INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

Established by the Computer Security Act of 1987
[Amended by the Federal Information Security Modernization Act of 2014]

MEETING MINUTES

June 24 and 25, 2020

Virtual Meeting Platform: BlueJeans

Board Members	**Board Secretariat and NIST Staff**
Steve Lipner, SAFECode, Chair, ISPAB Brett Baker, NRC Chris Boyer, AT&T Akilesh Duvvur, IBM Brian Gattoni, DHS Marc Groman, Privacy Consulting Arabella Hallawell, NETSCOUT Systems Patricia Hatter, Palo Alto Phil Venables, Goldman Sachs	Matthew Scholl, NIST Jeff Brewer, NIST Caron Carlson, Exeter Government Services LLC Warren Salisbury, Exeter Government Services LLC

Wednesday, June 24, 2020

Welcome and Opening Remarks

Steve Lipner, Chair, ISPAB, Executive Director, SAFECode

[Just prior to the official start of the meeting, Matthew Scholl, NIST, explained that this was the first time the ISPAB was meeting virtually. Participants were working through some of the logistics, connectivity challenges, and other technical kinks. He also announced that slight changes were going to be made to the Day 2 (Thursday) schedule.]

The Chair welcomed everyone to the meeting at 9:04 a.m., Eastern Time. He announced that three new members had joined the board: Akilesh Duvvur, IBM, Arabella Hallawell, NETSCOUT Systems, and Phil Venables, Goldman Sachs. They briefly introduced themselves.

The Chair explained that the Board would be catching up on topics originally planned for discussion at the March meeting [which was canceled] and covering new topics as well. Members were encouraged to ask questions and share opinions.

Welcome and ITL Update

Dr. Charles H. Romine, Director, Information Technology Laboratory (ITL), NIST

The Chair welcomed Chuck Romine, Director of ITL, NIST.

Dr. Romine explained that NIST depends on the advice of the ISPAB, and he provided an update on NIST's work:

Changes in ITL Leadership:

The most significant change since the last meeting is the retirement in May of Donna Dodson. She was a pivotal part of NIST, working as Chief Cybersecurity Advisor, NIST Fellow, and Director of the National Cybersecurity Center of Excellence (NCCoE). She is a finalist for a Samuel J. Heyman Service to America Medal. Kevin Stine stepped in as Acting Chief Cybersecurity Advisor. Jeff Greene is the new NCCoE director, having joined in February after serving on ISPAB.

Privacy Framework:

The Privacy Framework was released in mid-January after nine workshops with thousands of attendees. The release was followed by a webinar to promote the Framework's adoption. It is a voluntary tool that can be used to manage risk, help organizations meet regulatory obligations, and strengthen accountability. The Board would like to hear an update at the next meeting.

Other Newly Released Documents include:

- SP 800-171 Rev 2: Protecting Controlled Unclassified Information in Nonfederal Systems
- Secure Software Development Framework (SSDF)
- CSF Manufacturing Profile (NISTIR 8183 Rev 1 draft)
- SP 800-207: Zero Trust Architectures draft released for public comment
- SP 800-53 Rev 5 draft released for public comment
- 5G Cybersecurity Federal Register Notice seeking formal industry collaborators

Voluntary Voting Standards and Guidelines, Version 2.0 (VVSG 2.0):

NIST led the Technical Guidelines Development Committee for the new VVSG 2.0. NIST, EAC, DHS/CISA, and the FBI jointly issued the "Risk Management for Electronic Ballot Delivery, Marking and Return" report.

EO on Strengthening National Resilience through Responsible Use of PNT Services:

The Executive Order directs the Department of Commerce and other agencies to work with the private sector to identify and promote responsible methods of using PNT (Positioning, Navigation, and Timing) services that appropriately manage risk. A Request for Information (RFI) was issued May 27, and a webinar was hosted June 4.

Industries of the Future:

The five pillars of the Industries of the Future effort are: 1) quantum information science, 2) 5G and advanced communications, 3) artificial intelligence, 4) advanced manufacturing, and 5) biotechnology.

