
  - Update to NIST SP 800-50, Building an Information Technology Security Awareness and Training Program – Standards and guidelines for improving cybersecurity awareness of employees and contractors in federal agencies.
- Privacy Workforce Working Group
  - 600 members
  - Two project teams are crafting descriptions of tasks, knowledge, and skills, beginning with core categories in the Privacy Framework.

Publication Updates

- National Cybersecurity Center of Excellence (NCCoE)
  - Publications validating the integrity of computing devices; securing small business and home IoT devices
  - Securing the Industrial Internet of Things (IoT) – focus on solar panels
  - Securing Telehealth – focus on remote patient monitoring
  - Cybersecurity Considerations for Protecting Genomics Data and DNA sequencing techniques – ITL will collaborate with colleagues in other parts of NIST, particularly the Material Measurements Lab

Discussion

- Mr. Groman asked if there were any new developments with the Privacy Framework.

  Mr. Stine said they continue to be thrilled with uptake of the Framework and the increasing number of translations and adaptations. They continue to harvest resources developed by the community. Much of their attention now is on the workforce dimension for privacy and trying to drive toward some of the other roadmap areas, particularly around differential privacy and privacy-enhancing technologies.

- Mr. Groman asked if Office of Personnel Management is involved with the workforce effort.

  Mr. Stine said they conducted significant outreach to federal agencies, and he can follow up to get more specifics.

- Mr. Groman said he continues to be amazed at what NIST achieves with such limited resources. ISPAB sent a letter calling for additional resources for NIST in the privacy area. Was there any feedback or commentary on it?

  The Chair said the board approved the letter at the December meeting, and to the best of his knowledge they have not had a response. If it fell into a crack in the Administration transition because of the timing, it might be worth calling their attention to it.

  Mr. Groman strongly recommended, given the timing, re-sending the letter, noting that there are only four or five full time equivalents working on privacy.

  The Chair said he thinks it is appropriate to re-send the letter.

  Mr. Groman said four people are not enough for what they're being asked to do with regard to a national privacy framework. As a consequence, cyber suffers and incident response suffers. Then everyone gets frustrated and starts yelling at the privacy team. There are 4,000 people doing cyber, and four doing privacy.

  The Chair said they would take a look at the question of re-sending the letter during the recommendations session at the end of the meeting Thursday.

Identifying Cryptographic primitives that can be applied in different privacy-enhancing use cases

- Seminar series intended to ground next steps for research and potential recommendations
- The next event is July 6: Private information retrieval, searchable encryption, and fully homomorphic encryption

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

Executive Order 14028: Overview

Anne Neuberger, Deputy National Security Advisor for Cyber and Emerging Technology (NSACET), National Security Council; Jeff Greene, Acting Senior Director for Cybersecurity, NSC

Mr. Greene started the presentation. There has been pretty uniform positive reaction to the EO. As the concepts were socialized, he was pleasantly surprised that people in sectors he thought would be resistant were generally positive. The public-private effort is essential. The agencies have been on board. There is a ton of work, but there has been a positive effort.

Ms. Miller asked about how small businesses have responded.

Mr. Greene said he hasn't had direct interactions, but two questions had jumped out at him: 1) how to deal with open source; and 2) the reaction from small businesses. The things they are asking everyone to do are fairly common-sense things. Several small developers have said they can react more quickly and be more nimble.

Ms. Neuberger said she wanted the opportunity to talk to this group and thank them for all of the work that's been done. A number of the problems they sought to address in the EO are problems they have all known about for a decade, such as the issue of software supply chain and the issue of transparency. How do we incentivize improvement? There's been good progress, but there are still issues because of the complexity of software, among other things.

Administration's approach to cybersecurity

- Modernize Defenses: The first focus is on federal networks. Critical infrastructure runs on private networks, so the government's abilities there are limited. However, nearly 100 companies are participating in the industrial security effort. The level of progress and willingness of companies to step up in a public-private partnership manner is very exciting. The Energy Sector Coordinating Council was a key partner throughout the effort in rallying the sector and key executives.
- Rebuilding Our Role on the International Stage: Many U.S. partners and allies have been victims of significant cyber-attacks. The Administration decided to focus on building multilateral alliances. The G7 communique outlines an international coalition to hold countries to account. Sharing cybersecurity information was part of the NATO discussions.
- Bring all aspects of U.S. cyber capabilities to bear on these problems.

Main Pillars of EO 14028

- Shift thinking from incident response to prevention: They wanted to focus on five key areas for rapid progress to reduce the probability of attacks and the probability that data will be lost in the event of an attack – encryption, endpoint detection, indications of compromise, logging, and multifactor authentication. They saw in the Solar Winds incident, as they got the records back from federal agencies, that there wasn't adequate logging to be able to assess risk and harm and determine what was needed to recover. The key efforts are what they keep talking about because it can be overwhelming for companies or government agencies to know what they need to do to reduce risk. So they are putting tight timelines, some recovery plan money, and a tight implementation process to the effort.
- Software Standards: They mixed in private sector input so as not to lock in what needs to be done. DoD provides an example of what they sought to copy for the broader federal government. They want to remain cognizant of how different kinds of technology are built so that it is a dynamic process and enables innovation. NIST will help gather private sector information. They want to bring the power of federal government procurement to bear and set the expectations.
- Labeling: They wanted to take a page from Singapore's playbook with regard to visibility. They thank NIST for working with the FTC in designing a pilot initiative. They want to identify new and innovative ways to jumpstart security, to put a price on security, and to enable transparency and visibility.

Cybersecurity is not an easy field, but they can look back at how much has improved over the last 20 years in technology security. They can then look forward and see that the pace of innovation requires them to double down and make good progress.

The Chair thanked the speakers and invited board members to ask questions of Mr. Greene.

Discussion

- Mr. Groman said so many of the issues around cybersecurity necessarily impact data sharing and data collection. He served as the privacy lead during the Obama Administration. He noted that the Trump Administration did not have a senior advisor for privacy. To what extent are privacy and civil liberties being baked into cybersecurity policies today?

  Mr. Greene said privacy is baked in throughout the EO developments. In almost everything he's working on, there is a general awareness of and attention to privacy as an issue and a need. It feels a bit like they have turned a corner in that privacy is an original consideration in the development of the things they are doing. It is an ever-present consideration in a positive way.

  Mr. Groman asked if there is a privacy lead or someone who owns the effort across initiatives to see the whole picture.

  Mr. Greene said not that he's aware of.

  Mr. Groman asked if OMB is part of it.

  Mr. Greene said the OMB team has been terrific in the rollout of the EO and the development of pieces of the Solar Winds response. They partner on a variety of engagements. From a practical standpoint, it will take longer if they don't work together on the front end.

- The Chair asked about open source issues related to the EO.

  Mr. Greene said it is important to think about Section 4 not in terms of the prescriptive pieces that start in Subsection (e) but more about the end state – the level of security that should be present if the government is going to buy software. They want the effort to be focused not on new check-the-box rules but on how to get to the end state of security. If certain confidence levels are required from companies, how are you going to handle open source? Companies said once they start using something, the developers need to own it as if it is their own, in terms of putting it through security checks. It may require more on the front end, but there is some recognition in the world that it is a do-the-best-you-can. More importantly, if asked, they need to be able to defend steps taken so you have confidence in things they've done that will provide security. It was something they struggled to get the right balance with.

- Ms. Fitzgerald-McKay asked if there is a sense of what will happen after the minimal requirements defined in the EO are met. Is there a next step beyond the EO they are considering?

  Mr. Greene said the NIST process is the never-ending story. It is not supposed to end a year from now. There is a 180-day report and a 360-day report, but it is important that it is a continuing process focused on the end state. There are a lot of details in the EO about how they describe security, but that should morph with time. Ideally, the NIST process with the private sector and other agencies is continuing, so there's a continuous update.

- The Chair asked about the certification basis being self-attestation. How are the agencies and procurement organizations reacting to that? It's pretty trust-based.

