

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

March 9 - 10, 2022

Virtual Meeting Platform: BlueJeans

Board Members

Steve Lipner, SAFECode, Chair, ISPAB
Dr. Brett Baker, NARA
Giulia Fanti, Carnegie Mellon University
Jessica Fitzgerald-McKay, NSA
Brian Gattoni, DHS
Marc Groman, Groman Consulting
Arabella Hallawell, WhiteSource
Douglas Maughan, NSF
Essye Miller, Executive Business Management (EBM)
Katie Moussouris, Luta Security
Phil Venables, Google Cloud

Board Secretariat and NIST Staff

Matthew Scholl, NIST
Jeff Brewer, NIST
Charles H. Romine, NIST
Kevin Stine, NIST
Diana Proud-Madruga, Exeter Government Services
LLC

Wednesday, March 9, 2022

Welcome and Opening Remarks

Steve Lipner, Chair, ISPAB, Executive Director, SAFECode

- The Chair opened the meeting at 10:03 a.m. ET and welcomed everyone to the call.
- Reviewed the agenda
- Stated that, while the board provides formal input to the agencies with board letters, the members' comments and questions during the sessions with speakers also add value.
- For the visitors, he covered Federal Advisory Committee Act (FACA) committee rules including rules for asking questions.

Board Member Introductions and Updates

- **Douglas Maughan, National Science Foundation (NSF)**
 - Currently running a program called the **Convergence Accelerator**.
 - The idea there is we're not funding basic research, we're consumers of basic research and our job is to take technologies and ideas towards commercialization,
 - It's a 3-year-old program,
 - It's not just a cybersecurity focused accelerator. Just released a topic on a 5G security in partnership with the Department of Defense and getting ready to release topics in the areas of technologies for persons with disabilities, sustainable materials, and food and nutrition security
 - In addition to grants, we also do broad agency announcements to try to get industry and nonprofits to come and work with NSF
- **Arabella Hallawell, WhiteSource**

-
- Based in California
 - I've had a pretty long career on the cybersecurity side
 - A decade with Gartner as one of the first information security practice team members
 - Then with the Oracle vendor side and worked with a variety of vendors.
 - Now with WhiteSource that focuses on helping organizations fix open-source security issues and application security issues.
 - Interested in figuring out progress and implementation to help organizations struggling with application security issues around open source,
 - I'm interested in how we're helping governments and organizations with best practices and to become ready and resilient in the face of possible attacks?
 - Also interested in supply chain security as I think this is still an issue
 - **Dr. Brett Baker, National Archives and Records Administration (NARA)**
 - Changes and challenges in the IG community and with FISMA:
 - **Smaller time window:**
 - Time frame is usually from March/April through October to do our testing and come up with a reasonable conclusion on whether security is in good shape for an agency.
 - Now our cyber-scape reporting needs to be posted in July, so we're getting less time to look at the site's cybersecurity and ID security position.
 - **Metrics:**
 - We don't have the core metrics nailed down for the July report
 - Still waiting on final guidance.
 - **Resources:**
 - Frequently use contractors so our contracts have to be adjusted to accommodate the changes
 - **Testing:**
 - Testing, including PEN testing and vulnerability scanning, allows us to understand what is coming into the agency
 - Lack of core metrics and the shorter timeframe presents a challenge to completing testing the 75 shops that do this in the IG community.
 - Next year, if we're going to be aiming at July, we'll just start sooner.
 - **Essye Miller, Executive Business Management (EBM)**
 - Approaching my second year of retirement but using that time to contribute where I can on the advisory and consulting side
 - US Cyber Challenge and Cyber Start America
 - These are two major nonprofit programs to identify cyber talent across the country, particularly in underrepresented communities.
 - Working with the Center for Internet Security and National Cyber Scholarship Foundation to make sure we get word out about those programs.
 - **Phil Venables, Google Cloud**
 - SW Supply chain
 - Heavily focused on software supply chain security with advancing and putting it in the community
 - White House Open-Source Security
 - We were a big part of the White House's open-source security summit
 - Focused on driving the work with the Open-Source Security Foundation to improve all the tooling and to drive investment in ensuring the key open-source projects are properly secured and managed.

-
- Advancing the notion that physical separation can be replaced by cryptographic controls
 - We're talking about this in the context of FedRAMP
 - This will help improve security and give government more flexibility in adopting services formerly restricted by physical isolation requirements
 - Implementation of post-quantum cryptography
 - We're trialing a lot of the NIST candidate algorithms in big parts of our infrastructure
 - Starting work with some corporations, helping them with their crypto agility planning
 - Working with standards
 - We've been heavily engaged with a lot of the other standards bodies
 - For example, recently working with the 6G standards group to make sure the 6G standards are crypto agile.
 - **Brian Gattoni, Department of Homeland Security (DHS)**
 - Chief Technology Officer of Cybersecurity Infrastructure Security Agency (CISA)
 - Future Technologies:
 - Looks at the future technology opportunities and how they influence CISA's mission, either as adopters or identifying how we remain good partners with stakeholders adopting the technologies.
 - Managing the changes to risk for adopting those new technologies,
 - Keeping an eye on our adversaries' potential use of that same technology,
 - Doing move-countermove analysis to optimize our position to work with our stakeholders, protect national interests, and deny our adversaries their goals.
 - Shields Up Campaign:
 - Working with critical infrastructure to understand how important it is to be vigilant at this time with political tensions,
 - To be ready to work as one partnership to ensure preparedness and domestic response here at the homeland, and
 - Make sure that we're safe from cyberattacks from abroad
 - Standing up our joint cybersecurity defense collective, building relationships, sharing information in every direction that's helpful to parties, as well as participating in technology conversations.
 - **Giulia Fanti, Carnegie Mellon University**
 - Assistant professor at Carnegie Mellon in electrical and computer engineering
 - Studies the privacy and security of distributed systems and data sharing
 - I am particularly interested in the upcoming EO on digital assets.
 - Works on blockchains and distributed ledgers and understanding how that will relate to any potential efforts to build central bank digital currencies.
 - **Jessica Fitzgerald-McKay, National Security Agency (NSA)**
 - I'm the lead for NSA Center for Cyber Security Standards (CCSS)
 - CCSS has purview over NSA standards coordinating and engagement, ensuring standards exist for a National Security System
 - Our main technology focus areas are:
 - Insecure protocols particularly preparing for post quantum transition
 - 5G security, with a view towards what's happening in 6G or next G
 - Cloud security standards including traditional network security standards
 - Since our last meeting, one focus area has been on coordinating international standards with other allied governments and positions in standards,

-
- We're seeing a lot of influence by foreign governments that don't align with the US government (USG) position on letting commercial industry lead in these standards engagements, so we've been coordinating between ourselves, within the USG, and with allied governments, particularly on 5G standards, in understanding where our norms are not being adopted into the standard bodies and coming up with a strategy for how to deal with that.
 - **Marc Groman, Groman Consulting**
 - Served as a senior adviser for privacy in the Obama White House for his second term
 - Prior to that, served as Privacy Counsel on the House Energy and Commerce Committee
 - First Chief Privacy Officer for the Federal Trade Commission
 - I am an attorney so that brings a whole separate set of issues to our discussions
 - Teaches incident response at Georgetown law school
 - Consults with organizations and companies on data protection and international data flows
 - Serves on the Privacy and Civil Liberties Oversight Board at NSA
 - Concerned about how we effectively implement and execute our intelligence mission in a way that works with privacy and civil liberties.
 - Recent events have put pressure on those issues.
 - **Katie Moussouris, Luta Security**
 - Also based on the West Coast.
 - Serves on three boards or councils for the federal government:
 - ISPAB
 - ISTAC for Commerce
 - Asked to join because of her previous role in helping the US State Department led effort to renegotiate our arrangement around export control of intrusion software and intrusion software technology
 - The new DHS Cyber Safety Review Board (CSRB)
 - Brand new board modeled after the National Transportation Safety Board (NTSB)
 - Per the executive order, we have less than 90 days to produce a report that is examining the incident and the disclosure and all the events around log4j
 - Questions about Vulnerability Lists
 - There's been disparate guidance coming from different federal agencies on dealing with vulnerabilities
 - CISA has started a living list of vulnerabilities that are under active exploitation, and they seem to be adding to this list
 - Question – How sustainable is this?
 - we've had lists of vulnerabilities before and not gotten a straight answer on how to deal with the eventual fatigue
 - I'm interested in what this board and others think about that living list
 - Why are some vulnerabilities (the ones that are more recent) given a two-week deadline by CISA to apply a fix and then others (some as old as a decade or coming up on a decade) given six months to patch?
 - <https://www.ftc.gov/news-events/blogs/techftc/2022/01/ftc-warns-companies-remediate-log4j-security-vulnerability>
 - If we want private companies to follow CISA's guidance, the deadlines need more congruity and need to make sense.
 - **Steve Lipner, SAFECode, Chair, ISPAB**
 - Executive director of SAFECode, a nonprofit focused on software security

-
- Spending time providing feedback to NIST on their guidance on the executive order and participating in assorted workshops and forums that they've hosted.
 - We are a founding member of Nonprofit Cyber, an informal alliance of nonprofit organizations focused on providing advice, tools, and assistance in cyber security for the community at large.
 - Wrapping up role as chair of a National Academies Committee on the Future of Encryption

ITL Update

Charles H. Romine, Director, ITL, NIST

- **Purpose of ITL: Cultivating trust in IT metrology**
 - Cultivating trust in information technology and metrology.
 - Trust allows ITL to work closely with the private sector and academia in a partnership model
 - **Quality People:**
 - Charles Romine said, “I’m fiercely proud of the quality of people that we have in ITL. They do an amazing job. They change the world every day...”
- **From Innovation to Adoption**
 - ITL needs to maintain the balance between fundamental research and adoption of their work.
 - Fundamental research drives applied research and their standards
 - Activities that drive adoption ensure ITL has impact
- **NIST Leadership**
 - Dr. Laurie Locascio has been nominated for the Under Secretary of Commerce for Standards and Technology, NIST Director.
 - She was a longstanding member of NIST before she retired several years ago to take the vice president for research position at the University of Maryland College Park in Baltimore.
 - The Commerce Committee has referred her nomination to the full Senate and hopefully NIST will have a permanent new director soon.
 - Thanks to Jim Olthoff who is the current acting director of NIST and has been executing that function brilliantly.
- **The National Academy of Science, Engineering and Medicine (NASEM) Review**
 - NASEM conducts reviews of the various laboratories at NIST on a rotating basis
 - ITL was reviewed last fiscal year, about eight or nine months ago.
 - Because the scope of ITL is so large, NASEM reviews half of the laboratory each cycle so that they could do a deeper dive.
 - They were excited about the work that we were doing in these divisions that they reviewed
 - Recommendations:
 - Focus on recruitment, retention, and development of staff.
 - Many staff are either nearing or have crossed the retirement age
 - ITL needs to replenish the ranks of folks to maintain this extraordinary asset.
 - Democratize access to guidance documents
 - ITL guidance documents that are enormously beneficial and very technically detailed
 - Need to come up with a way to democratize access to our guidance documents and make them a little more digestible.
 - Maybe a bigger emphasis on some plain language or perhaps companion documents that do the job of explicating some of the details.
 - Would like to reach out to the board here for some advice on how we can best accomplish those things.

- **Noteworthy Mentions**

- Election Security
 - Recently we had some significant advancements in our efforts in election security.
 - Example: the release of the voluntary voting system guidelines 2.0.
- National AI Research Resource Task Force
 - This is a collection of national leaders in AI
 - The lead for our artificial intelligence research program on trustworthy AI, Elham Tabassi, is now serving on this task force
- Internet of Things Advisory Committee
 - ITL has stood up an Internet of Things federal working group and an associated advisory committee for the Internet of Things.
 - A federal advisory committee is under development in partnership with the Communications Technology Laboratory at NIST.
- Genomic Data Cybersecurity and Privacy
 - ITL was asked by Congress to initiate a genomic data cyber security and privacy program
 - Doing this in partnership with the NIST Material Measurement Laboratory
 - Activity also at the National Cybersecurity Center of Excellence
- Updated Federal PIV Standard
 - ITL updated the federal PIV standard
 - Wanted to add flexibility and permit things beyond physical ID cards to include electronic tokens and one-time passwords
- Trade and Technology Council
 - Heavily involved in the areas of standards and particularly artificial intelligence
 - This is in partnership with the International Trade Administration in the Department of Commerce
 - Meet regularly with the European Union counterparts
 - Working on things such as:
 - An early warning mechanism for international standards between the US and the EU
 - Ongoing cooperation in artificial intelligence
- Quadrilateral Security Dialogue Standards Sub-Group (Quad)
 - Have a standards subgroup co-led by NIST and the Department of State
 - Reported out on the first meeting of the artificial intelligence contact group and reached an agreement to establish a similar group on advanced communications
 - Is a partnership for strategic security dialogue among the US, India, Japan, and Australia
 - Also collaborating with NIST standards coordination office

- **Cybersecurity and Privacy**

- Quantum Resistant Encryption Algorithms
 - In the final stages of announcing our selections
- Cybersecurity Labeling for Consumers: IoT and Software per EO 14028
 - There is a lot of work under the Executive Order on cybersecurity labeling for consumers of both IoT and software
- Updated the Secure Software Development Framework per EO 14028
- Cyber Security Framework and Supply Chain RFI on Feb 22, 2022
 - Announced our intention to update the cyber security framework
 - Will be many upcoming workshops
 - Working on supply chain issues and supply chain security

-
- Undertook a strategic planning exercise for our entire cybersecurity program and identified some key areas
 - Suggest this as a topic for a future meeting
 - **Artificial Intelligence**
 - Goal is cultivating trust in the design, development, use, and governance of AI technologies and systems.
 - Development of AI Risk Management
 - Developing an AI risk management framework
 - Concern that if we don't address the trustworthiness and responsible use of AI, we could see a backlash or a lack of adoption
 - Establishing National AI Advisory Committee
 - Took the lead on establishing the National AI Advisory Committee
 - Preparing to announce the full committee members
 - AI Standards and Evaluation
 - Heavily engaged in AI standards and evaluation
 - Elham Tabassi is the federal government AI standards lead
 - **Physics World 2021 Breakthrough of the Year**
 - More on ITL's role in cultivating trust in metrology using artificial intelligence to improve metrology.
 - Physics World in 2021 announced the number one breakthrough of the year was the quantum entanglement paper from a team at NIST.
 - 5 of the 12 co-authors came from the Applied and Computational Mathematics Division in ITL.
 - Brilliant breakthrough that shows entangling of macroscopic entities rather than just entangling of qubits or quantum bits.
 - **Awards**
 - Dr. Romine shared a slide with many awards that people in ITL have received within the last year illustrating the breadth, scope, and talent in ITL.
 - **ITL Milestones**
 - In 2022, celebrating:
 - 75 years of applied mathematics and statistics
 - 50 years of Cybersecurity research
 - In 2023, ITL will be celebrating 60 years of Biometrics research
 - **Discussion**
 - Essye Miller asked if ITL plans to give the board a bit more insight on what you're doing with the cyber security framework.
 - Kevin Stine replied that they are planning to talk in a little bit more depth about that tomorrow. He mentioned they issued an RFI within the last couple of weeks that's open through end of April. They want to encourage and amplify awareness of that and encourage feedback from this community to help inform what the next steps will look like.
 - Essye Miller also asked the same question for the AI framework and indicated that may be worth a deep dive with the with the group at some point.
 - The Chair asked for other questions and added the same request for an update about the supply chain security strategic plan.

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

Office of the National Cyber Director Introduction and Update

Chris Inglis, Director, Office of National Cyber Director (ONCD)

What is the Office of the National Cyber Director (ONCD)?

- It's the newest agency within the federal government
- Typically designated as an office but legally an agency within the Executive Office of the President
- Created January 2021 by the National Defense Authorization Act of 2021,
 - Inspired by the [Cyberspace] Solarium Commission that had made some recommendations on how the US could make its cyber strategy more resilient and robust.
- Chris Inglis was nominated to fill the job in April 2021 and confirmed in June 2021
- Funding showed up November 2021
- Staffing is projected to be between 75 and 85 people. It is currently at 30.
- Two documents:
 - Statement of intent, written October 2021, essentially says the job of the office of the national cyber director is to:
 - Add context, coherence, to drive public-private collaboration, and to add leverage to the existing parts in this space.
 - Make it such that the sum of the parts exceeds its whole
 - We're going to focus on four different areas
 - Coherence – both within the federal enterprise and as the federal enterprise engages the private sector from the federal enterprise
 - Understanding who is accountable for what activities under what circumstances
 - Being proactive about pushing those resources to the private sector which increasingly is the supported organization in the realm of cybersecurity
 - Driving collaboration – private-public collaboration, not just collaboration with any given sector. The only viable way forward is to affect a collaboration where the transgressor has to beat all of us to beat one of us.
 - Future Resilience – we're good at responding to crises but that's not a strategy that will work at scale.
 - Need to build in resilient cyberspace technology, roles, responsibilities, and people so we're less likely to encounter these events.
 - Performance Assessment – In the statute, Congress levied an account for cyber dollars, but we'd like to broaden that remit to have assessments of:
 - Do we have the right roles and responsibilities?
 - Are the cyber dollars expended with the right time, attention, and priorities?
 - If they're not sufficient, how can they be made more sufficient?
 - How can we optimize the resources that we bring to bear in this space?
 - How can we make sure that we have the right people strategy beyond those folks who have cyber or IT in their job titles?