Encryption:

The Post Quantum Cryptography work is moving to round 3 selections soon. In Lightweight Encryption, the selection is down to 32 potential candidate algorithms. Analysis is ongoing.

Emerging Tech Standards:

5G is a significant focus for the Administration and for Congress. The goal is to ensure that the United States retains its leadership role. In March, the Administration released the "National Standard to Secure 5G," and NIST is playing a leading role in standards-related efforts in strategy development.

AI Program:

The focus of this effort is on the development of a trustworthy program. The initiative involves: 1) foundational research, 2) use-inspired research, i.e., using AI to accelerate scientific discovery, 3) test and evaluation, 4) standards and guidelines, which includes tools and guidelines for taxonomy, data, metrics, and testbeds, and 5) policy and engagement, which will include interacting with scientists, engineers, psychologists, lawyers, and others on issues of trustworthiness.

AI Happenings this Summer:

Events include a kick-off webinar August 6, a workshop on bias in AI August 18, and a second draft for public comment on the terminology and taxonomy of Secure AI later this summer.

USG AI Standards Coordinator:

NIST carried out the Executive Order by developing a plan for prioritizing federal agency engagement in the development of AI standards. They will facilitate discussions between the U.S. private sector and federal agencies to strengthen private-public sector coordination.

Congressional Hearings:

NIST officials have testified before U.S. Congressional committees on several topics this year: Walter G. Copan testified Jan. 15 on Industries of the Future; Charles H. Romine testified Jan. 15 and again on Feb. 6 on Facial Recognition; Rodney Petersen testified Feb. 11 on "More Hires, Fewer Hacks: Developing the U.S. Cybersecurity Workforce" and Mr. Copan testified Mar. 11 on NIST Reauthorization.

COVID-19:

In the area of quantitative PCR (qPCR) data analysis, researchers found that the manual threshold for detecting SARS-CoV-2 is confounded by background effects, resulting in a large possibility of false negatives. Impressive work has been done in analysis to improve the sensitivity of qPCR measurements. Additionally there has been a Call to Action to develop a machine readable COVID-19 dataset, including a TREC-COVID (building a pandemic information retrieval test collection.) NIST has 30 years of experience and was able to rapidly create a TREC-like evaluation track on COVID-19 data.

Celebrating 50 years of Cybersecurity Research at NIST:

In 2022, it will be 50 years since NIST initiated work in the data encryption standards arena, and a year-long celebration is being planned.

The Chair invited Board members to ask questions of Dr. Romine:

Mr. Venables noted that there are tremendous cybersecurity challenges in Industries of the Future. He asked if any thought is being given to applying a common set of work activities to plug cybersecurity work into these industries.

Dr. Romine responded that the Cybersecurity Framework is the umbrella under which ITL generally tries to engage industry sectors. The NCCoE is the nexus where research scientists interact with a large cross section of sectors, including healthcare, hospitality, manufacturing, and others. The Framework and industry engagement are used to try to keep a common lexicon across all Industries of the Future. The Privacy Framework will be useful as well.

Mr. Duvvur asked how industry can get more involved in the 5G Cybersecurity effort.

Dr. Romine explained that NIST tries to maintain direct communication with an active and broad list of interested industry representatives. Kevin Stine is the division chief of the Applied Cybersecurity Division. They would love to have Mr. Duvvur on the mailing list.

Mr. Stine said that they try to engage with communities of interest across all programs, and any interested party can join. They are in the midst of a formal letter of interest process through the Federal Register. They select companies to collaborate with in the lab environment. 5G has attracted a lot of attention from companies interested in collaborating.

The Chair noted that it might be interesting at a future meeting to hear more details on how ITL approaches the issue of integrating cybersecurity into new industries, applying the Cybersecurity Framework, and the NCCoE process.

Dr. Romine said that he would love to take the board through the entire process, as they have a couple times before. They are extremely proud of the Cybersecurity Framework, the development process, and continued engagement with industry. One secret of their success is the ability to engage effectively with industry because they are non-regulatory agency.

At 10:11 a.m. ET, the Chair recessed the meeting for a 4-minute break.