  Mr. Greene said there is a requirement for artifacts of certain testing processes to either retain or provide. There are things that vendors are required to do. There is also going to be a Federal Acquisition Regulation (FAR) process. Some private trade associations have looked at innovative ways to report compliance, so they expect a lot of that to come in. In the private sector, you have to be very careful with any attestation. Any confirmation has to be accurate and in good faith or you may find yourself with stiff penalties. Organizations are looking at innovative ways to report compliance. Also, there are private rights of actions.

The Chair thanked the speakers and complimented them on a terrific job done in no time at all. He recessed the meeting for a 10-minute break.

EO 14028: OMB Implementations

Chris DeRusha, Federal Chief Information Security Officer, OMB

ISPAB has a long history of providing expertise and advice to government, going back to the 1980s. There is a new set of priorities to implement and a lot of hard work. Feedback from the board will be very helpful. We're at a moment in history when we need to bring a sense of urgency to everything we're doing. It requires the work of industry and government together. We are taking a whole-of-government approach.

Sharing Threat Information

- This is already working with government and service providers at DHS, FBI, and other agencies. There is a series of actions intended to remove barriers to sharing threat information. This section is also about internalizing contract requirements. There was a data call that OMB ran on agencies to get inputs from the security clauses they have in contracts and pull them together to determine what should be standard across government.

Modernizing Federal Government Cybersecurity

- Migrations to Zero Trust architecture; accelerating cloud migration; implementation of multi factor authentication – things that we've been working on for a while but want to prioritize. The first order of business is a 60-day review of Zero Trust implementations by each agency. OMB gave the agencies supplemental guides to enable the OMB to assess different capability areas within Zero Trust architecture, which will help form guidance that OMB will put out.
- There is another piece in the EO regarding technical reference architecture. There is a body of work that NIST produced with the DoD. This is about taking the best of what's out there and making meaningful, clear guidance for agencies. Each agency is going to be in a different portion of the journey. How do we meet them where they are and help them accelerate their timelines? This is a paradigm shift in the security approach – no user, system, or network service, whether outside or inside the perimeter, should be trusted. Identify everyone and everything to establish access as a privilege. There are culture change aspects, impacts on the business side of agencies.

Enhancing Software Supply Chain Security

- Defining critical software, enhancing software development and testing, and secure development practices.

Cyber Safety Review Board

- Led by DHS, this effort brings together government and industry in a formal way. The first review is directed at the Solar Winds incident.

Standardizing Federal Government Playbook for Responding to Cybersecurity Vulnerabilities and Incidents

- We all know security operation centers have incident response plans, but this is more about what leaders need from a best practices perspective to help coordinate the response to a significant incident. When you're making decisions that affect mission delivery, communications plans, procurement, privacy decisions, legal calls, etc., getting it into a playbook is a good idea.

Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Networks

- CISA has provided some recommendations to OMB on endpoint detection response capability, and they will issue guidance to agencies. Another part of this section, which is bureaucratic but important, is getting memorandums of agreement signed or updated between agencies and CISA for the Continuous Diagnostics and Mitigation (CDM) Program to continue. Make sure paperwork is in place to achieve the mission.

Improving the Federal Government's Investigative and Remediation Capabilities

- This is largely about enhancing maturity around capturing, retaining, and analyzing logs. Log management could be viewed as a tactical thing, but it is a key enabler of all sorts of things. The strategic benefit of having the visibility to detect, contain, or remediate an event is something they need to move fast on across the federal government. That's a key lesson learned from recent events. There are so many different types of logs you need to capture from so many different places for a successful digital forensic investigation. Log management isn't the flashiest of topics, but it's a very important one. It's one of those things that the community will help make better over time.

There is a lot of work in the EO. OMB is directly involved in 45 tasks and is keeping tabs on all of them. Mr. DeRusha's office has an action in pretty much every section. This is a whole-of-government approach, but they are using the councils – the CIO Council, the Chief Acquisition Officer Council, and others – to get the deliverables sharp and get feedback early from agencies as to whether they are moving in the right direction.

Discussion

- Ms. Miller asked, with regard to Zero Trust Security Reference Architecture, if the CISO Council is looking at taking the standards DISA pulled together and considering some level of standardization across agencies to minimize interoperability issues. Also, what conversations are they having to adjust targets for FISMA and FITARA?

  Mr. DeRusha said they are looking at the DoD reference architecture. They don't want to move in a different direction, but agencies need more explicit guidance. They will start a new agenda across agency protocols and FISMA metric targets based on Administration priorities and update all of it accordingly.

- The Chair asked about the Cyber Safety Review Board and whether it has what it needs to work across the government. Or, as incidents occur, will there be impediments in terms of agency limitations and a need for legislation?

  Mr. DeRusha said DHS will kick it off and get it coordinated. Industry members have been collaborative since SolarWinds in figuring out how to work together in a more meaningful way than in the past. Everyone sees this as a moment to try harder. DHS has everything it needs to get the information that they are looking for. If they don't, it will be one of the findings that comes out in the review.

The Chair thanked the speaker and wished him well with the EO implementation. He recessed the meeting for a 13-minute break.

EO 14028 Section 4(e): Supply Chain Security

Jon Boyens, ITL; Matthew Scholl, ITL; Kevin Stine, ITL

Mr. Scholl noted that on Thursday the board would hear about specific, immediate EO-related deliverables NIST is working on as well as deliverables that DHS and CISA have completed. In this session, they will touch on some other areas of the EO at a higher level.

Mr. Stine said they have a slightly longer lead time for deliverable dates, but they are still very ambitious. Fortunately, they are not starting from scratch and have a body of resources to pull from and leverage as much as possible.

Overview of Section 4(e)

- Section 4(e) Task: Issue guidance and identify practices that enhance the security of the software supply chain. The guidance will include standards, procedures, and criteria regarding a number of areas. There are quite a number of subtasks under 4(e). A number of sub-elements focus on software development environment security.
- Timeline: Guidance will be issued around Day 270.
- Approach: Seek public comment on different resources. The Secure Software Development Framework (SSDF) will be the anchor for much of the work. They are always open to receiving guidance. They will extend the SSDF and produce additional guidance as needed.
- Touchpoints between 4(e) and other parts of Section 4. Section 4(r) has NIST consulting with the NSA to publish guidelines recommending minimum standards for vendors to test their software source code. Some of the same tools, potentially some of the same processes, and some of the artifacts and evidence generated along the lines of 4(r) can help achieve some of the desired outcomes in the two sub-elements of 4(e).
- Section 4(f) tasks NIST with publishing the minimum elements for a software bill of materials (SBOM). There was a lot of discussion about SBOM at the June 2-3 workshop. A lot of the input would be valuable to NTIA as well. The position papers received in advance of the workshop were terrific also.

Secure Software Development Framework

- When they looked at the EO, they built a flowchart to ensure that they understood not just the timing but also the dependencies of the different deliverables so they could leverage other sections. When they looked at some of the requirements, such as publishing guidance and standards, one of the first things they did was consider existing NIST guidance.

  In April of 2020, working with industry, NIST published a white paper titled “Mitigating the Risks of Software Vulnerabilities by Adopting a Secure Software Development Framework.” They looked at common outcomes that many different SDLs have to improve security of software. There are four over-arching outcomes that fit nicely into the requirements in the EO. One is “Preparing the Organization.” As people, process, and technology, they are prepared to perform secure software development at an organizational level and protect the software from tampering or unauthorized access. They plan to elevate the white paper to a NIST report or special publication and use it as the pivot point for the guidance.
- They are not planning to recommend or identify a single SDL that an organization should use. If an organization is using an IEEE process, ISO process, CMM process, or a process that they created that meets their requirements and can be expressed in the outcomes highlighted in the

white paper, then initially that is sufficient. They will be looking for a disciplined, repeatable, and managed process for creating secure software.