What are some of the connections ONCD has to other entities already in this space?

- Those four functions are already being executed by many others within the federal government:
 - CISA, at the Department of Homeland Security, is our “on the field quarterback”
 - NIST
 - Department of Commerce
 - Other activities within the Department of Homeland security, and

-
- sector risk management agencies
 - Department of Energy, Department of Defense, Department of Treasury, and some others who deal very specifically with their respective sectors
 - ONCD's job is to ensure each of them understands what their role is and is connected to some larger purpose, and we create a coherent result in the application of that talent without duplicating. That they complement one another.

Priorities

- Near-term
 - Focused on doctrine and people issues, getting the roles and responsibilities right to achieve unity of effort and purpose
 - Within the federal government, we're working our way across all the chief information security officers
 - The May 2021 EO dictated much on how we build in the attributes of that architecture
 - Ensure unity of effort and purpose in understanding what's happening on those networks and how we defend those networks
 - Understanding what the sector risk management agencies do. How do they do those things together?
 - How CISA can benefit from that so the government learns something once and it can quickly apply that for the benefit of the private sector.
 - Plus, a range of other activities:
 - Tabletop exercises
 - Looking at budgets
 - Preparing ourselves to create mid to long term resilience
- Mid-term
 - Start work on software and people resilience so that we're making the investments that, in 1 – 3 years, results in inherently more resilient software, hardware, and supply chains.
 - Open-source software as a case in point: who knew that Log4j would have the ubiquitous threat of something hard to find that was replicated far and wide
 - People resilience - create an upskilling strategy for all of those in cyberspace
 - Ensure that, from the earliest age, we make them cyber aware.
 - Address the 500,000 jobs that have the word cyber or IT that are not filled now?
 - Reexamine everything from how we specify the requirements jobs, how we educate and train the people for those jobs and do that at scale with diversity in mind to appeal to the broadest possible audience.
- Long-term
 - Ensure cyber worthy investments for anything dependent on digital infrastructure
 - Infrastructure, Investment and JOBS Act (IIJA) – one billion of the 1.3 trillion dollars is focused on cyber but all \$1.3 trillion will be investments in cyberspace dependent things.
 - Push the doctrine that investment in the resilience and the robustness of the underlying digital infrastructure must be cyber aware and cyber ready to have “a rising tide lifts all boats” effect on how people think about cyber.

Discussion:

Metrics:

-
- Katie Moussouris asked what are the metrics going into their assessment to determine the need for additional resources and where?
 - Chris Inglis responded that ONCD could use some assistance in that regard. The DoD has done good work on scorecards, defining objective metrics on sufficiency of the underlying technology attributes. But it's only a leading indicator, not proof of resilience.
 - He added that other questions to consider are, how well defended is that enterprise? Do the analytics work? Do you have the right people? Do you have the right doctrine so that you have confidence you'll catch something in the incipient phase? We need to figure out how to measure that as well. There are some emerging analytics that we could use on that.
 - Automation is going to be key.
 - The ultimate metric is how to quantitatively say that we've progressed. That absolute metric is elusive. We're trying to account for the dollars, the doctrine, and the people skills that we have. That'll be raw data. We will then go to the point where we count those leading indicators. Then we have to figure out how to account for performance and sufficiency as a byproduct of that.
 - Katie Moussouris replied that she does have ideas. The mean time to repair bugs is a useful metric. Not a lot of organizations have this because they're not tracking when they became aware versus when they repaired it.

Relationship between ONCD, OMB, Federal CIO, GDM, and CISA

- Marc Groman asked two questions: 1) how is ONCD working with OMB, the federal CIO, and the Deputy Director for Management (DDM)? Where is there overlap? 2) should we be more thoughtful about data retention in the government? If we don't have it, we can't lose it, it can't be stolen, and more.
- Chris Inglis replied in response to the first question:
 - Relationship with OMB: OMB has a significant responsibility in cyber policy and cyber operations.
 - All line CISOs in the federal enterprise report to the federal CISO at OMB
 - OMB had the authority to issue directives that bear on cyber and have control of the dollars that are applicable for broad missions and operations as well as cyber.
 - ONCD and OMB have agreed to dual hat the federal CISO, Chris DeRusha, as the Deputy National Cyber Director for Federal Cybersecurity
 - ONCD would give OMB money and ONCDs authorities and influence to achieve a unity of effort and purpose between the two organizations.
 - There are still lots of requirements that come from within agencies, from inspectors general, CISA, and OMB to align and harmonize but we're joined up in that regard.
 - Relationship with CISA: Jen Easterly, Director of CISA, is the self-described "quarterback" and Chris Inglis is the "coach". CISA is on the front lines and ONCD's job is to ensure their connectivity to the sector risk management agencies and, when necessary, to achieve some degree of advocacy and championship from the White House to ensure their further success.
 - Relationship with National Security Council: Anne Neuberger, the Deputy National Security Advisor for Cyber, ensures we use instruments of power outside of cyberspace such as military, diplomatic intelligence, and legal instruments of powers, to bring about conditions that we prefer inside of cyberspace. The National Security Council uses all those instruments to bring about the necessary conditions inside multiple domains, cyber is one of those domains.
- ONCD's job is largely inside of cyberspace, working on giving unity of effort and purpose to CISOs, connecting private and public sector entities that own and operate territory within cyberspace so that

we achieve the right result. Those two things can and do complement one another but it's something that's a work in progress

- **Data Retention:** Data retention is not on the front burner but we're thinking about it. As we build our architectures, we need to ensure we're using them for the appropriate purposes. We need to think about our risks so we can double down on defending those things and mitigating the threats and risks to that data.
 - Congress attached intrusion reporting legislation to the omnibus bill requiring critical functions within our society that had a cyber intrusion to report to the federal government, probably to DHS, so the federal government can use that information to characterize and respond to the defense of the private sector during the cyber intrusion.

Compliance Culture

- Essye Miller asked if there has been any discussion on how we move from just looking at compliance to helping CIOs and CISOs focus on more relevant data.
- Chris Inglis brought up the recently published Zero Trust Architecture Strategy which moves us away from compliance toward something that says, “do I actually know how these systems are being used?” If we understand how these systems are being used, we can have confidence that they're less likely to have an event because we've built resilience in by design.
- There's now a billion dollars in the technology modernization fund specifically to invest in features and attributes needed to achieve zero trust architecture
- Essye Miller asked if this would impact FISMA and FITARA?
- Chris Inglis responded there's a FISMA modernization component of cyber legislation that was bound with a cloud architecture security bill and the intrusion reporting bill. They pulled the intrusion reporting bill out and attached it to the omnibus bill. This means FISMA still has to be dealt with. The last update to FISMA was in 2014, before we understood that the right way to get resilience and robustness is not through compliance or scripting but through the attributes.

Cyber Workforce and Education

- The Chair mentioned asked if Mr. Inglis had any thoughts regarding workforce and education and how to make that coherent. There are many different agencies in the federal government trying to do things about workforce and education but, from outside government, it looks somewhat overlapped and convoluted. For example: open-source where the issue is getting people who do something other than cybersecurity to do security.
- Chris Inglis replied we're probably in agreement on this. Transgressors and aggressors in cyberspace look at three dimensions: technology, people, and doctrine. Typically, transgressors take advantage of this in reverse order:
 - If there's no one defending an enterprise of some consequence, then just take advantage of that doctrine,
 - If doctrine is shored up and there is somebody who thinks they're defending it but they're not, then try to find a weak link in one of the front-line people of that system. If that fails,
 - Go for the technology (zero-day vulnerabilities).
- We have to fix all three of those dimensions, but addressing doctrine and people is at the forefront
- CISA, NIST, and NICE have some good work in this regard. NSF and Department of Education have a part to play also.
- Need a strategy:
 - Where we reconsider what cyberspace is

-
- That says the doctrine and people are as important as technology
 - Will have a summit at the White House, probably at the end of April on how to account for each of the pieces, understanding how to better connect them to the whole, and understanding what's missing in that fabric so we can cause that to come into being. We welcome your participation in some way shape or form to inform how we set that up and follow through on that.

Effect of Current Geopolitical Events

- Jessica Fitzgerald-McKay asked how current geopolitical events might shape your mission? Is there an aspect to what we're seeing in the world right now that might inform priorities?
- Chris Inglis replied that the reality is we've got a lot of deficits, whether it's investment in technology or doctrinal deficits, we don't have enough people who have the word cyber right in their job title.
- We've been working hard to invest in the architectures. Things like multifactor authentication and segmentation. But this is a stunningly good opportunity to determine what to change on an enduring basis going forward.
- If you want tactical warning on what's happening at some moment, you can only learn that together. Typically, we overestimate what the government knows, underestimate what the private sector knows, and ignore what we can know together.
- Two activities that we've undertaken are:
 - The joint cyber defense collaborative
 - Established by law in the same act that created ONCD.
 - Offers a physical place with virtual extensions where we can co-discover and co-mitigate threats on the fly.
 - Still needs work but it's making a difference in discovering things together we can't discover alone so we can rapidly deploy that knowledge and collaborate in the defense of this space.
 - Working with the sector risk management agencies like Department of Treasury, with bank leadership, and CISA to share what we know.
 - This strategic learning allows us to strap together the various parties who have bits and pieces about what's happening so we can learn what's happening and deal with that together, protecting privacy and proprietary interest all the while.

The Chair mentioned that the board both provides feedback in the form of the discussions and through letters to the various agencies in terms of what we agree the government ought to be doing to try to address things. He let Mr. Inglis know the board would be happy to look at and provide feedback on specific questions. The board is also interested in hearing from his office about things that we ought to be paying attention to or looking at.

Chris Inglis summarized two transformative opportunities going forward: 1) to double down on resilience by design and resilience in technology and the doctrine, meaning roles, responsibilities, and the people components and 2) to affect a collective defense, a collaboration where we can discover and address things together in ways we cannot with any amount of resource alone.

Mr. Inglis said that input on either the sufficiency or the implementation of those components is welcomed.

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

National Security Council Efforts on Open-Source Software Security

Amit Mital, Senior Director for Cybersecurity Strategy and Policy, National Security Council

White House Meeting on Software Security (<https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/13/readout-of-white-house-meeting-on-software-security/>)

- There was a meeting on January 13, 2022, between government and private sector stakeholders to discuss initiatives and approaches to improve the security of open source software.
- Approach has three lines of effort:
 - Modernizing cyber defense for critical infrastructure
 - Returning to a more active role internationally and
 - Building cyber security into the infrastructure of tomorrow
- One idea was to use the purchasing power of the government to ensure that we could bring real change in improving public security.
 - EO requires government vendors to meet certain federal security guidance.
 - Our belief is that would propagate through all software because the government is such a big purchaser then the private sector will follow suit, which has worked.
 - We've also invested heavily shoring up our cybersecurity defenses and critical infrastructure
- Open-Source Software Security
 - Open-source is everywhere
 - Economics, national security, cybersecurity, and privacy all depend on whether some open-source library that 99.9% of Americans have never heard of was developed in a secure way
 - Example: Log4j
 - Suddenly this obscure implementation of a noncritical piece of software had the ability to impact hundreds of millions of people and the entire industry had to scramble to address
 - The status quo is untenable
 - The government can play a part but ultimately the solution has to be industry driven
 - White House meeting on how to drive rapid security identified several folks, including higher education training resources.
 - What emerged was a need for driving additional automation across the entire lifecycle of software development, deployment, testing, monitoring, and updating
 - Automation
 - Automation is a key concept because in cybersecurity one of the core challenges we're facing is capacity
 - There's a giant shortage of people with the requisite skill sets
 - when you have a process that depends on people implementing actions and taking remediation several things can happen:
 - You can have errors in configuration and deployment
 - Higher latency in response
 - Automation leads to efficiency, scale, repeatability, predictability, and shorter response
 - Automation of course is not the entire answer
 - Risk of false positives
- Discussions focused on three topics:
 - Topic 1: Preventing security defects and vulnerabilities in code and open-source packages
 - Software Development Process
 - How do we prevent defects and vulnerabilities from happening?
 - How do we incent developers to improve the quality of the software?
 - Give them tools to automate that process and give them tools to detect vulnerabilities in the software easily and quickly

-
- Use of software bill of materials (SBOM) seems to be one way in which you can track both the provenance of the software and what is in the software
 - Skills and Criticality Management
 - How do you manage the skills and criticality?
 - How do you find a more standard way of tracking what the skills are, what the competencies are to match those skills and competencies with their requirements?
 - We need a standardized way of doing change management, having a standardized way of increasing transparency but also improving the modes of tracking changes in codes, bugs fixes, deployments, updates, and security.
 - Making sure the build system is robust to reduce introducing vulnerabilities that seem like legitimate code
 - Securing Distribution
 - Need to ensure open-source software package warehouses are secure
 - Secure open-source distribution mechanisms
 - Increasing Community Participation
 - Need to figure out ways to incent people to participate in the full cycle of open-source software, not just be consumers
 - Don't expect everyone to write code but could participate by reporting bugs, making suggestions of improvements in the user interface, etc.
 - Developer Education and Capacity
 - There's a shortage of developers with the right level of training on security awareness
 - Need to find ways to make security a glamorous feature
 - Topic 2: Improving the Process for Detecting and Fixing Vulnerabilities
 - Focus on quickly and efficiently finding defects, responding, and distributing fixes
 - Identify how to prioritize critical projects on a couple of dimensions
 - The system's code or networking code by nature is critical for the operation of the system
 - Breadth of use. The code itself could be relatively benign but so widely used, with thousands of people depending on it, making it critical.
 - Once critical projects are identified, enabling scalable and sustainable maintenance.
 - ~ 80% of the most used packages are maintained and developed by two or fewer developers and often those people are doing it as a side job or hobby.
 - Need to complement and enhance these people, give them more resources and capabilities to better test the code, find the vulnerabilities, fix the bugs, and have mechanisms of distributing the fixes on a wide basis.
 - Topic 3: How do we improve the response time for distributing and implementing fixes?
 - Example: Log4j
 - Apache foundation released fixes within a couple of weeks, but it's estimated over 30% of the affected systems have still not been patched
 - This points to a couple of things:
 - Our ability to find which systems are vulnerable or dependent on a particular package is very primitive
 - Many organizations don't have the ability to respond.
 - For example, Amazon.com had to update 1.1 million servers in 9 hours. They were able to pull that off, but a medium or small website operator may not have the knowledge or resources to know if they even need to apply the fix.

-
- Use of a software bill of materials (SBOM) could help in identifying and fixing vulnerabilities, especially if you had an automated way of doing so.
 - Create a central repository and an automated response repository that showed all the packages that were deployed at all sites. The challenge is it goes against the libertarian ethos of many of the open-source proponents.
 - Link to the readout of the White House meeting: <https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/13/readout-of-white-house-meeting-on-software-security/>
 - Open-Source Security Foundation (Open SSF or OSSF)
 - Has about 300 or 400 members. The founding members were Google and Microsoft
 - OSSF has taken the lead in coordinating the response across private industry
 - About three weeks ago they announced a project called Alpha Omega which identifies the high priority open-source projects
 - They started with a \$5 million grant from Microsoft and Google are busy identifying and prioritizing the top 100 projects and identifying resources to secure the priority packages
 - They're working on another six or seven priorities such as finding ways to promote SBOM deployment and usage

Discussion

Government Engagement

- Phil Venables commented that there was a lot of positive reaction in the private sector to the Summit. He was wondering how much activity, post Summit, has Amit Mital seen in the federal government? Does he sense from the White House or, from the other direction, that CIOs and IT teams are going to get more engaged in things like the Open SSF?
- Amit Mital replied that the ONCD has taken the lead on bring all the agencies together. We need to:
 - Identify all the packages used in the Federal Government,
 - Identify which ones are critical and ensure SBOM deployment happens,
 - Improve responsiveness and deployment of fixes
- The government is working on a plan but nothing concrete yet.