Industry Inputs on USG Compliance Programs

Frank Kendall, former Under Secretary of Defense for Acquisition Technology and Logistics

At 10:16 a.m. ET, the Chair welcomed Frank Kendall, who served as Under Secretary of Defense for Acquisition Technology and Logistics from 2012 to 2017. He noted that he had seen an article Mr. Kendall wrote on Cybersecurity Maturity Model Certification (CMMC) in *Forbes*.

Mr. Kendall introduced himself as a private citizen representing himself. He serves on the boards of Leidos and other companies, and he is a consultant for Northrup Grumman. His background is in engineering and he doesn't consider himself a cybersecurity expert, but he has worked on a number of cybersecurity issues. Mr. Kendall spent 7 years in the Obama administration working on issues related to unclassified systems. The issue of compliance originally came up because it's a contractual requirement, and the government has a pretty good way of supervising its contractors. For the Defense Department, it is the Defense Contract Management Agency. The Defense Security Service checks for conformity with classification requirements. In practice, the government didn't have the resources to ensure compliance, and it relies on industry to largely certify itself as meeting the standards.

CMMC is an attempt to create an independent system for assuring that industry has met certain standards. What makes Mr. Kendall nervous is that a third party would conduct the certification and determine whether or not a company can get a contract, and that is an inherently governmental function.

The scale of the CMMC is enormous. The standards themselves don't look too bad, although there could be fewer levels. The government was racing ahead, and schedules more than anything else appeared to be the driver. Mr. Kendall said he was concerned that there had not been a field or beta test, and they were going to go ahead with initial contracts and adjust from

there. If a small business sought a certification and did not receive it, it could be fatal. The people he has spoken with about it, generally speaking, are nervous.

A cottage industry eager to offer consulting on CMMC compliance has emerged. Mr. Kendall said he has reservations both about the effectiveness and about the practicality of this arrangement. If the government has concerns about enforcing its contracts, maybe it should do more about enforcing its standards. From industry's perspective, this is something the government is enthusiastic about doing and they are not going to tell the government that it's a bad idea. His advice has been to meet the NIST standards but wait to see what happens with CMMC.

The Chair invited members of the Board to ask Mr. Kendall questions:

Brian Gattoni said that his stakeholder community has voiced some concerns about cohesion among CMMC, NIST Guidance, and other frameworks.

Mr. Kendall replied that he does not understand why DoD should have its own cybersecurity standards and enforcement mechanism. Cybersecurity is not just a DoD problem – unclassified, sensitive material is a problem for everyone. There ought to be a national standards body. One of the problems from the beginning is that the market has not demanded enough cybersecurity. When he worked in government, he wrestled with the process of getting programs approved and through their lifecycle. He demanded that his staff include a provision on cybersecurity – to let managers know they are responsible for the cybersecurity of their programs. For a senior executive who is not in the cybersecurity world, we should make it as easy and clear as possible to understand what they need to do to protect their data and systems.

Ms. Hallawell asked about industry adoption of CMMC and how it might dovetail with something like use of the Mitre ATT&CK Framework.

Mr. Kendall replied that asking every program or organization to address this independently seems like a laborious approach. Attackers are creative and well-resourced, and vulnerabilities are inevitable. This is going to be a never-ending struggle, and there is never going to be a shortage of employment for cybersecurity experts over the next few decades.

Ms. Hallawell commented that she has seen the private sector looking more at how to deal with attacks, and she was interested in how industry standards and frameworks are perceived vis a vis government standards.

The Chair said he is interested in what Mr. Kendall is hearing from the defense contractors he works with. His general concern about certification programs is the risk that they add cost and paperwork without actually further protecting systems.

Mr. Kendall replied that he shares that underlying concern. He fears that the certifications might result in an illusion of better cybersecurity. Defense contractors have a competitive reason to protect their data. The industry view, generally speaking, is to take cybersecurity very seriously and try to keep up with the technology. The CMMC is going to add a layer of bureaucracy. The cost will be passed on to the government eventually.

The Chair said that that strikes him as a very realistic perspective. It was hoped that the CMMC would make a difference among the lower- tier suppliers, not the Leidos or Northrup Grumman tier. Was this a realistic aspiration?