Discussion

- Mr. Venables said there are two ways of looking at this: 1) Secure software development lifecycles are designed to increase the likelihood that the software produced is as free from vulnerabilities as it reasonably can be; or 2) Secure the software development lifecycle to make sure the environment is secure enough that rogue software can't be maliciously introduced in the source code or in the build and development tools. In some of the public commentary, those two views have been mixed up. They have very different goals with very different requirements. A lot of organizations have implemented or are striving to implement the first. Will it be clear that they are two separate things driven by different implementations?

  Mr. Scholl said yes, they are going to do their best to ensure that they are clear in the guidance. There is a product that will be produced, and there is a clean room where it will be produced. A third piece in this section is for federal agencies – are there additional security concerns, considerations, or controls that should go along with the implementation? So, it comes down to (1) the development of the software so that it is as robust as it potentially can be, (2) the environment in which it is developed, and (3) the environment in which it is used.

  Mr. Baker said there may be an additional piece: Transmission

Other Areas

- The acquisition process is also raised in a couple different places in the EO. They are trying to pull all of those threads together and figure out what guidance is available and then see where the gaps are. They partnered with DHS on co-branding a white paper on defending against supply chain attacks, which pulls in guidance from different places. From a practical point of view, it isn't helpful to have to go to many different places for information. One of the jobs when providing the guidance is to streamline everything so it's simple and understandable for the agencies to use. That's where Section 4(c) fits in. They are publishing preliminary guidelines within 180 days, and so some of that can also be inserted in Section 4(e), which is due 90 days after the preliminary guidance.
- In 2018, NIST and NSA published a white paper titled "Security Considerations for Code Signing." They will leverage that paper to help address this specific piece of the EO. How to ensure you are set up for the capability to run a code signing practice in your organization. They will elevate the white paper and then re-open it for comment and discussion to ensure it is still relevant and applicable.
- For many tasks in the EO, they will use this method of taking existing work and re-opening it for public comment to ensure that, even with the quick timeline, they get as much external input as possible.
- Returning to Mr. Venable's question, Mr. Stine said that when he looks at the SSDF today, it is minimally focused on the build and development environments. This is an area for expansion in the SSDF. The feedback they will be looking for is building on the existing SSDF. They will start with the action in the EO, such as administratively separate build environments. They will want feedback on what else to include and the best way to incorporate it in the SSDF.

Identifying Practices that Enhance Security of Software Supply Chain

- Not too long ago NIST released an update to the foundational supply chain risk management guidance, SP 800-161. They are going into Revision 1, and comments are due Friday. They will have a second public draft out in October and a final next spring, but the timelines are flexible. The idea is to try to put Section 4(c) into the update to SP 800-161 as an appendix. That will add flexibility to be able to update it as needed, and it has the added benefit of getting public feedback into it.

Guidance on Attesting to Conformity with Secure Software Development Practices

- The intent is for vendors to self-attest. They are going to look at leveraging the ISO standard for vendor self-attestation. NIST is not planning to be an auditor of attestations or to verify them. They have found that self-attestations have muscle, generally because of the business risk that a company puts on the line when they themselves are verifying what they are doing. When it is a second- or third-party testing company, it becomes a business transfer of risk – they can say it's the second or third party's fault. When NIST looks at the range of risk they are trying to address, timeliness, the effect that an attestation will have on a company in delivering its product, and the effectiveness in providing confidence, self-attestation might be the only effective mechanism.

Discussion

- The Chair noted the distinction between the secure development process and the code integrity process. They're complimentary but different, and both are necessary. In the SSDF, we put less emphasis on the code integrity side than on the secure development side, but it is reasonable to go back and revisit that. The SSDF has enough specifics to know what you ought to do and enough generality to be adopted and adapted to size, scope, and process. Try to retain this balance in the SSDF as it is expanded.
- The Chair asked to what extent Section 4 applies to the Cloud and online services.

  Mr. Stine said the EO was not as clear on that as it could be. NIST is trying to take into account software in any shape or form – whether it is stand-alone software or software as a service.

  Mr. Scholl said this is about the dependencies and how things fit together. The software development lifecycle practice and the guidance on securing a development environment will be, to some extent, agnostic to the delivery method or the hosting architectures of the software. This is being aggressively discussed as far as the most appropriate scoping within the context the EO has given to consider critical software.

  The Chair said you have to do different things depending on whether you're building for Cloud or building for a boxed product. You're doing the same stuff at the SSDF level of generality. Things like attesting, deliverables, and information shared with a customer are the kinds of things that are done differently depending on whether you're shipping a software update every 6 months or delivering a SaaS Cloud that gets updated 16 times a day.

  Mr. Scholl said this comes back to some of the FISMA and audit sections as well. They have plenty of guidance around high-impact systems, high-value assets, and CUI-enhanced data. That's really a system for information, not really about software itself. Some of it will have to be tailored to be appropriate for software. They will revisit their configuration guidance and checklist programs where they have specific security configurations for specific products so that when a piece of software is identified as EO critical, they will focus on security configurations for that software. The checklist program for configurations is going to be one of the main areas they will look at.
- Mr. Venables asked if they need more input from ISPAB between meetings. Will there be sub-advisory boards for each of the areas?

Mr. Stine said they want as much feedback as ISPAB can give. There will be many opportunities for public comment and they would love the board to share feedback early and often.

Mr. Scholl said the board could do a half-day meeting between the main meetings. That's a decision for the board to make.

The Chair said NIST is requesting public comment on individual pieces of the EO, and board members are free to comment as individuals. It might be good if there was a time between now and the December meeting to take a look at things in the EO implementation where it might be helpful to provide input.

Mr. Scholl said they can set that up. He will send out the slide with the timeline of deliverables.

- Ms. Hallowell asked about the shift left movement and remediation. Were there discussions about doing software testing differently, maybe earlier in the cycle?

  Mr. Scholl said there will be a session on Thursday about software testing.

  Ms. Fitzgerald-McKay said the shift left topic has come up a lot.

Public Comment, Summary of Day 1, and Board Discussions

There were no requests from the public to comment.

The Chair thanked the board members and speakers and adjourned the meeting for the day at 3:40 p.m. ET.

Thursday June 24, 2021

EO 14028 Section 4(f): Software Bill of Materials

Allan Friedman, Director of Cybersecurity Initiatives, NTIA

The Chair opened the meeting at 10 a.m. ET and welcomed Allan Friedman, Director of Cybersecurity Initiatives, National Telecommunications and Information Administration (NTIA).

SBOM Overview

- Definition: A list of ingredients or a nested inventory for software; a formal record containing the details and supply chain relationships of various components used in building software.
- We should expect the same supply chain transparency from critical infrastructure as we do from tasty, non-biodegradable snacks. Knowing that Twinkies contain tallow doesn't prevent anyone from eating them. Having transparency supports a more sophisticated risk-based posture.
- "The trust we place on our digital infrastructure theater should be transparent – should be proportional to how trustworthy and transparent that infrastructure is."
- "Trustworthy or transparent, they're substitutes. So, the less trust you have in the actual software itself, the more important transparency is."
- EO 14028 defines SBOM functionally, looking at specific parts of the software lifecycle: Producers – Buyers – Operators: Many of us are in the middle.
- Section 4(f) gives the Commerce Department 60 days to define the minimum elements of SBOM

- Section 4(e)(vii) tasks the government with thinking about how to include SBOM in the broader effort of including supply chain security efforts and tools – how to take the definition of minimum elements and translate that into rules.

Proposed Minimum Elements

- Data Fields: Supplier name; component name; version of component; any other unique identifiers; author of the SBOM data; dependency relationship; cryptographic hash of the component.
- Operational Considerations: Elements of SBOM include operational and business decisions and actions that establish the practice of requesting, generating, sharing, and consuming SBOMs, including frequency, depth, and delivery.
- Automation Support: Any security approach in 2021 that is not built for automation is at risk of not coming to fruition. To scale across the software ecosystem, support for automation, including automatic generation and machine readability, is key. Three existing data standards to convey data fields and support operations have been identified: SPDX, CycloneDX, and SWID tags.