Guidelines

- Arabella Hallawell asked if he has any timeline of guidelines for federal and commercial enterprises? What is his role?
- Amit Mital replied that with commercial software, there's an entity that is directly accountable. With open-source software, it's more nebulous. But telling a midsize or small company a whole bunch of technical stuff is not tenable. That's why we believe we need to go to the source and improve the security performance of the open-source so when it gets to the consumer of the software the security is fundamentally better. Expecting millions of people to suddenly take technical security actions is obviously not viable. We need to enhance security itself.

Economic Incentives

- Douglas Maughan asked with all we know about the problems with software, software coding, finding bugs, are there any good economic incentives that were a part of the activity?
- Amit Mital clarified that Mr. Maughan is referring to things like bug bounty programs and Mr. Maughan confirmed but added that those aren't "all that great."
- Amit Mital replied that, unfortunately, there's already a very functional market for cyber security vulnerabilities where the economic incentives are already extreme. If you find, for example, a

legitimate zero day in Chrome or Windows, that's a good seven figures. So, you really have to be careful about how you incentivize people, who you incentivize, and where you get these bugs.

- Douglas Maughan clarified that he was wondering if they were any good economic incentives identified, if anybody came up with anything better than what we have.
- The Chair commented that in his experience the key consideration is the willingness or commitment of the developers who write the code to get on board with the need to create secure code. Automation tools can make it easier to write secure code, define the mistakes and correct them, but doesn't replace the developer fixing the code.
- The Harvard Business School, supported by the Linux Foundation, published a report about developer motivations. Attitudes toward security were described as, "a mind numbingly bureaucratic, awful process that I don't want any part of."
 - How do we solve that problem? If the developers want to write secure code, that solves about 80% of your problem.
 - Amit Mital agreed and replied that large companies can mandate working on security. For open source there's no such mechanism.
 - The Chair commented that even at Microsoft we had to get their hearts and minds on board.
 - Amit Mital replied we need to create an incentive structure for developers where security is a tier one feature set as much as performance.

OpenSSF

- Giulia Fanti asked how Mr. Mital sees the role of the government versus industry in leading these efforts. Does he feel government could play a larger role in encouraging enforcement for these issues? Is there any talk of this coalition of companies putting financial resources in paying open-source developers? If not, what exactly is this coalition?
- Amit Mital replied that the role government can play is twofold:
 - Convene companies and bring them together
 - Did that at the Open-Source Summit.
 - Use the purchasing power of the government to require certain security standards be met by vendors selling to the government.
 - The Deputy National Security Advisor, Neuberger, provided an update and clarification that this requirement applies not just to commercial software, but also to web services and open-source software.
- Open SSF is off to a great start in finding and fixing these bugs and companies have been very generous and shown a lot of leadership in providing the initial funding.
- Phil Venables added that the companies and others involved in the Open SSF have been funding a lot and just pledged another 100 million dollars to fund Open SSF projects, in partnership with government, encouraging the big tech companies and the major enterprise consumers of open-source to step up. A lot have but there are still many companies getting all the benefit from open source without putting effort into being part of the community to fund or provide resources to help manage the security of these things.
- The Chair asked if OSSF or member companies have thoughts for detailing people, or a fraction of their time, to an open-source project to support getting secure development integrated?
- Phil Venables replied that some things going on in OSSF are to encourage the adoption of secure development practices, secure tooling, and adopting frameworks to reduce the toil of getting security right. Some critical projects started to shift to safer programming languages and frameworks away from some of the ones that are more vulnerability prone.

-
- Focused on things that will drive improvements in the open-source community such as the Open-Source maintenance crew contract, where large numbers of volunteers from major companies donate significant amounts of their time to join the maintenance teams on some of the open-source projects. We have a long way to go but it's improving.

Other Roles

- Katie Moussouris commented that there are distinct roles and distinct jobs that are not being focused on at all in some of the open-source efforts. Certain companies are providing support by donating the time of fully paid developers, but nobody seems to be providing the apparatus and the know-how to run these types of investigations. Those are distinct skills. Is the NSC is thinking about how to get those specialty skills?
- Ms. Moussouris then asked what ongoing role the White House summit groups are having in advancing the topics that he identified?
- Amit Mital replied that in the next few weeks we'll have some announcements and that he agrees it's not just a specialty skill set on security that needs to be improved.

The Chair recessed the meeting for a 10-minute break.

GAO Report, Federal Response to SolarWinds

Jennifer R. Franks, Director of Information Technology & Cybersecurity, U.S. Government Accountability Office (GAO)

Introduction

- Jennifer Franks is one of the Directors of the Information Technology and Cybersecurity team at GAO.
 - Her current roles include:
 - Leading the portfolio for federal cybersecurity and looking at agencies' Information Systems and how they secure data.
 - Leading the healthcare IT and cybersecurity portfolio (pandemic related response efforts and data protection privacy related engagement)
 - Directing the Center of Enhanced Cybersecurity which provides security, operational technical services for GAO as well as technical support for their cybersecurity related engagements.
 - She also teaches diversity, equity, inclusion, and accessibility courses for the industry.
- GAO is called a "congressional watchdog"
- Every two years GAO reports on federal government's operations that are vulnerable to waste, fraud, abuse, and mismanagement.

The GAO High-Risk List

- The High-risk list has served to identify and help resolve very serious weaknesses across the federal government that involve resources for people and money and provide critical services to the public.
- Since our program began, the government has taken some good steps to implement measures to reduce risks. In 2021 there was improvement for seven of the high-risk areas. However, five areas got worse.
- We issued a report last week that focuses on how an agency, or a high-risk list topic, can come off the list.

-
- Unfortunately, cybersecurity will not be taken off the high-risk list anytime soon because of the evolving threats and the expanding cyber landscape.
 - One of the emerging issues for 2021 was Health and Human Services (HHS) leadership and coordination efforts in public health emergencies. We're:
 - Taking measures to identify efforts that HHS needs to lead and coordinate this effort.
 - Looking at the lack of coordinated situational awareness during the pandemic
 - Looking at network capability models that force an ecosystem of systems to communicate at a near real time across the federal government agencies, and then state and local and territorial governments during public health emergencies

Ensuring the Cybersecurity of the Nation

- Cybersecurity was added to the High-Risk List in 1997
 - This was updated in 2003 with critical infrastructure concerns, 2015 with personally identifiable information, and 2018 with comprehensive national strategy and oversight.

Four Major Cybersecurity Challenge Areas

- Establishing a comprehensive cybersecurity strategy and performing effective oversight,
 - Focusing on the need for the federal government to develop and execute a comprehensive national strategy and provide effective oversight.
- Securing federal systems and information,
 - This is the challenge area she focuses on in this presentation
- Protecting the cyber critical infrastructure, and
- Protecting privacy and sensitive data.

Key Objectives

- Summarize the SolarWinds and Microsoft Exchange cybersecurity incidents
 - SolarWinds is a Texas based information technology company that provides information, network management and monitoring software to its clients.
 - At the time of our review, it had about 300,000 customers,
 - The SolarWinds company managed the Orion platform software and it's the Orion software that was compromised.
 - SolarWinds – What happened:
 - A threat actor compromised the network management software.
 - The attackers planted malicious code into the Orion code by inserting a backdoor into certain software patches.
 - The customers downloaded and installed versions of the software with the malicious code via their routine updates.
 - The malicious code stayed dormant for a few weeks.
 - Once active, the malicious command and control code is used by the threat actor to steal data from customer networks.
 - The threat actor has been identified as a Russian Intelligence Service.
 - The timeline shows that they were active as early as September 2019.
 - The attacker can do things such as learn about the organization's network, impact email services and harvest data from emails, and reconfigure network devices which can have catastrophic implications for agency services.
 - In December 2020, FireEye experienced a compromise, made a public statement, and issued a blog post that alerted organizations about the malware.

-
- Microsoft flagged digital certificates of the malware and “sink holed” the domains used by the attacker.
 - Microsoft Exchange – What Happened:
 - State sponsored threat actors exploited zero-day vulnerabilities in the 2013, 2016, and 2019 versions of Microsoft Exchange Server to deploy backdoors and malware.
 - The attacker secured access to the servers through bugs or stolen credentials, and then created web shells to hijack the systems, giving the attacker persistent access after vulnerabilities were patched, and the ability to execute commands remotely.
 - Allowed access to other systems and networks within that agency
 - Determine the steps federal agencies have taken to coordinate and respond to the incidents
 - Increased guidance for agencies:
 - Statutory requirements from Congress, the Executive Order, a standardized playbook to respond to vulnerabilities and incidents, and supply chain risk management and security.
 - OMB memo on continuous detection with monitoring and logging
 - NIST is discussing supply chain risk management guidance that highlights the need for organizations to better identify, assess and respond in this area.
 - Microsoft Exchange:
 - All federal agencies with infected versions completed all required steps within the required timeframe and were able to present network system scans to show the compromise had been cleared.
 - Two Cyber Unified Coordination Groups (UCG) were established: one each for the SolarWinds and Microsoft Exchange incidents.
 - Each UCG had members from CISA, FBI, the Office of the Director of National Intelligence (ODNI) and the NSA, as well as private sector partners.
 - Met almost daily to receive active reports on information sharing, cyber threats, and other vulnerabilities and techniques,
 - CISA’s role: Served as the central point of contact to facilitate the conversation and collaboration.
 - FBI’s role: Served as one of the leads in threat response activities and investigated and gathered intelligence on the criminal activity.
 - ODNI’s role: Served as federal lead for intelligence support
 - NSA’s role: Engaged with Federal industry related partners to assess the scope of the incident, from the compromise to the remediation efforts, and provided technical mitigation guidance that needed to be managed
 - Challenges:
 - Just removing and updating the Orion software may not remove attacker
 - Identify lessons learned by federal agencies from the incidents
 - Coordination with Private Sector: Need to increase coordination, collaboration, and communication with the private sector
 - Coordination Across Government: Government agencies should further strengthen their collaboration across the government for information sharing on cyber vulnerabilities and incidents in the US,
 - Information Sharing Restrictions: Address challenges to information sharing between agencies with different levels of data classifications
 - UCG lessons learned: Need to align the technology investments with operational priorities, strengthen public private engagement, and improve threat intelligence information sharing among federal agencies.

GAO Report and Blogs

- Link to GAO Report - [Federal Information Security: Agencies and OMB Need to Strengthen Policies and Practices | U.S. GAO](#)
- April 2021: [SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response \(infographic\) | U.S. GAO](#)
- February 2022 blog: <https://www.gao.gov/blog/hacks-bring-new-urgency-moves-congress-and-agencies-reduce-future-cybersecurity-risks>

Discussion:**Information Sharing**

- Giulia Fanti asked if Ms. Franks could comment more on the types of information being shared and if there are types of information that should be shared, but are not currently and the reasoning for that?
- Jennifer Franks replied that information sharing starts at the indicator of compromise. Agencies can then begin to look at where and what their focus should be. They're communicating on containment procedures; Some agencies decommissioned systems then started the process of eradicating, some did not have to go that far.
 - Sharing information on network forensics but not so much on audit logs and monitoring procedures. These are significant details that would have provided us more of that breadcrumb trail of what was happening.
- Some agencies were more restrictive to share information. For example, NIH may have been reluctant to share because:
 - The breadcrumb could have been laid anywhere,
 - Of sensitivities around the pandemic and the sensitivities of the data on those systems.
- On the other hand, Commerce was going through the census and there was some cybersecurity sensitivity, but they were a lot more open in telling the public their emails were compromised.
- Sharing information on the types of data the attackers were after or other pertinent details would have helped other agencies to know where to look.

Correlation with Successful FISMA implementations and New GAO Study

- The Chair asked if they saw any correlation between how successful agencies are at implementing FISMA authorization to operate, continuous monitoring, etc. and how badly they were impacted by SolarWinds or the Exchange vulnerability.
- Jennifer Franks replied that the review didn't really look at that but her new review looking at federal-wide incident response efforts will. The new review is forensically looking at how agencies are complying with the federal guidance. It will be government-wide but focus on those nine agencies that were impacted and how they are managing their network.
- The Continuous Diagnostic and Monitoring (CDM) report, [GAO-20-598, Accessible Version, Cybersecurity: DHS and Selected Agencies Need to Address Shortcomings in Implementation of Network Monitoring Program](#), reviewed 12 agencies. All of them had the tools, the software, and hardware in place, but they had not fully deployed CDM. CDM would help an agency further review that network and be able to scope the network monitoring issues, the audit log.
- This new review will be looking at FISMA and how they're aligning those additional security control elements that would have helped them to better detect and then respond. The detect piece is key because going back to the six to nine months no one knew someone was lying dormant in their environment.

-
- The Chair then asked two related questions:
 - To what extent are federal agencies complying with requirements?
 - If they're meeting the requirements, did it make a difference on the impact to the agency? Did it matter?
 - Jennifer Franks commented that she likes that question: do the things being done matter? Once this type of high-profile event takes place, do their efforts matter? When there are efforts in place, are they sufficient?
 - The Chair commented that ISPAB will contact her when she does her next study.
 - **Other Reports and Studies**
 - Jennifer Franks commented that the DOD cyber incidents report will be out this summer and it will not be classified.
 - There is a State Department cybersecurity engagement, limited official use only, that will be out this summer and then the public one will come out later.
 - She has one looking at HHS and the subordinate departments: CDC, NIH, and FDA. That one should be out before the end of this year.
 - The IRS Incident Response focusing on securing taxpayer information should be out around September/October
 - The federal-wide ones will come last, likely top of the year.
 - Jennifer Franks added that there's no clear criteria from anyone on the cost from these attacks. Are the resources enough to have prevented or made an impact to prevent what took place?

The Chair recessed the meeting for a 10-minute break.

Senate Commerce Priorities in Cybersecurity

Richard-Duane Chambers, Senate Committee on Commerce, Science, and Transportation

John Beezer, Senior Advisor, Senate Committee on Commerce, Science, and Transportation

Maryasa England, Research Assistant, Senate Committee on Commerce, Science, and Transportation

Alice Hau, Technology Policy Fellow, Senate Committee on Commerce, Science, and Transportation

James Mazol, Staff Member for Senator Wicker at Senate Commerce Committee

Richard-Duane Chambers, Senate Committee on Commerce, Science, and Transportation

- Things we've been working on:
 - United States Innovation and Competition Act (USICA)([S.1260 - 117th Congress \(2021-2022\): United States Innovation and Competition Act of 2021 | Congress.gov | Library of Congress, USICA Section-by-Section 5.19.21.pdf \(senate.gov\)](#))
 - Runs the major investments into America's R&D pipeline and workforce.
 - Cyber Workforce Shortage: It's great to build out your technology and put up as many protections as possible in other systems, but this is going to come down to the availability of workforce.
 - USICA identified cybersecurity as one of the 10 key technology focus areas that we would like the government to be investing in, in particular, the new Technology Directorate that we are standing up inside of the National Science Foundation.
 - We've directed NIST to take further actions to help to provide resources to schools and institutions of higher education to protect themselves from cyber risks.

-
- Within the bill, we have directed additional funds to NIST Manufacturing Extension Partnership to help small and medium sized manufacturers mitigate vulnerabilities due to cyber-attacks,
 - Supply chain resiliency.

John Beezer, Senior Advisor, Senate Committee on Commerce, Science, and Transportation

- Privacy was mentioned in the State of the Union address and focused on children's privacy, talked about banning targeted ads to kids and had a great statement about the national experiment they're conducting on our children for profit.
- Two Bills:
 - The Kids Online Safety Act, Senator Blumenthal and Blackburn, is primarily a children's safety bill, but it gets into privacy.
 - [kids online safety act - one pager.pdf \(senate.gov\)](#)
 - It's coming out of the Francis Hogan whistleblower incident
 - It's patterned after the UK's age-appropriate design code, making it harder for strangers to contact kids, restricting the sharing of kids' location information, setting the strongest privacy protections on by default, and the general concept of duty of care
 - The idea of a duty of care is, legally, slightly amorphous but it's there as a backstop for all the new and interesting things that keep coming up in the world of privacy abuses.
 - Update to the Children's Online Privacy Act (COPA)
 - A little over 20 years old now
 - The upgrade is going to expand that to kids under 16.
 - The current version has an "actual knowledge standard." You weren't held accountable for the content you presented children if you didn't know you were interacting with a child. That's being updated to "constructive knowledge" which is you really should know that you're interacting with a child.
- Comprehensive Privacy.
 - We've done a lot of work and getting close.
 - Overview of current Privacy laws:
 - There are state laws in California, Virginia, Colorado, and Utah either just passed one or is about to.
 - There's the GDPR in Europe.
 - Privacy falls into two buckets:
 - Consumer rights: access to your data, the ability to correct your data, the ability to delete your data, and the ability to export your data.
 - There's also a general concept to that companies should not be collecting sensitive data on you without your affirmative express consent and, if you opt out of letting people and services collect your data, they can't or they shouldn't be able to diminish the service. That's tricky because some private data may be necessary for a service, and they might claim all private data is necessary.
 - Company obligations
 - Sticking points: private right of action.
 - Do individuals have the right to sue for damages and preemption?
 - How much does the federal law preempts state laws?
 - New things to consider:
 - The idea of algorithms and how they impact civil rights
 - Even if services are not trying to discriminate sometimes the algorithms do it anyway.

-
- How do we hold people accountable for that?
 - How do we prevent that?
 - We've had some conversations around arbitration and whistleblower protections are coming up.

James Mazol, Staff Member for Senator Wicker at Senate Commerce Committee

- Works for Senator Wicker on the Commerce Committee.
- The Senator did a good job of teasing out cybersecurity dimensions of USICA last year.
- Given the establishment of national cyber director position, we've been working to ensure there are clear roles and responsibilities for federal agencies regarding cyber security and that the establishment of the ONCD doesn't upset NIST's critical role in the standard setting process.

Alice Hau, Technology Policy Fellow, Senate Committee on Commerce, Science, and Transportation

- National Defense Authorization Act (NDAA)
 - Passed a couple of important bills out of committee and make those into NDAA:
 - [Harvesting American Cybersecurity Knowledge Through Education \(HACKED\) Act \(S.2775 - 116th Congress \(2019-2020\): HACKED Act of 2019 | Congress.gov | Library of Congress \)](#)
 - Supporting the cybersecurity workforce advancing certain cybersecurity workforce programs.
 - We want to continue our efforts to support the NICE program, which supports cybersecurity education, and encourage that to be adopted by other agencies looking to support the workforce
- Cyber Leap Act ([S.3712 - 116th Congress \(2019-2020\): Cyber Leap Act of 2020 | Congress.gov | Library of Congress](#))
 - Would mandate the Commerce Secretary to establish a minimum of five public competitions offering public cash or non-cash prizes to address the federal government's top cybersecurity challenges
 - Encourages research and development in the field of cybersecurity,
 - This continues support of research through NSF.

Discussion

Cybersecurity Workforce

- The Chair commented that there are 2 parts to the cyber security workforce:
 - The "cybersecurity" people who have to set the standards, do the technology, build the tools, and do the cybersecurity management,
 - The rest of the workforce who have to do the right things with regard to cybersecurity or else they can undermine everything that the agencies and the cybersecurity workforce try to do.
- The Chair asked if the things they're looking at regarding workforce go beyond direct cybersecurity positions to the broader needs of the entire US workforce?
- Mr. Chambers mentioned the importance of some of the other investments such as asking NIST to work with institutions of higher education. His expectation is that by sharing knowledge on cybersecurity, that knowledge isn't limited to the explicit cyber workforce but to a much broader central section of the population.
- He also expects more notifications in the coming period from members of Congress and the federal government reaching out to business groups and manufacturers. They're doing the same with

manufacturing Extension Partnerships (MEP) to provide information, give them access to resources, and asking them to take a second look at their cybersecurity defenses, update, and close gaps.

- James Mazol added the committee has done some work on fraud and cybersecurity literacy and at their last markup there was an American Cybersecurity Literacy Act which would direct NIST to develop tools and materials to spread that information beyond the direct cyber security workforce.

Use of Artificial Intelligence and Machine Learning

- Giulia Fanti asked what they think about storing and sharing machine learning or AI models that are trained using private data? Are there thoughts around regulating those kinds of indirect representations of data?
- John Beezer responded that at times data gets dumped into machine learning and it's assumed the data can't be extracted back out but when data is used to train an algorithm it's likely that data can be abused.
 - Example: The FTC went after Weight Watchers for a children's diet app for kids over 13. It was targeting kids under 13 by encouraging them to lie about their age. The settlement was:
 - Stop making the app available,
 - Destroy the data that was gathered from it, including the algorithms from the machine learning based on that data.
 - Even if that isn't a personal privacy violation, it was unethical, and they shouldn't benefit from it.
 - “Data laundering” – The use of data you're not supposed to have and that can't be commercialized to train an algorithm. The data is then disposed of.
 - They've gotten the benefit from the data without any traceable indication they've ever had the data.
- Giulia Fanti asked if he sees a trend towards trying to regulate the way that these models are handled?
- John Beezer replied that even when there's no intent, you have to look at what comes out of the process. We're trying to make sure that it's not enough to say that you can't develop an algorithm that has these characteristics; you need to prove that it doesn't have those characteristics.

Public Comment, Summary of Day 1, and Board Discussions

- No public comments were received.
- Board Discussion
 - The Chair called for comments from the board.
 - He mentioned that he's not sure if open-source wants the board to make a formal comment. He reminded board members of a letter sent a while ago encouraging NIST to sign up with the OSSF but mentioned that may have been overtaken by events in the White House meeting in January.
- **Open-Source**
 - Douglas Maughan asked Phil Venables if he has an opinion about what could be different in open-source this time compared to things the last 20 years?
 - Phil Venables replied that the big difference this time is the amount of effort behind things.
 - The formation of OSSF and its members are investing and participating.
 - Providing support, providing different types of people to help the projects, and investing in tool labor, among other things.
 - Need more end user organizations, corporations, and government agencies to participate.

- Need different types of people engaged with the open-source community, not just software developers but maintainers, security people, people that know how to manage vulnerability and disclosure, people who are experts at packaging software, testing the whole framework, all manner of things.
- There's a general realization in the community that the problem's never going to be fully solved but now we've got the apparatus and the community.
- Still more work ahead of us than behind us.
- **Additional Guidance, NIST Cybersecurity Framework and NCCoE Project**
 - Arabella Hallawell commented that a lot of organizations are still struggling organizationally. There's a gap between the developers and the security teams. She asked about the possibility of putting together, within the NIST Cybersecurity Framework, a recommendation or end user guidance around individual organizational best practices, such as SBOM, automatic dependency updates, or other things that help close the gap?
 - The Chair replied that the National Cybersecurity Center of Excellence (NCCoE) is wrapping up a demonstration project or pilot aimed at best practices for applying this secure software development framework.
 - Kevin Stine added that NCCoE recently issued a specific framework profile targeted at ransomware, almost like a quick start guide, that covers the things organizations should be focusing on to prevent, respond to, and recover from ransomware.
 - The Chair added that it's about getting people on board, getting the organization to understand its roles and do the right things. Resources that align with that are probably very important in scaling success.
 - Arabella Hallawell clarified that perhaps the Cybersecurity Framework could be a forcing mechanism where there was some structure and plan so organizations could organize themselves more efficiently.
 - Matthew Scholl commented that the Cybersecurity Framework has the five functions with resources mapped to each function. There was more on the protect side and not a lot of material for the end functions, such as respond, recover, and detect.
 - The Chair suggested that as Kevin Stein gets his NCCoE project going, he could present the technical, process, and organizational components.
- **Process Comments**
 - Katie Moussouris and Essye Miller asked that the presenters to be reminded that we have decades of security and privacy practitioner experience among the members and, to get the most out of their presentation, we want them to skip to the good part. She wants more interaction time with the speakers.
 - Matthew Scholl added that NIST tries to do prep calls and extensive discussions with the speakers about who the board is, including sending them the links to the board member pages and giving them the theme and bottom-line message that folks want to hear. We will do more in helping folks with pre-calls to dial it in tighter.

Day Review and Meeting Recessed

The Chair adjourned the meeting at 3:52 P.M. ET.

Thursday, March 10, 2022

The Chair opened the meeting at 10 a.m. ET and welcomed everyone to the call.

Congressional Research Service (CRS) Report (R46926) on Federal Cybersecurity: Background and Issues for Congress

Chris Jaikaran, Analyst in Cybersecurity Policy, Congressional Research Service (CRS)

This report was published September 29, 2021. Mr. Jaikaran's talk will cover:

- What is CRS?
- Federal cybersecurity concepts
- Federal Agency Roles
- History of Cybersecurity Bills
- How Congress and the public are looking at FISMA moving forward

What is CRS?

- Part of The Library of Congress
- Our mission is: Serve Congress with high quality research, analysis, information, and confidential consultation to support the legislative debate and members representational and governmental oversight duties.
- CRS does this is through products and consultative services:
 - Products: Our key product is the CRS report, but we also have blog posts, briefing documents, infographics, videos, podcasts, and seminars with both CRS analyst as well as extra speakers
 - Services: include in-person, remote, and telephone briefings for members and staff, emails, custom memoranda, and hearing support to include committee testimony and general research to support the legislative debate
 - All products and services are non-partisan.
- Products made public are available at crsreports.congress.gov.
- Our analysts occasionally engage with research communities like this one to present our research or get feedback and that helps us do our job for Congress.

Federal Cybersecurity Concepts

- Mr. Jaikaran covered basic cybersecurity concepts that apply to federal agencies such as the need for on-going risk management and for agencies to follow the NIST Risk Management Framework.

Federal Agency Roles

- The "Big Three"
 - Office of Management and Budget (OMB)
 - At the strategic level,
 - Have oversight of agency budgets and oversee agency adoption of cybersecurity policies,
 - Responsible for reporting annually to Congress and delivering guidance to agencies on how they should implement cybersecurity programs via circulars and memoranda
 - The Cybersecurity and Infrastructure Security Agency (CISA)
 - Operational level
 - Oversee agency adoption of programs and have authority to offer technical assistance to agencies
 - Have authorities to compel agencies to take certain measures to ensure cybersecurity
 - Each individual agency
 - Tactical level

-
- Responsible for managing the site security risks to their own agency.
 - May delegate this to a senior agency official such as an Assistant Secretary position or CIO.
 - Other agencies involved with Cybersecurity
 - NIST develops standard and guidance to inform agency security practices
 - Agency inspectors general have a responsibility to annually evaluate the agency's cybersecurity program and report back to Congress
 - The Comptroller General, the head of GAO, is also authorized to evaluate agency and government wide cybersecurity performance
 - The National Cyber Director has authority to streamline agency cybersecurity requirements and to review agency cybersecurity budgets.

The Chair informed the speaker that the board members are very familiar with federal cybersecurity practices. He doesn't have to worry about going into detail on introductory information.

History of Cybersecurity Bills

- The Privacy Act of 1974: which governs how agencies collect, retain, and disclose an individual's records
 - Establishes the trust and confidentiality that carries over in agency information security programs through the 80s into today
 - The Computer Security Act of 1987 established standards for protecting federal computer systems
 - The Information Technology Management Reform Act of 1996 required NIST to propagate compulsory standards for federal computer system security and privacy
 - The Federal Information Security Management Act (FISMA) of 2002 established federal cybersecurity roles and responsibilities.
 - Federal Information Technology Acquisition Reform Act (FITARA) of 2014 lays out roles related to the acquisition and management IT systems
 - The Federal Information Security Modernization Act of 2014 updated FISMA to recognize the role of DHS in government cybersecurity. OMB delegated some responsibilities to DHS for collecting information OMB can produce its annual report to Congress.
 - The Cybersecurity Act of 2015 Congress clarified some additional authorities for Department of Public Security and Congress established cybersecurity requirements for agencies including ensuring systems are encrypted or employed multifactor authentication
 - The National Defense Authorization Act for Fiscal Year 2021: Congress created the Office of The National Cyber Director.

The Chair asked if Mr. Jaikaran could skip the background information and talk about what Congress is doing and thinking now and his perspective on possible legislation.

How Congress and the public are looking at FISMA moving forward

- Congress has directed agencies to have responsibility for cybersecurity and resources available to agencies to perform that responsibility through the annual appropriation cycle, but they leave it to the executives to determine how the responsibilities will be met.
- Effectiveness of an agency's ability to execute a cybersecurity program, compounded by Significant cybersecurity incidents the past 15 years such as SolarWinds
- Congress:

-
- Passed laws to provide agencies with multi-year money to effectively plan and manage large complex appropriations and acquisitions for modernizing legacy systems.
 - Investigated the use of newer services and implementing new ideas such as endpoint detection and response, penetration testing, and Zero Trust Architecture
 - Pursued questions around the utilization of shared services so more is happening across government
 - Legislation is moving to modernize FISMA.
 - Two bills in the senate and one in the house.
 - Both seek to affect agency cybersecurity for mobile devices and
 - Create metrics for managing cybersecurity programs,
 - Create requirements for how agencies log and retain those logs,
 - Authorize active threat hunting,
 - Codify the vulnerability disclosure program that agencies were required to implement last year per operational directives,
 - Encourage agency adoption of zero trust architecture (Executive Order 14028),
 - Clarify and harmonize roles and responsible across DHS, NIST, OMB, NCG and GAO.
 - Differences between the bills:
 - The Senate proposal:
 - Encourages CISA to have an employee assigned for each federal agency to be their liaison and advisor.
 - Creates pilot programs for:
 - Continuous evaluations of the agency cybersecurity program and
 - Pilots around the shared services security operation centers.
 - The House proposal:
 - Codifies the position of the federal chief Information Security Officer and
 - Budgeting for pilots on cybersecurity risk, active cyber defense, and shared services and
 - Authorizes the deployment of endpoint detection and response capabilities.
 - Proposal to modernize FedRAMP
 - Both the House and the Senate have proposals that establish FedRAMP as a GSA program and set structures to coordinate cloud security across various departments and agencies like DHS, DoD, and GSA.
 - Senate bill S.3600 Strengthening American Cybersecurity Act of 2022: collapses proposals for fiscal modernization, cyber incident reporting, and FedRAMP authorization into one bill.
 - Adopted some of the provisions from the House proposal such as the position of the Chief Data Officer and the proposal around risk-based budgeting for agency cybersecurity programs. It passed the Senate last week.

Discussion

NIST's Role and the Relationship Across Agencies

- The Chair asked about Mr. Jaikaran's view on NIST's role and the standards and guidance that it provides. If Congress is looking at the relationship across the agencies, NIST, DHS and OMB and the National Cyber director?
- Mr. Jaikaran replied that he can only speak about proposals that were introduced into Congress but that he can't speak about his work with committee staff or members. On the first part of the question:
 - Congress has recognized NIST provides expertise in developing standards and guidance.

-
- NIST's process of consulting with experts, being open for debate, and then producing Special Publications or interagency reports is desired and not under question.
 - Congress has raised ideas around expanding this role and there were proposals in previous congresses to provide NIST authority to evaluate how well agencies are following NIST Special Publications. These proposals have generally not advanced very far in the congressional debate. Those authorities already exist in FISMA with the responsibilities of each agency's inspector general and the responsibilities of the Comptroller General at GAO.
 - On the second part of the question regarding responsibilities across the federal government:
 - There is an effort in the current proposals for FISMA modernization in the 117th Congress to clarify the roles and responsibilities between various agencies as well to harmonize those both for FedRAMP and for FISMA operations.
 - The Chair asked if he could comment on what that harmonization would produce or how it would change things?
 - Mr. Jaikaran replied that the legislation creates a little bit more clarity on who was meant to carry out what responsibility, especially at CISA, but he doesn't know how individual agencies will implement the legislation. That's a question that GAO would address as they conduct an evaluation a year after Congress' passage and the president's signing of the bill.

Selection of Areas of Research and Analysis

- Jessica Fitzgerald-McKay asked how the areas of research and analysis are selected; are they directed solely by questions from Congress, or can they choose topics that might be of interest to Congress?
- Mr. Jaikaran replied that consultation work is in direct support of congressional requests and questions. For their CRS reports, analysts will look at the congressional debate and come up an idea for a report to support the legislative debate.

Types of Evaluations and Evaluation Metrics

- Katie Moussouris commented that she heard him mention that there will be an evaluation of the implementation. Is that more an evaluation of if they implemented all the changes mandated or will there also be an evaluation of the effectiveness of the controls that are mandated? If the later, what metrics are you using to evaluate the effectiveness of the controls
- Mr. Jaikaran replied that would be a better question for GAO. When they are directed by Congress to perform a deployment audit, they follow the direction provided by Congress in the authorizing statute.
- Katie Moussouris asked if there are plans to assess implementation capability gaps? There is lots of information on what to implement but less on how to implement. As a result, agencies can be evaluated on if they did the implementation but that doesn't determine the effectiveness of the programs or look at staffing and tooling short falls in making the programs successful. Will there be a maturity and capabilities assessment?
- Mr. Jaikaran replied he thinks it does happen annually with the IG's evaluation of each agency's information security program.
 - OMB directs agencies to use the NIST Cybersecurity Framework categories for looking at an agency's cybersecurity program.
 - The agency IGs assess the maturity of the agency's implementation along functional categories
 - Agency IGs are employees of the agency and, while the reports are made available to Congress, they are submitted to the agency first and the agency does have some purview over the operations

of their IG. Congress can review the effectiveness of an agency's cybersecurity programs using IG reports and most of these reports are made public.