Discussion

- Mr. Groman said he continues to wonder why we didn't do this years ago, although he appreciates that the technology is relatively new and evolving. Potentially missing from minimum elements is something about risk. Before I pop code into a product or software, which I then sell, presumably I've done some assessment that I'm not enhancing risk.

  Mr. Friedman said he agrees with the vision. A lot of people in the security world are working toward it. SBOM is one of the building blocks needed to help that scale. One challenge is that we do not have a common way of thinking about risk. There is the Common Vulnerability Enumeration (CVE) platform, and even that is controversial. There are start-ups specializing in doing some of the due diligence. There is a lot of risk we know we need to capture, and SBOM is a step toward getting visibility.

  Mr. Groman asked if there is something that can reflect that somebody did something to assess risk, even if we don't have a common language for it?

  Mr. Friedman said there are people in the U.S. government, including in the Air Force, who have said they're doing this work – they've done the risk analysis.

- Mr. Venables said that one of the things he finds worrying is that SBOM would be seen as the answer to everything. You could have a great SBOM, but there is still malware implanted in the software. SBOM is a means of conveying information about the provider's build process. Are we doing enough to convey that SBOM is not the solution to everything?

  Mr. Friedman said the second most common type of comment was that this does not go far enough. How to convey it is an important question. There is a community-driven approach, which NTIA helps facilitate, devoted to awareness and adoption. We need to make sure we're not overselling the benefits. Like CVE, it doesn't solve any vulnerabilities by itself. It's just a way of tracking the data. But once we have the data, it supports an incredibly rich ecosystem of tools and data management that allow organizations to get a handle on their risk. SBOM is a data layer that allows better management and better integration into tools.

  Mr. Venables said it might be helpful to show a future roadmap so that people don't see this as a panacea.

Mr. Friedman said that as they think about a roadmap, they need to consider the diversity of the software ecosystem.

Processes and Practices

- How often do you generate an SBOM? What is the depth of the dependency tree? How is the data going to be shared? What is the access control policy?
- Having a single solution simply won't fit, but we can shrink the universe and offer some clearly defined paths.

Other Considerations and Related Issues

- Software identity
- SaaS
- Legacy and binary-only software
- Integrity and authenticity
- Supply chain threat models
- High assurance use cases
- Depth and transparency
- Risk management and exploitability ("VEX")
- Flexibility vs. uniformity: How to not overwhelm industry
- SBOM today vs. SBOM tomorrow

Process at NTIA

- Starting Point: Three years of open, transparent, industry-led efforts
- Request for Comments (June 2 – June 17) - Approximately 85 comments received:
  - Most common comment: Go Slow on regulations and requirements; begin with the basics.
  - We need standards. The challenge is, standards for what? CycloneDX and SPDX have been good about saying, "We're going to experiment, try things, use our open process, and then move that into an official standards process." The Linux Foundation has already standardized some of the work done on open source management.
  - Rules are out of scope of Section 4(f), and a deliberate process is explicitly built into EO 14028. The minimum elements are insufficient for supply chain risks. We need a lot more data from the build process and from the supply chain. We will make sure we can have a path towards moving forward.
  - SBOMs and software manifests exist already. People are doing this internally. Several large trade associations said this was an industry best practice.
  - How should we think about SaaS and cloud-based applications? The use cases on how the data should flow downstream should be treated differently for a variety of reasons.
- Cross-government consultation
  - Many people said they needed this yesterday.
  - There is some concern, especially from less well-resourced organizations, that if this data is on their network, it will create an obligation to act on it and they would need support for that. Related to that is the need for tools. That's been one of the challenges expressed – we're stuck in this chicken-and-egg approach.
  - There was some desire across different corners of government to ask if the data can be pooled to think about overall risk for national security or the U.S. government in general.

Ongoing NTIA SBOM Community Work

- Finalizing "playbooks" for SBOM generation and consumption

- Revising initial definitions and framing documents
- Plugfests to support the tooling ecosystem and interoperability
- Proof of concept work beyond healthcare (automotive; energy/power; finance)
- VEX and CSAF Collaboration – not all vulnerabilities put customers at risk – allow someone to communicate downstream that they are not affected
- Awareness and adoption: Push back against idea that SBOM will solve all problems

Discussion

- Ms. Miller asked how agencies with national security systems deal with the issue of SBOMs.

  Mr. Friedman said that is not a community he had extensive experience with. After defining the minimum elements, they will share it with their colleagues to make sure it doesn't raise red flags for them.

- Ms. Fitzgerald-McKay said national security systems often refresh at a different pace. They may need the SBOM data but not be able to procure something new to get it. Is there a process built in for an organization to create an SBOM on their own?

  Mr. Friedman said that question has interesting complications. There are licensing rules, and people have different perspectives about their obligations. It varies by which corner of the software world you're dealing with.

- The Chair commented that the challenge of reflecting risk in an SBOM is that it will vary depending on what you are using a component for. You can either mitigate or amplify an upstream vulnerability. To the extent organizations start to adopt secure development processes, it might make sense to attribute that sort of process.

  Mr. Friedman said that goes to the range of maturity where we might expect an organization that has this data to use it. For example, the Mayo Clinic demands an SBOM before they allow a new device on their network. Their security team will seldom overrule the medical team in terms of what they need. But if they see it's full of outdated, vulnerable stuff, it will delay the purchase. Their customers have learned they need the SBOM. When there is life-saving technology they need, there are other things the security team can do, such as segment the networks, tune the intrusion detection system, or work with the threat intelligence community. We see this maturity path in just about every area of cybersecurity. Threat intelligence used to be a specialized, bespoke, hand-rolled thing that only the elites had.

- Ms. Fitzgerald-McKay asked about the appetite for adopting SBOMs in the telecom community.

  Mr. Friedman said different trade associations have different approaches. They will be meeting with TIA, which is working on ISO standards that they think are relevant. In the 5G space, we are moving towards a purely software-based approach.

- Mr. Groman asked if we are heading to a place where this will be mandatory.

  Mr. Friedman said that as he reads the EO, the next steps are that NIST is going to be working with folks across government on standards and practices and that will get folded into acquisitions.

The Chair thanked the speaker and wished him luck with the EO efforts.

EO 14028 Section 8(b): Logging Events and Retention

Harry Mourtos, IT Specialist (INFOSEC), DHS

Overview of Section 8(b)

- Directs DHS to make recommendations to OMB on logging events and retaining other relevant data within an agency's systems and networks.
- Roughly 35-40 tasks in areas they are either participating in or consulting on.
- The EO is greater than the sum of its parts. For example, the last line in Section 8(b) stipulates keeping the recommendations in mind as they put together the FAR Council recommendations that are tasked in Section 2.
- The EO tasks the OMB Director with producing a policy memo to enact the logging recommendations. DHS is still working with OMB to reach a balance on what the memo will look like. The memo is due within 90 days of CISA providing the logging recommendations.
- One of the goals is to ensure a commonality and common standards across the federal government.

Recommendations

- They provided recommendations on log storage requirements, log formatting requirements, standardized time stamps, and more. They organized it by criticality levels: What do agencies need to do right now? What is the next critical set of logs? What can they put off for a while?
- Criticality Levels
  - Criticality 0: The absolute baseline needed to enable an incident response or forensic capability: Keeping tabs on identity/credential management; DNS logs for source and destination; IP input; monitoring IP and domain reputation data for email, network device infrastructure.
  - Criticality 1: Authentication and authorization; endpoint detection and response. Virtualization logs; mobile device management.
  - Criticality 2: 72-hour full packet capture
  - Criticality 3: User agent logs; spam dictionary modifications
- Maturity Model: They wanted to build a roadmap and path forward to empower adoption and provide a chance to ramp up to build capacity over time.
  - Maturity Level 1: Minimum logging data for Criticality 0 and Criticality 1. Building consistent timestamp infrastructure across logs to make sure the timestamps match up so you can accurately determine a course of events.
  - Maturity Level 2: Making sure DNS logging is visible at the top-level enterprise SOC at the department or agency. Not just storing and maintaining them, but also having them in a format where they can be queried on demand.
  - Maturity Level 3: Looking at user behavior monitoring, implementation of automation for log analysis, and advanced, centralized access.
  - They realize this is going to be a big shift for the federal government. They are looking at a variety of possibilities to help agencies move forward to the higher level of maturity when it comes to log management. They are exploring a self-assessment tool, which will be a questionnaire for agencies to determine where they fall on the maturity model.