- The updates to FISMA during the 117th Congress authorized not just the vulnerability disclosure program but also penetration testing. It will be interesting to see how agencies adopt recommendations from the pen test reports or how those will be built into congressional budget justifications for future year appropriation asks.
- When you look at the authorities for binding operational directives and emergency directives, CISA releases binding operational directives for things they can independently verify have been accomplished. Emergency directives have been used for things for which CISA does not have purview into the agency, so they rely on the agencies to report.

Privacy

- The Chair asked about any thoughts or observation on congressional directions around privacy?
- Mr. Jaikaran replied that privacy is not a topic that he has been tracking and doesn't have any information to share on privacy.

National Academy of Public Administration (NAPA) Report: A Call to Action: The Federal Government's Role in Building a Cybersecurity Workforce for the Nation

Dan Chenok, Co-Chair of the Academy Panel,

Karen Evans, Co-Chair of the Academy Panel,

Sarah (Sally) Jaggar, Study Project Director of the Academy Panel

Introductions

The Chair introduced the speakers and mentioned that Dan Chenok as a former ISPAB Chair.

Dan Chenok:

- Served as ISPAB Chair 2006-2012.
- Worked for OMB prior to that

Sally Jaggar:

- A fellow at NAPA
- 25-year career at GAO, followed by the Partnership for Public Service
- With NAPA for about 10 years.

What is NAPA?

- National Academy of Public Administration is a nonpartisan, congressionally chartered entity to do studies, to provide advice and assistance to organizations throughout government.
- About 40 years old
- "The Academy" works with organizations at all different levels of government, academicians who are members, and about 1000 fellows giving NAPA insight into challenging issues of today, including cybersecurity.

The Study:

-
- The FY 2021 Consolidated Appropriations Act for Homeland Security included a clause for DHS to contract with NAPA or a similar group to do a study of the cybersecurity workforce programs at CISA in DHS and to how they fit into a larger context.
 - Study team is overseen by almost 1000 leaders and fellows from government and industry including many from nonprofits and academia.
 - Exploring ways to amplify and extend this work

The Focus and Scope

- Initially just focused on what is happening at CISA, particularly their Cybersecurity Defense, Education and Training (CDET) program.
 - Worked with cyber.org and other organizations around the country to develop programs.
 - Congress was interested in knowing how CISA's education related programs were working
- We realized people were facing larger issues in cyber workforce and knowledge that's needed by people at all different levels in the nation.
- Broadened the focus of the study to identify and address the issues and needs to achieve the desired results
- The Challenge:
 - Currently a half million jobs unfilled that are cybersecurity related in the in the country
 - Estimates of 3 million unfilled cybersecurity jobs around the world
- (Referred to slide 2 for the research questions addressed in the study)

Methodology

- Interviewed over 90 individuals involved in cybersecurity training or have cybersecurity workforce needs
- Tried to address the larger question of, "what would make a difference?"
- We did focus specifically on the CISA workforce development program
- Realized what is needed is reliable information on overall needs and what kind of impact are the current programs and initiatives having.

Findings and Recommendations

- Need a comprehensive, government-wide workforce development strategy
 - There are terrific examples of strategies ongoing, such as the NICE strategic plan
- Need alignment and amplification of these strategies and a comprehensive government wide strategy that:
 - Drives workforce development that builds on previous work
 - Allows all players to understand their role and their program's role in the strategy
 - Implementing that strategy needs a governance structure to coordinate all the players
- Currently that coordination happens organically across many of the workforce programs that NIST helps to drive but no tie-in to the new Office of the National Cybersecurity Director (ONCD).
 - ONCD is working with CISA, NIST, NSA, DOD, across NSF, and the other agencies to create this governance framework to drive strategy to address the issue
 - ONCD plans on having a session at the end of April around workforce and other elements.
- Need good data to understand the impact of cybersecurity workforce programs.
 - There's not a lot of good data around the federal workforce imperative as opposed to national workforce imperative.
 - There isn't a Bureau of Cyber Statistics or something similar.

-
- It was important for this activity to provide a common set of guideposts for people to understand the impact of workforce programs
 - Study used three criteria in assessing CISA's programs:
 - Diversity,
 - Scalability and
 - Excellence
 - Referred to the report for detail on those findings
 - Overall, CISA is making good progress.

Essye Miller asked if they looked at what the Federal CIO Council was doing in this workforce space as a point of reference in their efforts.

Mr. Chenok and Ms. Jaggat replied that they spoke with Chris DeRusha and the OMB leadership team.

Government-Wide Strategy Elements

- The first element is around the K-12 pipeline, encouraging people in schools to understand that cybersecurity can be a valuable career and provide opportunities for kids to understand what those NICE careers look like.
 - Elevate and expand NSF and Department of Education cybersecurity education
- The second element is around pre-professional training, enabling schools, colleges, universities, vocational schools, community colleges, and certificate programs in cybersecurity with technical, operational, and managerial competency skills that are needed to enter a cybersecurity career
 - Cybersecurity workforce issues and the level of education and awareness needs to be focused on all three of these categories:
 - Those working directly in cybersecurity (the "few"),
 - People designing and developing programs, especially in technology, where cybersecurity is a critical input to their work, but who aren't a "cyber professional" (the "many"), and
 - The entire nation of users (the "all").
 - and the.
 - The report primarily focused here on cybersecurity workforce, but the cognitive skills and competencies could be adapted to train those larger groups of individuals who need cybersecurity understanding and awareness.
- The third element is around matching people to jobs.
 - NAPA has done work around how to reform the federal hiring practice, for example, DHS work around direct hire authority for cybersecurity and the US digital service has shown a new model for bringing in technology talent.
 - Recommend developing more of this kind of job matching capability, working both with government and the private sector.
- The fourth element is being able to assess the performance of the workforce system in a way that:
 - Promotes innovation such as experiential learning
 - Demonstrates competencies for the wider workforce as they develop and enter more in the digital economy
 - Pays attention to developing performance metrics and creating a Bureau of Cyber Statistics or some other type of enterprise to provide data to build on the efforts.

Katie Moussouris commented that one of the key problems in getting roles filled is that cybersecurity jobs require some degree of experience and expertise to be effective in those roles and that there is an apprenticeship to journeyman to expert pipeline problem. She asked if there is any strategy that, instead of

matching people who already have the qualifications for those roles, designs hands on learning programs to bring people along and grow their capabilities to facilitate that pipeline of expertise and close gaps?

Mr. Chenok replied that he's an example of that being an English major and the report did address apprenticeship programs and alternative pathways and the need to broaden, diversify, and drive forward the ability and skillset of people that have the potential to move along a pathway to cybersecurity professionalism.

Ms. Jaggard added that this is an area that we really recommend there be further action because we discovered there's a mismatch between what employers are looking for and what they need. We want to try to increase the conversation about getting people in who have the hands-on experience that is needed rather than just focusing on formal education. This is also a focus of interest at CISA.

Karen Evans added that there's the also the idea of hiring based on aptitude. There are promising practices and mechanisms for testing and measuring aptitudes in people that are in different fields and then bringing them in so that they can do the jobs, get the on-the-job training and other kinds of training or education to do the job.

Key Elements of the NICE Strategic and Implementation Plans

- Strong alignment between the recommendations on the strategy and the elements of the plan such as:
 - Promoting discovery of careers, sustaining a diverse and skilled workforce, competencies, pathways, and closing gaps.
 - The study recommended that the new DHS Cybersecurity Talent Management System (CTMS) program could be extensible to other agencies.
 - Mr. Chenok suggested this as a future topic for the board
 - Driving more research on statistics and how you know if things are working
- Recommend that the national strategy needs to complement and amplify the NICE work.

Governance Framework

- Departments and agencies had pieces of a good solution for the nation.
- Cyber is a bipartisan issue and everyone recognizes the need to close this gap on cyber workforce issues so there is the opportunity to leverage the recommendations to create a structure so that the resources are there.
- Recommend the creation of a national strategy going forward so everybody can see their part in that strategy and can contribute to the outcomes.
 - There are a vast variety of private sector, public sector, state level, needs and private sector, public sector, State level, and federal government initiatives underway, and
 - People can't keep track of who's doing what.
- The recommendation is that the National Cyber Director's Office:
 - Would lead and bring the strength of White House Office capabilities to ensuring that the execution was happening within the departments and agencies,
 - Help efforts, such as NICE, to accelerate, move forward, and leverage partnerships between the private sector, academia, and the federal government,
 - Ensure coordination and collaboration so all the initiatives are going in the same direction, and they complement versus contradicting and competing each other, and
 - Provide a place for keeping track of all the moving parts.

Discussion

- **Increasing Productivity**

- Phil Venables asked if they looked at how to increase the productivity of the people we've already got in the cybersecurity workforce?
- Ms. Evans replied that the CIO Council has an initiative underway looking at existing workforce activities and folks within the federal government, and re-skilling and providing them with tools to be able to close some immediate gaps. We need statistical measurements and metrics. That's why we were really pushing on the idea of a Bureau of Cyber Statistics. Let's get official statistics on cyber incidents and reporting, including armed forces statistics. Statistics is an area that the government does well, and we could then share that information and inform national strategies.
- Phil Venables added that some commercial organizations say they've got 300 cybersecurity vacancies for different types of roles but, upon inspection, 250 of those roles could be automated. They're just not doing the work in the right way. We have to look at the supply and demand side of all of this and include a heavier emphasis on automation and productivity to get rid of a lot of the kind of the grunt jobs that discourage people from progressing.
- Mr. Chenok commented that was a key part of the matching element. There are certain types of skills that are appropriate for certain types of jobs and there are certain types of skills that will be automated, made more efficient, and that provides an opportunity for the workforce to advance.

- **Retention**

- Giulia Fanti asked if retention was a focus of the report?
- Mr. Chenok, Ms. Evans, and Ms. Jaggar commented that the focus was on the career development and diversity aspects of security, not identifying monetary and non-monetary incentives for cybersecurity professionals and how those incentives could be structured to increase retention. They think that that's a very fruitful area for future research. If we have data on retention, that will help us understand the demand side and help match up the supply with demand. This could be a good job for the Bureau of Labor Statistics.

- **Collaboration and Coordination**

- The Chair commented that he wasn't aware of the number of players prior to reading the report. He knew about NIST, the NSA efforts around GenCyber, NSF and the academic side of things but not DHS. Some of these are congressionally directed and each has its own piece to do. Your suggestion of collaboration and coordination is important to ensure that the agencies in this space understand what others are doing. There's an opportunity for them to know what's going on and take advantage of each other rather than starting from scratch. It seems the National Cyber Director is aware of and sympathetic to the need to do this. The government certainly needs to address it for its own sake and for the country.
- Mr. Chenok noted that there are communities of interest in cross-collaborative functions. The NICE, as a community coordinating council, can build on, amplify, and bring in more executive focus across the agencies working together. There already are good relationships across many of the programs at the at the operator level.
- Ms. Jaggar added they were impressed at the coordination and the significance of NICE as a major coordinating function, but decisions are needed about who's doing what. For example, they identified four different entities developing K - 12. programs. If those are being sent out to state or educational entities, how do they decide which one to go with? That's why collaboration is important, looking at similarities and differences in the curricula and determining the effectiveness or if it is wasted effort. That's why it's recommended that the ONCD role be more than just bringing people together to chat about what they're doing.

-
- Ms. Evans emphasized the need to have follow up on the performance of these programs so that they know what they need to continue or what additional authorizations they need to get going forward to address these problems.
 - **Flexibility**
 - Katie Moussouris mentioned that many cybersecurity jobs are emerging as a new profession and asked what kind of elasticity are we allowing in this job study? For example, threat hunting wasn't popular a decade ago, but it's essential.
 - Mr. Chenok replied that they didn't get into which specific competencies are coming down the pike. They suggested a process for agencies to work together to develop an understanding of what those jobs are going to be, develop a pathway to give people skills to move toward those evolving jobs, and a framework to match people who have those skills to the evolving picture.
 - Ms. Evans added that's the reason they were stressing that the National Cyber Director's office would be the place for the governance structure. If they formalize the governance structure, then the elasticity in forward leaning and emerging areas would be addressed there and would allow them into the channels of the agencies with the proper resources and support from OMB. The process and governance structure they're recommending would allow this flexibility for future job roles.

The Chair recessed the meeting for a 5-minute break.

Open Security Controls Assessment Language (OSCAL)

Michaela Iorga, NIST

The Challenge

- Frustration with the slow, labor intensive, lengthy, difficult process of assessing cloud services,
- The need to automate assessment of cloud services demonstrating compliance with statutory requirements
- Understanding FedRAMP's, cloud providers', and government customers' challenges
- Solution needed to be useful as the adoption of the technology was crucial
- information technology is complex and because of that, vulnerabilities are difficult to find and to remediate.
- Much of system owners and CISA's work is done using paper-based compliance which is out of date the day after it is written,
 - Critical risks may remain undiscovered or unaddressed
- Supporting and demonstrating compliance with many different regulatory frameworks can lead to mutually exclusive guidance and controls
- Adoption and deployment of complex cloud solutions was calling for interoperability and standardization

The Solution

- A general and flexible solution that will provide the means for implementing interoperable security assessment automation. This led to OSCAL.
- Stakeholders will be able to exchange the information in an interoperable fashion by using the same language. This language is:
 - machine-readable
 - Supports multiple formats: XML, JSON, and YAML

-
- OSCAL enables actors, tools, and organizations to exchange information about automation by supporting a cheaper, better, faster continuous system security assessment and monitoring

What is OSCAL?

- ~5-year collaboration between NIST and FedRAMP
 - OSCAL 1.0 released in June 2021: <https://github.com/usnistgov/OSCAL/releases/tag/v1.0.0>
- Target: to support the FedRAMP process
- But also wanted to build a solution that will extend beyond the government space
- Supports multiple compliance risk management frameworks:
 - SP 800-53, ISO 27001 & 2, and COBIT 5
- Enables automated traceability from the selection of the security controls through the implementation of the controls and the assessment of system security posture.
- OSCAL is a collection of related models linked to deliver traceability.
- OSCAL models are grouped in three layers:
 - The Control Layer
 - The Computation Layer
 - The Assessment Layer

OSCAL Adopters

Ms. Iorga shared a list of adopters who presented their OSCAL solutions at 2021 and 2022 events. This list can be found on slide 5 of her presentation.

How is OSCAL Different?

- OSCAL is designed:
 - To be a universal machine-readable language for the presentation of the security information.
 - To allow for custom extensions
 - Crucial for dealing with limitations
- No information is to be duplicated
 - Supported traceability allows for the linking of the information enabling tools to assemble the information when needed.
- Supports custom granularity
 - Controls can be decomposed all the way to the statement level
 - Parameters have unique identifiers so they can be referenced, and information is preserved for all steps in the process including, the catalog, the baselines or profiles, implementation, and assessment
- Vendors can document their product system security implementation into components
- Allows assessment plans and activities to be captured with custom cadence for selected components.
 - Nothing is monolithic; everything can be sliced and diced the way the consumer wants
- Plan of actions and milestones (POA&M) model can convey open risk back to the system owner and present them online with a system capabilities and controls.

OSCAL Layers and Models

- The Control Layer has two models:
 - Catalog Model
 - An organized collection of controls
 - May also define objectives and assessment procedures

-
- Profile Model
 - Defines a specific set of selected security controls requirements from one or more control catalog
 - Can concatenate catalogs and create custom profiles or baselines
 - Allows creation of custom controls for inclusion in profiles for merging with controls from other catalogs
 - The Implementation Layer has two models:
 - System Security Plan (SSP) Model
 - Allows the security implementation of an information system to be documented by starting with a selected OSCAL profile as the baseline
 - Component Definition Model
 - Allows definition of a set of components
 - Components provide description of the control supported by:
 - Specific implementation of the hardware, software, or service or
 - A given policy, procedure, process, or compliance.
 - These models are designed to work together
 - Component definition information can be used to populate the SSP with information identifying how the components of a system are satisfying the controls.
 - Allows granularity when documenting the parameter settings in multiple instances of the implementation of the controls
 - The Assessment Layer has three models:
 - Assessment Plan Model
 - Represents the planning of periodic or continuous assessment
 - Assessment Results Model
 - Captures assessment results such as findings, observations, and the risks that were identified
 - POA&M Model
 - Represents a set of findings for periodic or continuous assessments that need to be addressed by the system owner or maintainers.

Using OSCAL Models

- OSCAL models:
 - Not tools
 - Define the structures and schemas used to validate the OSCAL content,
 - OSCAL content is the collection of documents in open security controls assessment language (OSCAL).
 - Analogy:
 - OSCAL models are like language dictionaries and grammar books,
 - OSCAL content is the collection of literature in that language,
 - The formats, XML JSON and YAML, are like .pdf, .doc, or .rtf formats
- OSCAL Repositories:
 - Available to the public
 - NIST provides and maintains the following in OSCAL:
 - NIST SP 53 r4 and r5,
 - NIST 800-53A and B
 - FedRAMP provides and maintains the FedRAMP baselines in OSCAL

OSCAL Benefits

-
- Supports authorization to operate (ATO)
 - Bottom of slide 9 shows how the OSCAL models align with the NIST Risk Management steps and process
 - Top of slide 9 shows the actors that can use those models
 - Slide 9 shows the automated flow of information through each model resulting the authorization to operate.

OSCAL Supports Complex Systems

- OSCAL also supports:
 - Authorization to use and common control authorization,
 - inherited security capabilities,
- OSCAL system security plan (SSP) models support tightening up the inherited security capabilities and customer's responsibilities for logically stacked systems like:
 - Cloud systems that have distinct authorization boundaries, or
 - General support systems (GSS)
 - But NOT external service or interconnected systems
 - Not considered a stacked solution
 - Not leveraged authorization
 - Supported by OSCAL, just not as a Leveraged Authorization (LA)

Leveraged and Leveraging Systems

- Leveraged systems provide the capability
- Leveraging systems inherit the capabilities and controls
- In an SSP, the leveraged system can identify what may be inherited by the leveraging system, including a customer appropriate description of the control inheritance and any new responsibilities that must be addressed by the leveraging system to fully satisfy the control.
- The leveraging system can propagate the process
 - If there are multiple stacked solutions, then the same thing can be identified for customers.
- Flexibility of OSCAL
 - The leveraging system owner may either inherit the provided capability or address the control directly as if no inheritance is provided, at the discretion of the system owner.

BloSS@M Proof of Concept

- A CRADA pilot
 - Research collaboration agreement between NIST, DHS and UMBC
- BloSS@M stands for **B**lockchain-based **S**ecure **S**oftware **A**sset **M**anagement
- Is a proof of concept for asset management using AWS managed blockchain that supports hyper ledger fabric version 2.2.
- Also tried to demonstrate how state and federal agencies can use distributed blockchain solutions to meet professional requirements:
 - How could they engage such a service?
 - How would they demonstrate compliance with requirements upon them?
 - How it works:
 - There are two networks deployed and owned by DHS and by NIST
 - They each deploy their own members that provide services for use by other agencies
 - Before they can connect, they have to trust each other by demonstrating:

-
- They ATO their services,
 - They preserve that security posture, and
 - It is done in a manner that provides the same confidence and the assessment is done with the same rigor because it's important to be able to implement and assess the controls in the same way.
 - The proof of concept demonstrates the use of a separate channel of the blockchain solution to document the ATO to those members
 - That channel also provides permissions that allow or deny member access to the service.
 - If a member is deficient doesn't pass the test or something happened, the blockchain service and all the others can vote that member out until they remediate the deficiencies.
 - Using OSCAL to demonstrate that
 - Still in development
 - Plan to demonstrate the inheritance using AWS managed blockchain

OSCAL Website

- <https://nist.gov/oscal>
- Contains tutorials and collaboration information
- Resource page containing open-source tools and libraries that collaborators are developing
 - <https://pages.nist.gov/OSCAL/tools/#open-source-tools-and-libraries>
- How to collaborate:
 - Our effort is community driven: <https://github.com/usnistgov/OSCAL>
 - To contribute to the development of OSCAL: <https://github.com/usnistgov/OSCAL/blob/main/CONTRIBUTING.md>
 - Bi-weekly community meetings: <https://pages.nist.gov/OSCAL/contribute/#community-meetings>
- Publicly available resources:
 - Documentation: <https://pages.nist.gov/OSCAL/documentation/>
 - Examples: <https://github.com/usnistgov/oscal-content/tree/master/examples>
 - NIST SP 800-53 r4 & 5 catalog and baselines (XML & JSON): <https://github.com/usnistgov/oscal-content/tree/master/nist.gov/SP800-53>
 - FedRAMP Repository:
 - <https://github.com/GSA/fedramp-automation>
 - <https://www.fedramp.gov/using-the-fedramp-oscal-resources-and-templates/>
 - Tools:
 - OSCAL Java Library: <https://github.com/usnistgov/liboscal-java>
 - XSLT Tooling: <https://github.com/usnistgov/oscal-tools/tree/master/xslt>
 - OSCAL Kit: <https://github.com/docker/oscalkit>
 - OSCAL GUI: <https://github.com/brianrufgsa/OSCAL-GUI>
 - OMB OPAL: OSCAL Policy Administration Library (OPAL): <https://github.com/EOP-OMB/opal>
- OSCAL is internationally adopted.

Discussion

The Flexibility of OSCAL

- Phil Venables asked where she's seeing the balance between the use of OSCAL to be able to communicate control objectives between assessors, auditors, and implementers and in driving,

continuous control monitoring and instrumentation of controls according to an OSCAL catalog in the early-stage implementations?

- Ms. Iorga replied that they initially designed the models, having in mind the Risk Management Framework and trying to support the FedRAMP process. We realized that we have to be very dynamic so that's the reason for component definition models and others. One of the diagrams showed the alignment of the models with a Risk Management Framework at the bottom and who can use that. In a DevSecOps environment you can use OSCAL content to drive automation. The process can use OSCAL content, and the rules specified, to do testing and capture the results of that testing.
 - OSCAL is just the format that allows you to put in place whatever you want. Yes, it was initially controls driven, but we've seen from the community that they generated controls that were not in the catalogs that we are familiar with and demonstrating that the language allows them to do whatever they want.
 - The rules we're putting in place now allow you to go beyond just the catalogs for compliance. They allow you to demonstrate different aspects of your systems and bring all that information into the automation process.
 - We are also exploring how to capture the threats that could exploit identified vulnerabilities and what are the actions at the system level that you envision your system could mitigate? We have had initial conversations with Mitre to see how we can expand and integrate more support in that direction as well as developing language for future versions of OSCAL with enhanced features as the community is requesting.

Key Management

- Jessica Fitzgerald-McKay mentioned the key management in the data center use case and asked if OSCAL helps one assess the key management provided if you're a tenant on the network or is that not captured in the OSCAL capabilities?
- Ms. Iorga replied that OSCAL is the language. If you want to represent some processes or procedures in machine readable format to do validation against that information, you can do so. For example, certificates could be represented in machine readable format then tools can go and process that information during the testing of cryptographic modules to be able to look at the environment where the module is operating and aggregate that information

Further Clarification on Using OSCAL and Benefits of OSCAL

- The Chair said that he's trying to understand OSCAL usage scenarios. He presents a scenario and asks if it is a valid OSCAL scenario. The scenario: A team builds a system or deploys a virtual machine on infrastructure as a service provider, then associated with that, they have to build or acquire or install a set of tools that verifies the presence and configuration of the authorization, user authentication mechanisms, auditing controls, and then that tool set reports what it's found in the OSCAL language and that gets captured in some blockchain that somebody else can validate to see that they're complying with the requirements that apply to them.
- Ms. Iorga confirmed that is one possible scenario and indicated that if we want to learn more, they have one of the presentations demonstrating how OSCAL is generating information in machine readable format and using that information.
 - Using AWS config to monitor all the deployments in AWS environment, they process the information in OSCAL for the system, the system security plan, and check against AWS configuration, highlighting what is faulty and providing the assessment of a deployment with integration on AWS.

-
- In the pilot, we deploy a network with a service. All the information on the network was generated in machine readable format. We used AWS managed blockchain system security plan to look at the inherited controls, to document the controls that our service is going to inherit. We are also using OSCAL to document in the OSCAL SSP the controls that our service is implementing and then we document in there because we are using a CI/CD pipeline for the deployment. Those are static tests first, before we deploy on the environment.
 - We wrote our new chain code there because we used for hyper ledger fabric overwritten chain codes as was provided with NGAC with a NIST solution.
 - We document before we do the deployment of parts of the pipeline. We use the information that is in machine readable format that the tests are reading from, perform the test, verify that the configuration is as expected, and then, dynamically at runtime, check that the configuration is preserved and supports an ongoing process.
 - The Chair asked about the state of design automation for AWS, CI/CD tool developers, and others and if that is something where you'd include the OSCAL assertions as part of the system design language?
 - Ms. Iorga replied that AWS presented how they're adopting OSCAL. They are working with a GRC tool, but they're using that to generate information in machine-readable format in OSCAL and monitor the environment.
 - She mentioned that she's also working with Google to use OSCAL document the security posture of their systems and log information internally for them and for their customers. When a customer requests a service, Google can also deliver information such as, how to configure it, what are the controls that are inherited, and what is the customer responsibility, in machine readable format. In this way, they can build their system and all those pieces that they need are already documented.
 - In early evaluation of the benefits, we're showing that about 60% of the controls assessment in a cloud environment can be automated and for the others it is easier.
 - For FedRAMP validating packages, if they receive the package in machine readable format instead of 800 - 900 pages in Word or PDF, the benefit is huge as it cuts on the back-and-forth time and the validation can be done with tools that they developed in a matter of minutes. And the tools are made available for the code providers to do their pre-validation before they even submit the package.

OSCAL User Presentations

- The Chair expressed an interest in having an agency or vendor who is applying OSCAL in real world scenarios to come and talk specifics in terms of what OSCAL does for them and what it doesn't.
- Ms. Iorga mentioned that they recorded presentations from recent workshops and that she could share the videos with the board. She also mentioned that they would be hosting a mini event for the Air Force to present their efforts and would invite the board if there is interest

The Chair recessed the meeting for a 45 min lunch break.

GovCAR Overview and Use

Branko S. Bokan, Cybersecurity and Infrastructure Security Agency (CISA), Cybersecurity Division.

Introduction

- CISA was founded in 2018 as part of the Department of Homeland Security
- Specifically tasked with protecting the nation against cyber security threats

-
- The office Mr. Bokan works for, is tasked with protecting the federal civilian executive branch against cybersecurity threats.
 - Work with 101 FISMA agencies, making sure that federal information systems and data are properly protected.

What is GovCar?

- GovCar is a threat-based approach to designing cybersecurity architectures and a threat-based approach to analysis of cybersecurity infrastructure.
- Many CISOs do not have a methodology to determine where to invest their cybersecurity budget. They rely on:
 - Vendor recommendations
 - IG directions
 - “Best cybersecurity practices”
 - A few use risk management processes and risk policy
- In 2015, the DoD came up with this methodology
- Originally called “NASCAR” they had to change the name and went with GovCar
- DHS adopted this methodology around 2017 or 18 and modified it slightly.
- Two versions:
 - The Department of Defense version is not publicly available
 - The DHS version is unclassified, open source, and publicly available. Our intent is to share information with the general public and promote the use of this methodology.

Move to Stronger Risk Management

- Traditionally, risk management was done through compliance checklists using NIST 800-53 controls.
- The concept of cyber hygiene was introduced.
- Started looking at vulnerabilities but we've never really incorporated threat information and threat feed into that decision making process
- Threats are an “intelligence feed” we receive that change on a daily, sometimes hourly, basis.
- They are difficult or impossible to use for long term, multi-year cybersecurity decisions.
- Traditional definition of risk:
 - Risk = consequence (likelihood or impact) X vulnerability X threat
 - Had an idea of potential impacts and started looking at cyber hygiene vulnerabilities but never been able to incorporate the real threat information into this formula.
- The GovCar methodology allows us to consider the threat actions that organizations are facing and incorporate them into this decision-making process.
 - Allow us to look at the problem of cybersecurity from the standpoint of an adversary rather than a vendor.
- GovCar is a methodology developed to provide a threat-based assessment of cyber capabilities aka material capabilities and non-material capabilities such as 800-53 controls
- GovCar is vendor agnostic
- Looking at cybersecurity at an architectural level
- GovCar allows us to identify gaps in protections against the actual cybersecurity threats and identify where we need to focus for next year’s investments.
- GovCar also allows us to identify overlaps and see where we have multiple technologies or multiple capabilities protecting us against the same things,

Other Threat Methodologies

- GovCar isn't the first threat modeling methodology but none of them:
 - Incorporate the cyber threat framework covered below
 - Can be applied to architectures of architecture and validate the entire enterprise

How GovCar works

- All cyber-attacks can be divided into different stages of attack:
 - The Administration Stage
 - This is when they prepare their capabilities, learn the skills, gain the tools, and hire people
 - The Preparation Stage
 - The adversary or threat actor identifies a target and the target organization, evaluates that organization, conducts reconnaissance, and looks for vulnerabilities
 - The Engagement Stage
 - The threat actor tries to execute or exploit vulnerabilities that were found
 - Most of the time, things don't work and they go back into preparation stage.
 - Once in the organizational network, they establish a presence and move laterally.
 - Regardless of the purpose of the impact they want to maintain an ongoing presence.
 - There's a lot of back and forth and the stages are not sequential.
 - Each stage (he also refers to these as phases) has objectives and each objective has different ways or means of achieving those objectives called threat actions.

Cyber Threat Frameworks

- "Cyber Threat framework" is a generic term
- There are several different products on the market that have been used for many years such as Lockheed Martin's Kill Chain and Mitre Att&ck, which is used at GovCar.
- You can take any framework that that your organization is using and apply it in the same way
- These frameworks may have different groupings and may use different terms, but they all standardize the language used to describe cyber-attacks and enumerate all possible threat actions that an adversary has in their toolbox.
- We enumerate all the threat actions and different things that a threat actor can use and then we can pick any piece of our cyber architecture, if we understand where the capability is in the network and what it sees and does, we can start the evaluation of that capability
- Cyber Threat framework is a spreadsheet/table with a little less than 300 different threat actions that an average actor has in their toolbox

Marc Groman asked how this model framework fits with those that are already widely deployed and used, for example, the NIST Cybersecurity Framework and other frameworks that NIST has produced or standards that already complement that including standards put out by other entities? Does it fit right in? Does it complement? How does it work together?

Mr. Bokan replied that he's talking about cyber threat frameworks, not cybersecurity frameworks. There is no conflict; they all complement each other, and they all work together. He mentioned that as far as he understands, NIST doesn't have a cyber threat framework.

Mr. Groman clarified that the point of having a threat framework is to improve your cybersecurity posture and standardize vocabulary?

Mr. Bokan replied that the Cyber Threat framework is an input into the GovCar methodology. This is not something we developed. This is just something that we are reusing. The idea behind the cyber threat framework is to create the standardized terminology because we tend to use different terms to describe the same things when it comes to cyber-attacks, cyber-attack chains, or lifecycle of cyber-attacks. The purpose of using any cyber threat framework is to standardize terminology and have an enumeration of all possible threat actions. That's what it does in the GovCar methodology.

- Using the spreadsheet of threat actions, our capabilities, and different technologies that we want to evaluate, and we ask many questions
- We focus on protect, detect, and response functions of the NIST Cybersecurity Framework
- Uses subject matter experts working together. This takes some time.
- Protect: for each capability, we go over ~ 300 threat actions, and we ask:
 - Does this capability protect me?
 - Can this capability protect me against this threat action?
- Detect: Same process - we ask:
 - Can this capability detect this type of threat action?
- Respond:
 - Can this capability allow us to respond to this threat action?
- In cyber relevant time, protect-detect is relatively short. Respond can be significantly longer.
 - For example, if we want to know if we can go back into our logs, redo logs, in case of an incident where we have to do Incident Response, response times may last for hours, days and sometimes even weeks.

Matt Scholl and Katie Moussouris asked if, after looking at that mapping of prevention or protect, is there any root cause analysis done that could lead to re-architectures so that, instead of just protect, you could either prevent or be immune to such activity in the future? There may be architecture level changes that would prevent some of the threat activities that you're evaluating.

Mr. Bokan responded that GovCar looks at the bigger picture architectural capabilities that exist and the problem of investment, if I need to buy another tool, which tool is the highest priority for me right now? We do not evaluate tradeoffs. We do not evaluate individual configuration settings and do an analysis of what would happen if we flipped this switch. In theory, it could be done but it is not something that we have done.

Ms. Moussouris recognizes that this is out of scope for GovCar. She clarifies that she brought it up because of this question of investment. You're assessing the capabilities to see if you can you detect when a threat actor is "punching holes in the ship," but if you invest only in those capabilities and enhance the security, you're missing what caused the vulnerability in the first place. When you talk about that investment strategy, I get it that it's out of scope for what you're doing, but are you aware of other programs that take that overall investment strategy into account?

Mr. Bokan confessed that he doesn't know of any and agreed with Ms. Moussouris' premise. GovCar just tries to fix a small piece of this bigger picture, investments in buying technologies, so we're not buying things just based on vendor recommendations. GovCar is human based, not automated. We rely on subject matter experts who understand particular technologies and how they fit in the architecture and enterprise and federal networks.

The Chair brought up agencies going to zero trust and was wondering if GovCar would help in the move from perimeter-based network security to zero trust?