Other EO Areas CISA is Working On

- Section 6: CISA is tasked with creating a vulnerability and incident response playbook.
- Section 7: Endpoint Detection and Response – This is factored that into the criticality and maturity models.

Discussion

- Ms. Hallawell asked how they are assessing criticality.

  Mr. Mourtos said a qualitative analysis was made by their incident response teams.

Ms. Hallawell asked how someone would interpret a criticality level in terms of what more it would give them.

Mr. Mourtos said that if an organization has not implemented Criticality 1, then Criticality 2 is not going to add a substantial value.

- The Chair asked if there are standards that are already in place or need to be developed.

  Mr. Mourtos said this is one of the biggest difficulties in producing something like this. They can't account for every potential configuration. They aim to keep recommendations at a strategic or tactical level. Built into the maturity model are recommendations for standardized date and time formats and a recommendation that they be standardized using GPS or the NIST federated timestamp system. They are asking that when the incident response team shows up, they will have the capability of knowing what they're looking at.

  The Chair said it seems like that would be of value for CISA and NIST to think about. More standardization and sophisticated tools would be helpful.

  Mr. Mourtos said a lot of their recommendations were born out of the experience responding to the December 2020 incident. They found that logs would not always be in a machine-readable format, and it would take several days to get the data ready to be analyzed.

- Mr. Gattoni said we should look at standardizing not just the format but also the meta data and the tagging around it. It's probably easier to convert like time formats than to discover that a random integer represents time.

  Mr. Mourtos said that is part of Maturity Level 1 – that all logs should have a standardized date and time structure that they've prescribed.

- The Chair asked about log integrity and protection from modification.

  Mr. Mourtos said that is baked into Maturity Level 1. It is one of the elements mandated as part of EO Section 8(b). It is one of the more specific technical prescriptions in the EO.

The Chair thanked the speaker and recessed the meeting for a 20-minute break.

EO 14028 Section 4(r): SDL and Software Testing Guidance

Paul Black, ITL, NIST

Section 4(r)

- "Within 60 days, NIST shall publish guidelines recommending minimum standards for vendors' testing of their software source code, including identifying recommended types of manual or automated testing."

Sections 4e(iv) and 4e(v)

- There are no teeth behind Section 4(r). There's no mandate in the EO that it must be followed. After this report gets published, the real work begins because there are some testing mandates in the EO that do have some teeth: Sections 4e(iv) and 4e(v)
  - 4(e)(iv): Use automated tools to check for vulnerabilities.
  - 4(e)(v): Provide artifacts of the tools and make summary data available.
- Goals of Guidelines for 4(e)(iv) and 4(e)(v):
  - Effectiveness: Lead to more secure software.
  - Efficiency: Apply some of the highest benefit/cost ratios, approaches, tools.

  - Flexibility: Keep an eye to current variations and future innovation. Ensure that small shops will be able to adopt them.
- The challenge of 4(e)(v), in particular, is efficiency: Prove that you tested, and prove that it helped. What could you provide that communicates assurance? We want the summaries to be reasonable to produce and review without disclosing too much proprietary information.

Scope of Section 4(r)

- "source code" – Include binaries, bytecode, and executables. If there are libraries or packages in the product, you should do a software assessment assurance on those. Simply saying "source code" is too limiting.
- "testing" – Defined broadly as software assurance – any techniques or procedure performed on the software itself to gain assurance that the software will perform as desired, has the necessary properties, and has no important vulnerabilities.
- "vendors testing" – It is more efficient to have developers do the testing as they develop the software. They know the ins and outs. They can produce artifacts, like proof-carrying code and proofs of properties that could be checked.
- "minimum standards" – Get the developers to use techniques they should be using, and this would be a basis for more rigorous standards (Sections 4(e)(iv) and (e)(v)).

Discussion

- The Chair said he thinks of testing as dynamic. If the EO thinks of static analysis as security testing, different vendors and different technologies will have different optimum combinations of static and dynamic source code versus binary.

  Mr. Black said there is a surprisingly large amount of formal methods work that is practical and used often. Many times, some of the hardest vulnerabilities to fix are architecture problems. Formal proofs of the architecture or the data flow are done all the time, especially in Europe. There's no reason it couldn't be done here. It's about getting people to understand that if they do formal development, they can reduce development time. The formal methods are telling yourself upfront that this is going to work out and filling in details as you go along. It doesn't require a whole host of PhDs. Regular programmers can do it.

  The Chair said large development organizations are applying formal verifications successfully to some things. He saw a recent presentation by a colleague whose experience with formal code verification was the opposite of what Mr. Black asserted. The tools were immature and required that wizard run his wand over them every morning. Ordinary developers couldn't use them. He does agree that security and security processes should be done by real industrial developers.

  Mr. Black said there are places where formal methods can be dropped in.

Guidelines for Section 4(r)

- Threat modeling
- Automated testing framework: They need to be executed automatically so that they're done correctly, and the outputs need to be checked carefully.
- Static *and* dynamic testing
  - They complement each other. There are some things you can find only by looking at the code. If you've got a backdoor, if the message starts with a particular string, there's no possible way that external testing could uncover it. If you look for hard-coded passwords and encryption keys, they are most likely found by looking through the code. With dynamic

  analysis, you get to skip the questions such as, "Did my compiler do the right thing?" There are fewer assumptions involved.
  - The space of functionality. If you're thinking about a program as a gigantic function table, you have an enormously high input. Most bugs have a very small cross section, and only certain conditions will expose them.
- Code-based (static) analysis:
  - Use a code scanner to look for top bugs.
  - Use heuristic tools or focused manual code reviews: Look for malicious code or "values of concern." Backdoors and logic bombs may be triggered by a nearly endless variety of conditions. Threat modeling may reveal small sections of software at very high risk thus warranting additional manual code review. Examination may be manual, tool-assisted, or automated. Tools can do better if they're looking for hard-coded passwords or encryption keys.
- Dynamic analysis (i.e. run the program on test cases)
  - Compile and run with built-in checks and protections on. Compilers have incorporated a lot of things that used to be external checkers; too many people don't know about them, and too many people don't turn them on.
  - Create black box test cases: Look at the specifications, security policies, threat assessment and run test cases based on those.
  - Create code-based test cases: Look at how the code is structured; make sure you're exercising all the options.
  - Use test cases created to catch previous bugs: If you wrote test cases to prevent bugs, run them again.
  - Run a fuzzer: Fuzzers don't usually go very deep, but they're relatively cheap to run and they tend to exercise the code with bizarre inputs that even crazy testers would not think of using.
- Specialized testing: If the software is going to be connected to the internet, it should be tested with a web app scanner. Advanced web app scanners (Interactive Application Security Testing) have probes that watch the execution paths and try to drive the tests to look at many paths and values more thoroughly. If it's multi-threaded or parallel processing, it should be tested for race conditions and deadlocks.
- Fix the critical bugs that are uncovered. If we merely say, "Do the test," then somebody might say, "I did the test. I didn't fix anything, but I did the test." Improve your process to prevent the bugs or catch them earlier.
- Do some sort of testing on the libraries, packages, and services you are embedding in the software.

Rest of the Report

- Section 2 explains how the pieces of the minimum relate to each other.
- Section 3 talks about techniques and approaches, and each subsection is a mini-tutorial. It includes information such as going beyond the minimum, example tools, citations for documents, published reports, and related practices, standards, guides, etc.
- Section 4 expands beyond testing to the full software development life cycle (SDLC). It outlines the need to design well, have at least some programmers with security training, and have security principles. There needs to be the SBOM.