Mr. Bokan replied that zero trust is just a concept but, as you are considering the concept of zero trust and all the capabilities that are required to achieve that concept, GovCar can help with prioritization and make sure that you identify gaps and overlap.

Threat Heat Mapping

- The result of previously described analysis is a capability coverage map.
- Heat mapping
 - Provides a visual mapping of gaps
 - In his example, red means gaps in protection. These are the threat actions for which my current architecture, whether I'm looking at a single technology or all the technologies that are protecting my network, I'm not protected right now.
 - Allows prioritization using the heat mapping score for each threat action
- Additional analysis is then done to determine what to do about these gaps

Analysis To Date

- The GovCar program has been looking at different capabilities.
 - Worked closely with CDM program to help them determine capabilities
 - Looked at mobile architectures and what types of protections (EMMs, maps, enterprise mobility management, mobile application vetting, and Mobile Threat Detection) and type of protection they provide.
- Example: FedRAMP IaaS
 - Moderate categorization
 - Looked at FedRAMP controls to see how many threat actions the controls touch.
 - Slide shows a heat map
 - Gray boxes are threat actions that are currently not protected or FedRAMP controls don't touch
 - Showed that even a fully authorized FedRAMP infrastructure as a service, implemented as intended would only be protected against a very limited number of threat actions.
- Example: Mobile infrastructure.
 - Showed how the combination of enterprise mobility management, mobile application vetting, as well as mobile threat detection significantly improves the coverage against known threat actions.
 - Link to white paper available on request.
- Finding from past analyses: Top capabilities
 - Application device health check has the biggest coverage in terms of the number of different threat actions it can protect against.,
 - Ability to discover a new device coming on your network, ability to check the health of that device before it connects to the network, and ability to quarantine that device,
 - Application Allow Listing (a.k.a. Whitelisting) is one single capability that has the most significant coverage against the highest number of individual threat actions.
 - It has significant coverage against almost 40 different threat actions.
 - Implementing application allow listing would have the biggest impact

OMB Max Repository

- Max.Gov Home: <https://community.max.gov/x/FqVIY>
- Technical Annex Documents – Restricted Access: https://community.max.gov/x/_9n7YQ

Discussion

Scoring of Capabilities

- Marc Groman mentioned that the Australian Defense Security Directorate had their top four controls and that application allow listing was at the top. He then asked if they have done a notional scoring of those, versus maybe full FedRAMP ATO versus, maybe some idea of best practice/ zero trust?
- Mr. Bokan replied that zero trust is not a capability but yes, they have done analysis of a lot of these capabilities. He referred to the OMB Max Repository links for more info. This methodology allows us to look at these capabilities from the standpoint of an adversary and allowed us to validate what some others have suggested. In some instances, we've demonstrated that those controls or technologies or tools are not as useful as some vendors may claim.

More on how GovCar works and integration with existing standards and frameworks

- Mr. Groman asked how does this tie into and integrate with standards that are already widely deployed across the government? If he's working with people who are already using the mobile security guidelines from NIST, and implementing 800-53 and the Cybersecurity Framework, how would he explain to them where this helps them? Where this fits into their risk assessment, security and control assessment process so it's adding value to the end goal of cybersecurity?
- Mr. Bokan replied that the purpose of this methodology is for review of cybersecurity architecture to determine where you need to invest. None of the existing NIST guidelines or standards address purchasing technologies. The GovCar analysis addresses what are the tools that you need to invest in?
- Matt Scholl added that his understanding is that FedRAMP adjusted their requirements based on GovCar analysis results. They reduced the number of individual controls for one of their high baselines and they've created a tailored baseline above the 800-53 minimum.
- Mr. Groman clarified that GovCar is a tool that would be used for tailoring? An entity has done a system assessment to determine low, moderate, high. They put their controls in place and want to do assessments of their controls for continuous monitoring. They can use GovCar for tailoring?
- Mr. Scholl replied yes, because part of tailoring is deciding what else you might need to meet the risks that you're facing, similar to what Frank was saying about investment. Absolutely for assessing and tailoring decisions or even in POA and M prioritization.
- Mr. Groman wanted confirmation that NIST documents do help with investment and Mr. Scholl confirmed that they do but at a minimum baseline and it's focused on asset rather than threat activity. GovCar provides another dimension of information around threat.
- Mr. Groman suggested that this is something worth discussing. To him, the implementation of a control is to guard against a particular threat.
- Mr. Scholl replied that is correct and this is also a tool that helps you identify those best bang for your buck tools that you might get. There are a lot of different potential utilities and use cases.
- Kevin Stine added putting controls in place based on an assessment of risk and threat is an important part of a risk assessment and these tools can help support that. The NIST guidelines and other resources do talk to these capabilities and make recommendations at a technical, process, and policy level. GovCar fits within the discussion of threat assessment as part of a broader risk assessment to inform decisions agencies are making.
- Mr. Groman commented that he thinks it goes to understanding where the pieces fit. This fits into a risk management framework because you have to understand your threat actors to understand your risk and then when you mitigate risk, you are taking steps to mitigate this full range of threats as part of that.
- The Chair agreed that you don't do it in isolation. You make the investment because you're managing risk and the 800-53 for example, gives you a large catalogue of things to do. But which of those pays

off is something that it's important to consider in deciding what controls to actually implement? He suggested that it may be possible for NIST to look at the at the 800-53 controls against a general or notional agency environment and readjust the baselines or provide some additional guidance on how to select or how to prioritize.

National Initiative on Cybersecurity Education (NICE) and Workforce Update

Danielle Santos, NIST

Karen Wetzel, NIST

Introduction

- Danielle Santos is the NICE Lead for Communications and Operations.
- Karen Wetzel is the Manager of the NICE framework

NICE Strategic Plan and Implementation Plan

- NICE Strategic Plan:
 - Five-year strategic plan with five goals.
 - One of the goals is on expanding the use of the NICE framework
- Implementation Plan:
 - Community of public and private sector participants helped develop the plan
 - Has several strategies that build off each objective in the NICE framework.

Goals for NICE framework

- Goals are:
 - Documenting and disseminating successful uses of the NICE framework,
 - sharing examples of how people have used the NICE framework, and
 - building a resource center with materials that people can use.
 - Aligning the framework with other relevant cybersecurity standards, best practices, and guidance,
 - Establishing a process for regular reviews and updates for the NICE framework,
 - Exploring tools to help people access and use the framework,
 - Identifying areas that might change with new technologies, such as automation, and
 - Expanding international outreach.

The NICE Framework

- NICE framework establishes a consistent lexicon to clearly share information about cybersecurity work.
- This common language helps us to work with employers, subject matter experts, and education and training providers, to identify specific tasks, knowledge, and skill (TKS) statements.
- TKS statements are used to define cybersecurity specific workloads and competencies.
- The NICE framework can be used by employers to track and develop cybersecurity workforce capabilities and to establish processes from hiring to development and retention.
- A study conducted by the InfoSec Institute found that organizations that were aligning their job descriptions to the NICE framework were significantly more likely to have well defined roles and descriptions, and they had a 57% increase in recruiting satisfaction.

The NICE Framework Evolution

-
- People, processes, and technology mature and change, and the NICE framework evolves in order to more accurately reflect both current and upcoming cybersecurity workforce competencies.
 - 2017: The NICE framework was first published.
 - Started as a federal cybersecurity workforce effort
 - Expanded as a national framework to address the needs of public and private sectors
 - December 2020: First revision
 - Updates to incorporate improvements based on community suggestions.
 - The title was changed because the NICE framework definition of the cybersecurity workforce is expansive, to include those whose primary focus is on cybersecurity as well as those in the workforce who need cybersecurity related knowledge and skills to perform work in a way that enables the organization to properly manage the cybersecurity related risks to the enterprise.
 - Beginning of 2021:
 - Worked with the NIST Privacy Engineering Program to develop a TKS guide
 - Used that publication to begin our review of those core TKS statements, categories, work roles, and competencies.

NICE Framework: Attributes

- Evolution is to ensure the NICE framework remains:
 - Agile: Enables organizations to keep pace with a constantly evolving ecosystem
 - Flexible: The application of the NICE framework can adjust to support individual organizational needs
 - Interoperable: No one size fits all solution, the consistent use of terms enables organizations to exchange workforce information with that common language.
 - Modular: The structure and foundational content of the NICE framework enables communication with other workforces, for instance our privacy workforce, within an enterprise and across organizations or sectors.

NICE Framework History

- Beginning of 2021:
 - Launched the NICE framework User's group to make sure there's a place for regular conversation, engagement, sharing and input around the NICE framework, and
 - Launched the NICE framework Success stories to highlight applications of the framework.
 - Soon after published the TKS authoring guide and a first draft of initial informational reports on the NICE framework competencies for review and comment.
 - Started with a series of virtual workshops to engage the community and subject matter experts around measurement competencies on how education and training providers interact with the NICE framework on two new areas for development and inclusion:
 - Operational technologies and
 - Cybersecurity awareness.
 - End of the year published three new items for comment including:
 - A second draft of the competencies NISTIR,
 - A preview of our upcoming public comment process, and
 - Refactored ability statements which had been deprecated on our last revision.
 - Also released a machine-readable JSON version of 2017 data.
- This year we started with more stakeholder conversations,
- Working to ensure the NICE framework will support both current goals and future ones.

NICE Framework: Updates

- The NICE framework has two pieces:
 - The NICE framework publication
 - Describes the framework structure and how it can be used, and
 - The data that supports it.
 - Competencies,
 - Work roles, and
 - Task, Knowledge, and Skills (TKS) statements.
- Have completed our initial review of the knowledge and skill statements to align with our TKS authoring guide and address duplications and redundancies
- We expect to put those out for comments in the next couple of weeks.
- Next, we're looking at potential updates to the work roles and categories
 - Need to arrange work roles to address feedback about changes needed for broad applicability
- Then start looking at the 1000 task statements and aligning the knowledge and skill statements to each of those tasks.

NICE Framework: Competencies

- The need for competencies is driven by:
 - The shift in recruiting practices, changing from a degree-based and competency-based hiring to expanding the applicant pool; identifying and bringing in individuals capable of performing the work in emerging areas with new technologies or with new kinds of threat vectors that may be identified.
 - The desire to have a different avenue for identifying people with capabilities in those areas.
 - Support for an assessment-based approach to hiring and promotion, to identify current gaps and future needs, and to align training and education to organizational goals.
- Competencies serve as a bridge between the employers, their needs, and the training and education providers who are translating that into ways to train people to be prepared for the cybersecurity work defined by the NICE framework.
- Currently working on a report on the scope and sufficiency training efforts to measure proficiency of cybersecurity content in the NICE framework.
 - Reaching out to various other agencies to learn about their efforts in this space to hear their recommendations.

Competency Areas vs. Work Roles

- Competency areas are:
 - A new way of applying the building blocks of the NICE framework.
 - Additive and complementary to the work roles
 - learner focused, looking at the person and their capabilities and serves as a mechanism for organizations to assess individuals in a particular domain
- Work roles are
 - More focused
 - A defined group of tasks someone's responsible for; a capability that an individual can demonstrate,
 - Something that can help define positions and responsibilities.
 - Work roll assessments are typically done at a fairly small, task level.

NICE Framework Competency Areas

-
- Came out with a draft list in March
 - Competency areas measurable clusters of related TKS statements correlating with performance on the job and improved through education, training, or other learning experiences.
 - Competency areas are grounded in a workplace context.
 - What is the performance on the job?
 - The application of the learning, not just theoretical knowledge.
 - They offer a higher-level perspective on cybersecurity work to define it broadly.
 - They allow for the inclusion or removal of specific statements in response to shifting needs.
 - Three ways competencies could be used:
 - As an overlay on work roles where, in some cases, additional capabilities may be needed to effectively fulfill a role.
 - A person responsible for more than one role may need a competency across both.
 - The competency serves as common ground for communication and coordination between people. For example, when a specific sector or domain expertise is needed for a role or for staff who don't work in cybersecurity primarily but need cybersecurity expertise to mitigate risks.
 - Students, job seekers and employees can use a competency as a starting place for gaining knowledge around a certain domain area, or when someone wants to develop higher level expertise in an area.

Identifying NICE Framework Competency Areas

- Work has been guided by workforce investment principles and guided by multiple community partners.
- We engage with those different areas across federal government, private industry, and various stakeholders to ensure they are useful and reflective of needs.
 - We had several meetings with individual groups and organizations and a virtual workshop to gain additional feedback.
- Started by looking at the 2011 OPM Competency Model for Cybersecurity.
 - We compared them to our existing work roles and our specialty areas, which were deprecated in our last revision, and making sure that we're not going to be doing a competency area that's the same as our work role and cause confusion.
 - Coming up with a refined list that aligns with some existing models, such as the cybersecurity framework, the risk management framework, 800-53 and related resources, and other relevant models, looking at the most common things, how we align to those, and make sure that they are reflected in our competency areas.
 - Put out an early draft in March of last year, and received a lot of feedback

NICE Framework: New Platform

- Moving the NICE data outside of manually updated spreadsheets into an online platform to expand its use and application
- Phase I
 - Have content in a browsable, searchable, and exportable fashion, and supporting machine readable content.
 - Will enable use of the framework, allowing people to bring it into their own tools.
- Future phases:
 - Still being defined,
 - Capabilities to further strengthen tool development and support potential customization,

-
- Connections with other workforce frameworks and support integrated mappings
 - We're going to be having several community conversations on this and are open to input.

NICE Framework: Public Commenting Tool

- Currently have public commenting where people send us emails with their information when we have open calls for comments around specific items.
- Having a public commenting tool is a new and additive way of asking for feedback to suggest changes to the NICE framework data.
- This tool is going to help us identify and incorporate emerging areas of need.
- Tool is additive to our existing update processes such as through the defined public comment periods and stakeholder engagement.
- Following the public comment model that's already been established by 800-53 and managed by NIST principles for standards and guidelines development, including openness, balance, and continuous improvement.
- This tool will be open to all NICE framework users and submissions can be made at any time.
 - We will have defined review and publication periods.
 - Proposed changes may be for new or existing data, and we will continue to follow our established practices of engaging subject matter experts as part of the review process.
- Process steps when change is submitted:
 - Proposed change goes through a review process, working with subject matter experts in the area and seeing how it relates to other changes that might happen, what kind of impact it might have,
 - We make it available in a sandbox
 - Final release at a defined time.

What to Expect

- New content:
 - Operational Technology: updating to align with the newly revised 800-82.
 - We're hoping to put something out in spring
 - Making sure that there's an alignment with the vast community of interest in this space.
 - Cybersecurity Awareness Role: aligns with efforts to update 800-50 and 800-16.
 - Both suggestions were brought to us by our communities
- Things to come in 2022:
 - Resource development including a quick start guide, and guidance for individuals in specific work areas, who might need to have a knowledge of how to use the NICE framework for specific topic areas.
 - Updating the NICE framework Resource Center,
 - Website has links to a lot of tools, guides, and support resources for educators,

Stakeholder Engagement

- Our mission is to build a community working together with academia, industry, and government to build broader communities for the work that we're doing.
- Also want to make sure the NICE framework is useful for the people who are using it.
- The resource center is a web page we've set up with materials including:
 - The current versions of the NICE framework, that data's currently in a static Excel spreadsheet version

-
- Supplemental materials such as a playbook for workforce frameworks that can serve as a guide for others
 - TKS authoring guide
 - We share these resources by audience to hopefully make it easier for them to find.
 - Resources are for employers, education and training providers, and learners.
 - A resource for education and training providers – the NICE challenge project which is a teaching and testing tool for students to be able to show their capability to do tasks that are in the NICE framework.
 - Two Example Applications and Uses
 - Success stories - quick, two-page summaries, why and how an organization has used the NICE framework.
 - We have these stories from large and small businesses, academic institutions, and international organizations that describe the drivers behind why they use a NICE framework and the benefits.
 - Framework and focus interviews which focus on the people doing the NICE framework, their workloads in relation to the NICE framework, and showcase their jobs. Each interviewee talks about how they got to their role, the credentials they have or don't have, the teams that they're on, what they do, and how they got there.

Community Engagement

- Interagency Coordinating Council Monthly Meeting is:
 - A group of our federal departments and agencies who are focused on building the National Cybersecurity workforce,
 - Meet monthly to coordinate programs, collaborate, and share information.
- Community Coordinating Council is:
 - Open to anyone who wants to join.
 - Have several working groups and communities of interest within this group:
 - A group focused on career discovery uses the NICE framework to describe the different careers available for people and help them identify how they can get into those careers.
 - A standing agenda topic is called the NICE framework feature. This is where we feature a guest speaker who comes in and talks about how they use a NICE framework.
- NICE Framework Users Group.
 - Set up as a forum for anyone who has questions about the NICE framework, wants to share their experience, or wants to share feedback with us.
- Ad hoc meetings with our stakeholders as needed.
 - Used to coordinate and create the ecosystem across employers, education and training providers, and learners / job seekers to create that ecosystem.
- Mostly done domestically, but we don't exclude our international partners.
 - Over 54 countries looked at the NICE framework last year.
 - Working with Department of State partners getting translations done of the NICE framework in Spanish and Portuguese.
 - Have a few others in progress as well.
 - We have regular meetings with international organizations and groups who want to learn more about the NICE framework, how they might use it or adopt it for their own countries.

-
- Have a series of activities or events, such as the US cyber team preparing themselves to compete in the international cybersecurity competition. They're using the NICE framework to make sure they're training and preparing themselves to meet certain cybersecurity areas.
 - Last fall we partnered with our annual conference coordinators to put on the regional initiative for cybersecurity education targeted for the Latin American region.
 - Working with the Department of State, held two workshops for countries to talk about capacity building
 - NICE framework Resource Center link: www.nist.gov/nice/framework

Discussion:**Supporting Binding Operational Directives**

- Katie Moussouris asked if their partnership with CISA has included work that supports binding operational directives (BODs)? For example, the mandatory patching of known exploited vulnerabilities and the emergency directive that that came forth for the Log4J.
- Ms. Santos replied that she isn't familiar those, but they do work with all agencies and with the public to identify roles or gaps in the NICE framework.
- Ms. Wetzel added that they do engage with CISA but not at that level. She commented that this question makes her think that they may need to be more active in understanding them and that she will follow up on that but, at this point, that's not done.
- Ms. Moussouris added that CISA is not necessarily going to be the authoritative source to know what roles are required to support those operations. They may need to go more broadly for help and that she is willing to help them.

Coordination with NAPA

- The Chair asked if they coordinate with NAPA Cybersecurity, Defense Education and Training Branch strategy plans, priorities and so on?
- Ms. Wetzel replied that they haven't, but they are open and would welcome that kind of coordination. She mentioned that the NICE Director, Rodney Petersen would likely have more information.
- Matt Scholl mentioned that Mr. Petersen has met with NAPA at least twice with some extended meetings to establish their understanding of NICE.
- Ms. Santos confirmed they meet with NAPA regularly. Regarding strategies and objectives, they work with their interagency group, including CISA, to develop the strategic plan.

The Chair recessed the meeting for a 10-minute break.

NIST Cybersecurity and Privacy Update

Matthew Scholl, NIST

Kevin Stine, NIST

Cybersecurity Framework (CSF) Update

- Four years since last update
- In early stages of an update, starting with an RFI in the Federal Register to get feedback from the community because:
 - Technologies, the threat landscape, and policy landscape have changed and evolved
 - To make sure that the framework continues to be a useful tool that keeps up.
- The RFI really focuses on three primary areas:

-
- What's working and what's not. Are there areas to improve in either structure, content or complementary derivative / external resources that help organizations use the framework in more meaningful ways?
 - Alignment and harmonization of cybersecurity language and taxonomy between CSF and other NIST guidelines, frameworks, resources published since the last update in 2018 such as the Privacy Framework, the Secure Software Development Framework, and supply chain risk management activities.
 - How do they all fit together and what is the role of the Cybersecurity Framework in helping to bring along that alignment that harmonization?
 - How are organizations, federal or non, using them to enhance their ability to better manage different types of risk?
 - Cybersecurity and supply chains.
 - Understand the resources that folks find valuable and the gaps to work with the community and address those gaps
 - To what degree is the supply chain work integrated in the framework today and if it needs to be increased
 - Gather info on the need for a Supply Chain Framework:
 - Incorporate software supply chain security work related to the executive order
 - Possibly expand to hardware and firmware information technologies and operational technologies.
 - Broad-based set of questions around supply chain to help us get smarter and chart a path that will provide value to the entire community.
 - Continue to produce resources related to the framework, outside of this update process.
 - Issued a final version of a cybersecurity framework profile and quick start guide for ransomware risk management.
 - Covers prioritizing cybersecurity outcomes in the context of ransomware.

Post Quantum Cryptography

- The team seems to have come to a consensus around deciding the finalists and anticipate making the announcement this month.
- Working on addressing a few bureaucratic loops first
- While this announcement will be big, there is still the follow-on work to create specific implementable standards with known parameters
- Need to ensure people understand the difference between the announcement of the winner and the finalization of a standard
 - Commercial implementations by the government will still need that final standard / special publication.

The Chair asked when the team says, “this is it” and you make that announcement, are vendors who are trying to develop unlocked to start coding?

Mr. Scholl replied no and indicated that is one of his concerns and he needs some assistance with. If vendors do that there will be a risk that they might implement with a different set of specific parameters than what we specify in the implementing standard or specification. We still might, and probably will, tweak the implementation.

The Chair clarified that it would be uncertain enough so they're not going to be able to write code yet.

Mr. Scholl replied that is correct. It is possible the final standard might use an entirely different algorithm.

Lightweight Encryption Algorithm

- Continuing to finalize a selection for a new lightweight encryption algorithm.
- The security strength of the lightweight algorithms will be equivalent to something like an AES 128 implementation.
- The “lightweight” will be in either size or latency
 - Size: will potentially accept a punishing hit in size for really good throughput or latency.
 - Latency: might accept horrific latency to get greater efficiencies in size
- Would like to find one algorithm that will have the flexibility in its implementation to do both.

Identity

- Updated PIV card specification to allow for a federation of identity tokens to be used
- Adding equity and inclusivity to ensure access to identity services by the largest representative population so they can take full advantage of our digital economy.

Workforce Recruitment and Retention

- Beyond recruitment, NIST is focused on providing a significant amount of job satisfaction which then directly relates to be able to keep the highest talent. We come to work at NIST because we have a purpose to inspire trust.

NIST SP 800-63 Digital Identity Updates

- Updating the Digital Identity Guidelines, NIST SP 800-63.
 - Anticipate a draft out for public comment of all the volumes within the next quarter.
 - A lot of attention is placed on identity proofing
 - Want to give providers many different options at different assurance levels to allow organizations to advantage of balancing those different options against the risks and mission needs and then have a robust discussion of compensating controls

Implementation of EO

- Issued the final version of the Secure Software Development Framework (SSDF), version 1.1.
 - It is responsive to section 4E of the executive order, which is an assignment for OMB to issue policy related to federal procurement of secure software 30 days after NIST issues SSDF.
 - Last Friday, OMB issued a policy statement on enhancing the security of federally procured software
 - Indicates that agencies must begin to adopt the SSDF effective immediately
 - Can tailor it to their risk profile & mission,
 - OMB recognizes that attestation of those practices can be challenging for both industry as well as how government asks for them
 - NIST is hosting a workshop on behalf of on March 23 with a focus on vendor attestation of secure software development practices and on a consistent agency process for requesting those attestations,
 - Through that workshop, OMB has issued a series of questions to help prompt discussion.
 - Requesting position papers and information in advance of that.
 - Papers are sent to OMB, the Office of the Federal CIO.
 - We expect this will attract a lot of attention as the discussion at the workshop and the input provided through that call for papers will inform implementation guidance

National Academy Review of NIST Research Program

-
- The focus was not on the cybersecurity divisions, but recommendations are applicable to our work such as ensuring NIST can make its resources more digestible, use plain language, etc....
 - Using short video clips on different topics to distill technical topics into something more relatable that won't take up a lot of time.
 - Have videos on ransomware, phishing, and multi factor authentication.
 - Can share a link to those. Would like to get feedback on those and additional types of resources we can put out to help reach a broader audience.

“Freeing” NIST data

- Making NIST data more available through the variety of PDFs that we issue
- Making sure we can take the data provided to the broader community publicly in different ways so that it can be used, for example:
 - Offer data in machine readable format, ingested through tools
 - Starting with frameworks including the Cybersecurity Framework, Privacy Framework, Secure Software Development, and the NICE workforce framework,
 - Providing that data in an online format that's searchable, that's downloadable, that can be sliced and diced in different ways, and be ingested by machines, will allow new innovative opportunities for folks to work with the data in different ways including:
 - Demonstrating different alignment and linkages between the data,
 - Align with specific controls and 800-53 and potentially even associate the different work roles and the different framework outcomes and controls to data within the National Vulnerability Database as well.
 - Being able to demonstrate how these things align, relate, and to improve and update them in a much more agile manner.

The Chair recessed the meeting for a 14-minute break.

Final Board Reviews, Recommendations and Discussions

Steve Lipner, ISPAB Chair

Lessons Learned

- Don't schedule half-hour slots
- Better alignment of speakers and topics to ISPAB's purpose
 - Ensure speakers recognize ISPAB board's experience and knowledge
 - Maybe change the format of the speaker slots – less lecture, more Q&A
 - Understand the mission of the agency represented by the speaker, for instance Mr. Groman pointed out that no amount of time for CRS would have enabled us to dig down on some of the issues we raised.

Topics for Future Meetings

- How GovCar fits into the control selection agency architecture and FISMA risk management process.
 - Topic raised by the Chair
 - Help agencies understand how GovCar fits with the NIST cybersecurity framework and other models. What's the “big picture?”
 - Are there any alignment or harmonization issues that need to be addressed?
 - Are there norms coming from the GovCar effort that should be adopted?
 - Does GovCar help in assessing new and emerging technology investments?

-
- Is there an ongoing mapping of GovCar to NIST standards/guidelines?
 - How NIST supports new initiatives
 - Topic raised by Katie Moussouris
 - As new initiatives are spun up, do they get a NIST liaison?
 - Is there someone assigned or detailed to them at these other federal agencies, who can help them map to NIST standards and guidelines, i.e., an ongoing mapping and integration project?
 - Ms. Moussouris commented on the apparent disconnect between NICE and what CISA's new role requirements might be for some of the directives
 - Bi-lateral and one-way mappings in NIST
 - Education Initiatives around Open Source
 - Topic raised by the Chair
 - NSC initiatives
 - Other Solutions to Solving Cybersecurity Workforce Issues
 - Topic raised by Phil Venables
 - Focusing on productivity
 - Identifying activities that can and should be automated
 - “Getting non-cybersecurity people to do the right thing”
 - Update from CISA on timing and criticality decisions and the Regulator’s forum
 - Topic introduced by Katie Moussouris and added to by the Chair and Marc Groman.
 - There's been disparate guidance coming from different federal agencies on dealing with vulnerabilities
 - Example: Patching timing where, for the same vulnerabilities, differing timing requirements and mandates are coming from CISA for federal agencies vs FTC for private companies.
<https://www.ftc.gov/news-events/blogs/techftc/2022/01/ftc-warns-companies-remediate-log4j-security-vulnerability>
 - The role of the Regulator’s forum
 - What is their decision process?
 - Are these types of conflicts part of that process?
 - How do they determine criticality?
 - How does CISA manage the vulnerability list?
 - CISA has started a living list of vulnerabilities that are under active exploitation, and they seem to be adding to this list
 - How sustainable is this given that we've had lists of vulnerabilities before and not really gotten a straight answer on how to deal with the eventual fatigue?
 - How do they (or do they) work with developers in building capacity to address application vulnerabilities?
 - Optimizing mitigation strategies to address an agency’s true attack surface: balancing vulnerability criticality with exploitability, and discoverability. Going beyond CBSS.
 - Helping governments and organizations with best practices to become ready and resilient in the wake of possible attacks (suggested by Arabella Hallawell)
 - Supply Chain Security Updates (suggested by the Chair)
 - GAO study on federal-wide incident response efforts
 - Topic suggested by the Chair
 - The new review is forensically looking at how agencies are complying with the federal guidance. It will be government-wide but focus on those nine agencies that were impacted and how they are managing their network

- NCCoE pilot on applying the Secure Software Development Framework
 - Topic suggested by the Chair
 - NCCoE is wrapping up a demonstration project or pilot aimed at best practices for applying this secure software development framework.
- Applications of OSCAL
 - The Chair expressed an interest in having an agency or vendor who is applying OSCAL in real world scenarios to come and talk specifics on what OSCAL does for them and what it doesn't.
- Contact Matt Scholl via email with additional issues or ideas for future meetings.

Letter about the Government in Open Source

- The Chair reminded the board about the letter sent a while ago regarding the government in open-source. He indicated that it may now be O.B.E.
- No new letters were identified in this meeting

Next Meeting

- The July meeting will, hopefully, be in-person in Washington, DC.

Motion made and seconded to adjourn meeting. The Chair thanked everyone for their participation and adjourned the meeting at 4:16 p.m. ET.

INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

Minutes, March 9 and 10, 2022

Page 59

ISPAB – March 9 and 10, 2022		
Last Name	First Name	Affiliation
Board Members		
Lipner	Steve	SAFECode (Chairperson)
Baker	Brett	NARA
Fanti	Giulia	Carnegie Mellon University
Fitzgerald-McKay	Jessica	NSA
Gattoni	Brian	DHS
Groman	Marc	Privacy Consulting
Hallawell	Arabella	WhiteSource
Maughan	Doug	NSF
Miller	Essye	Executive Business Management (EBM), LLC
Moussouris	Katie	Luta Security
Venables	Philip	Google
NIST Staff		
Brewer	Jeff	NIST
Scholl	Matt	NIST
Carlson	Caron	HII
Salisbury	Warren	HII
McConnell	Andy	HII
Lurie	Kirk	HII
Speakers		
Romine	Chuck	ITL, NIST
Inglis	Chris	ONCD
Mital	Amit	NSC
Franks	Jennifer	GAO
Chambers	Richard-Duane	Senate Committee on Commerce, Science, and Transportation
Beezer	John	Senate Committee on Commerce, Science, and Transportation
England	Maryasa	Senate Committee on Commerce, Science, and Transportation
Hau	Alice	Senate Committee on Commerce, Science, and Transportation
Mazol	James	Senate Committee on Commerce, Science, and Transportation
Jaikaran	Chris	CRS
Chenok	Dan	NAPA
Evans	Karen	NAPA
Jaggar	Sally	NAPA
Iorga	Michaela	NIST
Bokan	Branko	CISA
Santos	Danielle	NICE
Wetzel	Karen	NICE
Scholl	Matthew	NIST
Stine	Kevin	NIST
Registered Attendees		
Bab	Omer	Israeli Government
Banks	Chiara	NSA
Barrett	Catherine	Mitre
Beutel	Richard	Cyrrus Analytics LLC
Boeckl	Katie	NIST
Boyle	Mike	NSA
Cantu	Julie	GSA
Castro	Safira	IBM
Cloward	Lauren	Western Governors Association
Didiuk	Lauren	DOC

INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

Minutes, March 9 and 10, 2022

Page 60

Doyle	Harry	HD Healthcare
Escoto	Willmary	Access Now
Fincke	Chet	Gigamon
Friedman	Sara	Inside Cybersecurity News
Fu	Kevin	HHS
Funn	Kelby	SEC
Guirrerri	Joseph	Guirrerri cyber Consulting
Heyman	Mat	NIST
Hilder	Brandon	Treasury
Ignaszewski	Kathryn	IBM
Jaggar	Sally	NAPA
Johnson	Derek	Cyber Risk Alliance
Jordan	Roger	SAIC
June	Kimberly	Maryland State Government (MSDE)
Kerben	Jason	State
Kumar	Geeta	Telos
LaSalle	Connie	NIST
Leipold	Jack	SSA
Lewey	Jonathan	Notorize.com
Lum	Brandon	Google
Lyles King	Tauriana	AT&T
Mahn	Amy	NIST
Manners-Weber	David	DOC
Matthews	Jeanna	Clarkson University
Mazmanian	Adam	GovExec
McCabe	Karen	IEEE
Meier	Kaye	Masimo
Mitchell	Charlie	IWP News
Neboshynsky	Andrew	Maryland State Government
Okunade	Olijade	Maryland State Government
Pascoe	Cherilyn	NIST
Perera	David	Mlex (lexis nexis company)
Quinn	Sean	IBM
Ross	Renault	RNSC Technologies
Santillan	Olive	Telos
Sapp	Lanis	Hillsborough County (FL) Public Schools
Sedgewick	Adam	NIST
Shah	Alpesh	IEEE
Snodgrass	Harry	Leading Edge Training
Sokol	Annie	NIST
Souppaya	Murugiah	NIST
Steib	Cara	NSA
Stenger	Charlie	Tenfold Security
Suh	Paul	NIH
Tanya	Brewer	NIST
Throneberry	Sandee	LMCO
Tull	Meredith	Booz Allen Hamilton
Tupitza	Charlie	Future Feed
Underwood	Rosa	GSA
Walther-Puri	Munish	NYC Cyber Command
Weinberger	Peter	Google
Wink	Sean	NOAA
Wissolik	Erica	IEEE

INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

Minutes, March 9 and 10, 2022

Page 61

Wood	Jennifer	Luta Security
Wood	Daniel	Treasury
Yaniv	Orlie	Gigamon