Discussion

- The Chair said with regard to backdoors, it would be useful to publish a special publication on what to look for when you're looking for malicious code.

Mr. Black said he has been trying to find papers and articles that back up the things they say. Most of the stuff is out there someplace.

- Ms. Fitzgerald-McKay asked if there is a sense that they will have to attest to the bugs they fix.

  Mr. Black said he doesn't see that that would be valuable to report the bugs found or fixed. It might be interesting in auditing the process to say they found 88 bugs and maybe they should go back and change their process.

  Ms. Fitzgerald-McKay said she thinks that's less valuable for new code being developed. She asked if there might be a case for it for code being imported into a product.

  Mr. Black said that commenting on the bugs found and fixed is a way of estimating the ones you didn't find or haven't been fixed. That could have value. If you found a bug and didn't fix it, there is an argument for listing it and telling the people you pass it along to. It makes it a little easier for the attacker, but the attacker has to find only one weakness. If we're helping the defender, we're helping them a lot. If we're helping the attacker, they would have found a vulnerability anyway.

  We don't have an algebra for risk. Composition of risk in SBOM is a difficult subject. The more pragmatic people say, well yeah, but let's do something. Rating riskiness or threat levels really depends on context. He heard that Google just restarts the code if a search crashes because of the code. Because the crash is such an evident failure, they just ignore it. Being able to come up with one risk or threat composition is an interesting topic.

  Ms. Fitzgerald-McKay said maybe the Cyber Safety Review Board could have some kind of role in figuring out what went wrong in an incident, and maybe that information would eventually get us closer.

  Mr. Black said there is the notion of looking at failures that occur and reviewing possible checks, and maybe they wouldn't happen again.

  The Chair said the capture/recapture model is useful. It's a good way to know where you are. More actionable is characterizing the must-fixes based on actual impact on the kinds of systems you're building.

- The Chair noted that they had not heard much about Section 4(e)(i), secure development environments.

  Mr. Scholl said they very lightly touched on it the day before. They will move into SDLs and securing the development environment.

  The Chair said that might be a topic for an out-of-cycle meeting.

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

EO 14028 Section 4(g): Critical Software

Barbara Guttman, ITL, NIST

Section 4 Requirements for Critical Software for:

1) Government procurement: Security measures vendors have to attest to, like using a secure development process, testing the software, having integrity and provenance checks. These security measures are called out in Section 4(e).
2) How the software is used inside government

Process of Defining Critical Software

- Timeline: Definition of critical software was due 45 days after the EO was signed. It was set for release June 25.
- There is a tight coupling between NIST, which comes up with the definition, CISA, which comes up with the categories, and OMB, which writes the implementation rules. They also received input from other agencies.
- Workshop; white papers submitted

Three Over-arching Goals

- Seamless transition from NIST to CISA to OMB
- Clarity: Vendors need to know if their products are in or out.
- Viability: Implementation must consider the complexities of the software marketplace.

Terminology

- The term "EO critical" is used within the definition to distinguish it from the common usage of critical.
- Context orientation vs. product orientation: This issue was seen in a lot of white papers they received and discussions they had. Security people tend to talk about "critical" in terms of what a system does – a context-oriented way of thinking. The EO is product-oriented – a vendor needs to know if a product is EO critical independent of context or use. You have to think in a product-centric way because that drives procurement.

Phased Implementation

- Start with a subset of all possible software that could be considered critical and then improve the program as it goes along. This allows time for coordination.

Definition

- Core Definition: Any software that has, or has direct software dependencies upon, one or more components with at least one of the following attributes:
  - Is designed to run with elevated privilege or manage privileges
  - Has direct or privileged access to networking computing resources
  - Is designed to control access to data or operational technology
  - Performs a function critical to trust
  - Operates outside of normal trust boundaries with privileged access

  This applies to products that are going to be used operationally, not just used for research purposes.
- Initial Implementation Phase: Focus on standalone, on-premises software that has security-critical functions or poses similar significant potential for harm if compromised. If you have a hybrid system and you have agents running locally and they have EO critical functions, that counts in the initial phase.
- Preliminary List of Software Categories Considered to be EO Critical (The official list of categories comes from CISA.)
  - Identity, credential, and access management (ICAM)
  - Operating systems, hypervisors, container environments
  - Web browsers
  - Endpoint security
  - Network control
  - Network protection

- Network monitoring and configuration
- Operational monitoring and analysis
- Remote scanning
- Remote access and configuration management
- Backup/recovery and remote storage

There are many other categories of important software that aren't in the first step, such as database access control, email servers, collaboration tools, cloud-based and hybrid software, software development tools, code repository, integration software, and packaging software.

The vendor only needs to attest to the EO critical components. The question was raised, won't this lead to confusion or a gaming of the system? The answer is potentially. The higher level objective when using self-attestation is to have vendors make specific attestations that are meaningful. The goal is to focus on these components and have maximum transparency and honesty.

- FAQs – Because there are a lot of different ways to look at this problem, people had questions about things like direct software dependencies and functions that are critical to trust.
  - Does it matter if the software product is in the Cloud, on-premises, or in a hybrid environment? No. If the software is doing something critical, then the software has to meet the EO critical definition.
  - Won't this lead to gaming of the system? Potentially. The objective is to have vendors make specific attestations that are meaningful. The goal is maximum transparency.
  - What about open source? If an open source software performs functions that are defined as EO critical, then it is EO critical. From a practical point of view, most open source work ends up in other products, so those vendors will need to handle the 4(e) security measures and attestations. If open source is brought in directly to the government, then the government needs to handle the 4(e) security measures.

Discussion

- Mr. Groman asked about the definition of "harm" in this context.

  Ms. Guttman said it's "potential for harm." Once you start defining harm in terms of your critical operations or critical things, it becomes a rabbit hole. They tried to circumvent the rabbit hole by building this bridge with CISA to go directly into the categories.

  Mr. Stine said the EO uses the phrase "the potential for harm if compromised." They had to make determinations about what that meant in the context of the criteria or the definition that they were going to propose. Some of this will have to be more fleshed out as the program evolves.

  Ms. Guttman said if your OS is compromised, that's really bad. If your VPN software is compromised, that's really bad. They looked at these security-critical functions. Most harm is going to be context-sensitive, and this is product-oriented. You have to come at the problem from both sides, and they meet at the table of categories.

  Mr. Groman said that in the legal and policy world, the word "harm" is incredibly problematic because it is used to circumvent, manipulate, or navigate around. Harm around data security is like an externality to the vendors.

  Ms. Guttman said that level of harm is very downstream. They are upstream at the product level with its potential for harm.

Mr. Groman asked how the government as a buyer gets a supply chain that's secure? When you have thousands of small incidents that accumulate to, "Wow . . . all of our data is sitting in North Korea now," that's hard when we talk about harms. One vendor selling one product may not think about it.

Ms. Guttman said the EO doesn't solve all of these problems. It is trying to address one piece of it. The goal is to make the world better, not to boil the ocean.

Mr. Scholl said it's an interesting topic that maybe they may need to take up later. Mr. Black had made a statement about building codes in his analogy to testing. Software harms could be portrayed as not as significant – quantifying harm is an interesting topic. Maybe potentially this is a topic for an interim meeting.

Ms. Fitzgerald-McKay said the ultimate concern is how this definition would be applied. What is the role of OMB and CISA to make sure it is applied to the right places?

Mr. Groman said he's operating at a bigger picture level. The government could do this but hasn't had the will to do what is necessary.

Mr. Black said the Bureau of the Census looks at the question of cumulative knowledge leaking.

Mr. Groman said everybody gets a waiver or an exemption, and all the exemptions swallow the rule. He would like to see more ownership of the bigger harm.

The Chair recalled that the government, up until when the EO was signed, has had no requirements or effective measures that would influence the security of the software it acquires. If this EO raises the bar, the world becomes a better place. The requirements of the EO apply to everyone from Microsoft to Joe's Storm Door and Firewall Co., so they have to be general. A secret about building codes is that they're extremely detailed – what kind of nut, what kind of thread, what kind of metal in the nut, what kind of torque to fasten the nut. NIST can't get down to that level of detail. At the moment, what we need to do is put down a marker that says, hey, you've got to pay attention to this stuff and do basic development hygiene.

Mr. Groman said there should be more consideration around the concept of "the potential to cause significant harm." Having more explanation around that concept would help a vendor think about it. We can never have granular requirements on everything, but everyone should think about harm in a certain kind of way.

Mr. Venables said this places an absolute imperative on the frameworks that are going to come out of the other processes. It's important to have frameworks that permit companies to have different maturity levels. The magic is to enable criticality over time. The key is how the whole thing holds together as a coherent system. The only thing he worries about is the rush to get all of the components done. He encouraged NIST and other agencies to take a step back and ask if it's all going to hang together as they expect.

Mr. Groman said he never started a process in government in cybersecurity where everyone in industry did not say, "Slow down" or "My small company can't do this." If you want to sell to the Pentagon, you've got to be secure. Period.

- Mr. Venables said that getting people through the maturity levels is what will be key. He asked the NIST team how they envision this working. Will there be interim milestones? There are a lot of companies in good shape, but there are a lot more companies that will have to fundamentally re-engineer themselves.

Ms. Guttman said that the EO doesn't have levels; you're just in or out. The Section 4(e) requirements are NIST's minimums for everybody.

Mr. Stine said some of this will be reflected in the FAR. The timelines will be determined in the FAR process. NIST's work is informative.

Mr. Scholl said the FAR updates will drive a lot of the start times. OMB in its oversight process will also be a governor of initiating a lot of the requirements internal to the government.

The Chair said he agrees with Mr. Venables that when starting from zero on the maturity curve there may be a lot to do. Mr. Groman makes a good point that people always say, "Gee, that's hard. Slow down." We know a lot more about software security and supply chain security than we knew 15 years ago. Keep up an appropriate level of pressure so that organizations don't say, "Let's do it next year, or next decade."

- Ms. Fitzgerald-McKay asked what was said in the FAQ about national security systems.

  Ms. Guttman said that is covered in Section 9.

- The Chair asked if someone has a component that's EO critical, is everything it depends on also EO critical?

  Ms. Guttman said everything it directly depends on is EO critical.

The Chair thanked the speaker.

EO 14028 Section 4(s): Pilot Labeling Programs

Katerina Megas, ITL; Warren Merkel, Standards Coordination Office, NIST

NIST Standards Coordination Office

- One responsibility of the Standards Coordination Office is to assist the federal government in implementing requirements in the National Technology Transfer and Advancement Act, where federal agencies use standards and conformity assessment to meet mission needs.
- They are advisors for other agencies when they have to establish programs that require use of certain standards or practices for conformity assessment, like testing, certification, or a supplier's declaration of conformity. Within the office is the National Voluntary Laboratory Accreditation Program (NVLAP), which includes a program that relates to labs that perform information security testing.

Section 4(s)

- This section of the EO talks about labeling and a potential scheme for how to do the conformity assessment that would result in a label.
- The task is informed by existing consumer product labeling programs generally.
- Educating the public is central to the effort.
- Along the way, they can also consider ways to incentivize device manufacturers and developers to participate in the program.

Section 4(v)

- They are required to conduct this in a manner consistent with OMB Circular A-119 and NIST SP 2000-02 (Conformity Assessment Considerations for Federal Agencies). The guidance is to look to the private sector when it's appropriate so that they don't re-invent things already available.
- They also look to international standards. There is a collection of standards published by ISO that look at how to perform conformity assessment – standards for testing, certification, supplier's

declaration of conformity. Those form the framework for how requirements can be placed on organizations doing those activities.

Section 4(w)

- One-year deadline to conduct a review of the pilot programs and consult with the private sector and relevant agencies to assess effectiveness.

Section 4(t)

- Requirements for the labeling program for IoT devices.
- Within 270 days, they have to identify the cybersecurity criteria for the labeling program and consider whether the program may be operated with, or modeled after, similar programs.

Section 4(u)

- Identify secure software development practices or criteria for a consumer software labeling program and consider wither the consumer labeling program may be operated in conjunction with others. It's a little bit more flexible in terms of the criteria.

NIST Approach

- Still in the planning and consideration stage.
- The intent is to be open, transparent, collaborative, and inclusive. They are in the planning stages for a workshop, which will probably be a 2-day event.
- They want to build on the experience of others in the United States and internationally.
  - They are seeking comments on recent white paper, "Confidence Mechanisms for IoT Devices," that looks at the standards and existing security labeling schemes for IoT in particular.
  - Existing efforts might be compatible with criteria and schemes NIST develops.
  - It is critical that they harmonize their approach so it doesn't create unnecessarily difficult or unique requirements.
  - The intent is to identify key elements for the labeling programs in terms of minimum requirements, technical requirements, and desirable attributes. They are not looking to establish a new program.
- They are taking into account public and private sector input to other software supply chain directives included in the EO

Initial Considerations

- Conducting landscape review of existing consumer IoT labeling and CA initiatives
  - National and international policy initiatives – They are taking a very broad view of the landscape.
  - Standards
  - Existing IoT device labeling schemes – Singapore has a labeling scheme, and there are efforts in the U.K. and in Finland.
- Processing public comments received on the white paper "Establishing Confidence in IoT Device Security: How do we get there?"
- A starting point for baseline technical criteria for IoT is likely the NISTIR 8259 series. Adapting core recommendations may need to be tailored for consumer market to consider:
  - Consumer as the customer
  - Inclusive of all components of consumer product
  - Informed by landscape review

  - Fit to be used as technical criteria
- Technical requirements will drive the assessment scheme. They have not made any determinations about conformity assessment yet, and they will evolve as they move forward. There are a number of different combinations of effective and appropriate conformity assessment tools.

Discussion

- The Chair noted that they said they were trying to avoid creating a new program. Would that imply something fitting under FTC product certification?

  Mr. Merkel said that rather than having NIST create its own program for evaluating products or software and making the attestation and putting on the label, they are thinking more along the lines of what the technical requirements for the device or software should be. What should the framework for conformity assessment be? They want to look to existing programs and see what elements are already out there that could meet those requirements. It is extremely critical to ensure that they are being ambitious enough that it's meaningful to consumers but also achievable.

- Ms. Megas asked the board for feedback on the shift to thinking about products. Do they think that any sort of product label would need to articulate features related not just to the security of the actual device but back-end systems also? Do they need to expand the device view to the system? Do they need to look at the mobile apps? Also, do increasing levels of assurance mean that at the lower levels are you looking at a baseline, and as you look at higher levels you require secure development environment?

- Ms. Hallawell said some of the high-level requirements around SDLC and penetration testing go to the level of oversight. How could we make sure that manufacturers are actually doing these things? How would that be monitored?

  Ms. Megas said they are looking at different models. There is one model that, at the higher level, requires third-party certification. Those requirements aren't at the lower level of assurance. At the lower level, it's mainly around self-attestation. At the other end, they're seeing a model that provides a baseline and options, but it doesn't have increasing levels of security requirements on the device.

  Mr. Merkel said it's important to be clear about the two different vectors at play. One is increasing levels of technical requirements. There could be very simple baseline requirements that are appropriate for a class of devices that would never need more than the baseline and potentially not a lot of independent verification. At the other end of the spectrum would be higher technical requirements that may inherently require additional resources, either at the manufacturer, developer or third party. On the conformity assessment side, with even the simplest requirements, if independence is important, you move to third parties. If further independence and more rigor are needed, you could go to a full third-party product certification. It's a matrix of the level of independence and the need for additional rigor and conformity assessment against the risk of non-conforming products in the marketplace. When you look at the risk of non-conformity, it really depends on what the technical requirements are. And then, how much do we need to bring to bear from a conformity assessment side to actually demonstrate to the consumer that the requirements have been met and meeting them was meaningful?

- Ms. Hallawell asked if they had seen any models internationally or in the United States that have particularly good guideposts around the stringent model for the higher levels. Is there anything that could be scaled or replicated?

  Mr. Merkel said there are examples that take various approaches to consider. The main thing for some of them is that the market effect would not be as large as it might be here. They are hoping to get feedback on those models.

  The Chair said they would not want to issue a label and have it become a joke. You want back-end practices and mobile app practices scoped so that the consumer gets a secure system, not a device that is broken into through a piece of software that isn't really part of the device.

The Chair thanked the speakers and wished them luck with the EO. He recessed the meeting for a 5-minute break.

Final Board Reviews, Recommendations and Discussions

The chair opened the discussion.

- Mr. Venables said it is important for NIST to take a step back and look at how all of the elements in the EO will hang together and influence each other. How will all the recommendations and frameworks be compatible?

  The Chair said that's a recommendation they could make without sending a letter. It's important to take a systems view of the pieces.

  Mr. Scholl said it's an excellent recommendation. After Friday, they can do that and ensure they aren't inadvertently cancelling out another action, so to speak.

  Mr. Stine said they are finalizing the project description now based on feedback received, and there will be more to talk about at the next meeting.

- The chair said he worries about the PQC transition and the number algorithms and opportunities for things to go wrong. There may not be a need to write anything formal, but it would be good for the board to hear about it.

  Mr. Scholl said they will also consider future agility issues in the context of PQC.

- Ms. Hallawell asked if the board should write a statement or position on the EO overall and on some of the NIST-specific deliverables. Is it in the board's purview to comment on overall EO and specific areas they talked about?

  Mr. Scholl said it is, and the comment can be made back to NIST and OMB.

  Ms. Hallawell said there are important specifics in the EO, and the overall coordination also is important.

  Mr. Gattoni asked if that's something they want to combine with an interim meeting.

  The Chair asked if it makes sense to meet in late September or early October. That may be a better time to make a recommendation. They will have the guidance for vendor testing, which is due in July. The supply chain guidance is due in November.

  Mr. Gattoni said he would add the reference architecture work, especially for the cloud security areas. He would also be interested in Mr. Groman's perspective on privacy implications of gathering and retaining data and making decisions based on identity, not just for users of federal systems but also public-facing systems.

The Chair said it might be timely to plan a half-day meeting in late September.

Mr. Scholl said that sounds great. They'll take a look at what the board wants to dive into, possibly including the threat information section, the Cyber Safety Review Board section, and the federal security improvements section.

- The Chair said that at some point it might be useful to hear from an agency or two that have implemented the measures required in the EO. Maybe at a meeting in 2022.
- Ms. Miller said that while all aspects of the EO apply to national security systems, the order makes a subtle distinction between NSS and everything else. Even in the discussions during the meeting you could see that separation. At some point we have to convey the message the NSS is not exempt from this. Given the push to modernize legacy systems, we need to consider everything discussed, including SBOM and supply chain security.

  Ms. Fitzgerald-McKay said she was surprised that Ms. Guttman decided in the critical software definition to treat NSS as the purview of Section 9. They had asked her to include it. There needs to be a comprehensive requirement for NSA procurements in NSS and otherwise. The distinction is going to cause problems down the road.

  Ms. Miller said she agrees.

  The Chair asked if it would be worth getting a brief update about the NSS and civil systems interface.

  Ms. Fitzgerald-McKay said she and Matt can find the right person.

  Ms. Miller said that would respond to her concerns.
- The Chair asked about the suggestion from Mr. Groman to re-invigorate the letter ISPAB sent in December regarding resources for privacy initiatives. He asked if the board was comfortable with the idea of trying to elevate that issue again and said he and Mr. Groman could get a draft together offline.

  Mr. Gattoni said it makes sense to re-send the letter, given that it was sent at a time of transition.

  The Chair asked if there were any objections. Hearing none, he said he would work with Mr. Groman to re-send the letter.

The Chair thanked Mr. Scholl and Mr. Stine for putting together a good meeting.

Mr. Scholl said NIST is not hosting in-person conferences through October. The board's interim meeting in September will be a one-day, virtual event. They will explore WebEx and Zoom and potential video conference platform alternatives. They may or may not be back in person for the December meeting.

Mr. Stine said he appreciates the Board's time and feedback.

The Chair adjourned the meeting at 3:10 p.m. ET.

ISPAB – June 23 and 24, 2021

Last Name	First Name	Affiliation
Board Members		
Baker	Brett	Nuclear Regulatory Commission
Fitzgerald-McKay	Jessica	NSA
Gattoni	Brian	DHS
Groman	Marc	Privacy Consulting
Hallawell	Arabella	NETSCOUT SYSTEMS
Lipner	Steve	SAFECode (Board Chair)
Maughan	Doug	NSF
Miller	Essye	Executive Business Management (EBM), LLC
Venables	Philip	Google
NIST Staff		
Brewer	Jeff	NIST
Scholl	Matt	NIST
St. Pierre	Jim	NIST
Stine	Kevin	NIST
Tabassi	Elham	NIST
Kerman	Sara	NIST
Carlson	Caron	HII
Salisbury	Warren	HII
McConnell	Andy	HII
Lurie	Kirk	HII
Speakers		
Neuberger	Anne	NSC
Seymour	Sezaneh	NSC (Anne Neuberger's Contact)
Greene	Jeff	NSC
Gingrich	Mary	NSC (support staff for Anne Neuberger)
DeRusha	Chris	OMB
Bray	Denise	OMB (Chris DeRusha's Contact)
Boyens	Jon	NIST
Friedman	Allan	NTIA
Mourtos	Harry	DHS
Black	Paul	NIST
Guttman	Barbara	NIST
Megas	Katerina	NIST
Merkel	Warren	NIST
Registered Attendees		
Cohen	Dylan	House of Representatives
Doubleday	Justin	Federal News Network
Eliot	Daniel	NCCoE
Estep	Steven	ICBA
Farooqui	Aly	IBM Cloud
Feldman	Harriet	ASRC Federal
Friedman	Sara	Inside Cybersecurity
Gaffey	Roger	IBM Corp
Geller	Eric	Politico
Haria	Alkesh	IBM
Heckman	Jory	Federal News Network
Heyman	Mat	NIST
Huffman	Robert	Covington & Burling LLP
Ignaszewski	Katie	IBM
Jackson	Caryn	The JEC Group, LLC
Jasmin-Benoit	Jonathan	Embassy of Canada

Kerben	Jason	Department of State
Kerman	Sara	NIST
Mazmanian	Adam	1105 Media Inc.
Moussouris	Katie	Luta Security
Nekkalapudi	Krishna	Lumen (formerly branded CenturyLink)
Pascoe	Cherilyn	US Senate Commerce Committee
Peterson	Ross	Cognizant Technology Solutions
Popowycz	Alexander	Hedera Hashgraph
Quillin	Tom	Intel
Quinn	Sean	IBM
Riaz	Asif	IBM
Riotta	Chris	1105 Media Inc.
Roberts	Taylor	Intel Corporation
Rogers	Susan	FS-ISAC
Rosberg	Stacy	Raytheon Technologies
Ross	Renault	RNSC Technology
Sakelakos	Sophia	Luta Security
Schroeder	Katherine	NIST
Sokol	Annie	NIST - Information Technology Laboratory
Souppaya	Murugiah	NIST - Information Technology Laboratory
Steib	Cara	LACR/NSA
Straight	Robert	IBM
Takamura	Eduardo	NIST
Throneberry	Saundra	Lockheed Martin
Tupitza	Charlie	Americas SBDC
Tworek	William	IBM
Weinberger	Peter	Google Inc
Wiener	Jake	Electronic Privacy Information Center (EPIC)
Williquette	Joel	ICBA
Wood	Jennifer	Luta Security
Yaniv	Orlie	Gigamon
Young	John	Veterans Health Administration