Mr. Kendall replied that the middle-tier companies he works with also take cybersecurity very seriously. As we go down the chain of contractors, there is a responsibility on the primes to work with their subs. There will be a practical impact when a company has not been certified or failed a certification and is not allowed to be a subcontractor. There will be less competition and more delays. There are also concerns about conflict of intertest and paying someone to come and give you a certification. What exactly does the certification entail? How thorough are the checks? Do they just look at some documents? Do they do any penetration testing?

The Chair said that he had concerns about the effectiveness of this certification versus the real-world results from penetration testing. There is a degree of validation that can't be done overnight.

Mr. Kendall added that he could envision a bunch of firms being certified and then, when they are put to the test, it is revealed that they are not actually all that secure.

Mr. Duvvur commented that regulations change, making it difficult to ensure compliance. The moment a technology is certified it is potentially out of compliance.

The Chair said that big cloud providers pay a lot of attention to continuity, and it would be interesting to hear from them at a future meeting.

Mr. Kendall said that if someone wants to impose their will on the United States, there are ways to deny functionality. That is very different from breaching systems and stealing data.

The Chair said that the Board might like to have Mr. Kendall speak again at a future meeting.

Marc Groman said that he does not track this issue very closely, but the way the discussion was framed is troubling. A certification cannot and will not say that a company or contractor is secure. CMMC has a very narrow focus: Certifying that there is a baseline security necessary to be a contractor. Security will never be a checklist. The problem is if there isn't adequate staff, talent, or resources, the program itself doesn't matter.

Mr. Kendall said that inspectors will be trained for CMMC, but what expertise will they have? If someone is a cybersecurity expert, they are out working in the field.

Mr. Scholl mentioned the area of machine-readable techniques developed to reduce paper and documentary review requirements.

The Chair said that might be another topic the Board could hear about in the future.

Mr. Kendall concluded by saying that if he is wrong about CMMC he will admit it. *Forbes* asks him to contribute one article a month and he chose CMMC one month, but he has no desire to make it a major cause. He would be delighted to hear any feedback.

The Chair recessed the meeting for an 8-minute break.

Overview of USG and US Testing, Assessment and Conformance Model

Lisa Carnahan, ITL Associate Director for IT Standardization, NIST

At 11:16 a.m. ET, the Chair welcomed Lisa Carnahan, ITL Associate Director for IT Standardization, NIST.

Ms. Carnahan began her presentation by explaining that conformity assessment is about confidence, and there are three main points to remember: First, there is a toolbox of conformity assessment approaches intended to meet a range of needs. Second, conformity assessment program models vary based on balancing risk and resources. Third, software and cybersecurity bring challenges to conformity assessment, and there is a recognition of the need to try to push the models and adapt to the challenges.

The Basics of Conformity Assessment:

Conformity assessment is the demonstration that specified requirements are fulfilled. Basic terms and concepts include: 1) *Requirement*: How should the product or system perform? 2) *Determination*: How do we know it performs? 3) *Attestation*: Who says its performance has been demonstrated? and 4) *Surveillance*: What about assurances next week, or how are we looking at it on an ongoing basis?

NIST prefers that requirements are voluntary consensus standards. They need to be understood and be as objective as possible. If they are testable, all the better. Cybersecurity requirements change, the environment changes, and requirements can change.

Determination is made through testing, inspection, and audit. It can be performed by the manufacturer, the purchaser or a third party. Attestation made by a manufacturer is a Suppliers Declaration of Conformity (SDOC). A third-party attestation is a certification. The output is not that a product or system is secure; it's that requirements have been met.

Conformity decisions are often based on a sample at a point in time, and surveillance activities help ensure ongoing conformity. They can include pre-market activities, such as quality checks at manufacturing plants, and post-market activities, such as sample testing and complaint resolution. Conformity assessment is very hard in the cybersecurity space, where products are being updated all the time.

Standards for Conformity Assessment are published by the ISO Committee on Conformity Assessment (CASCO) in cooperation with the IEC. They involve testing, inspection, SDOC, certification, and accreditation. NIST does not rely on SDOC but uses accreditation instead.

Factors in Building a Conformity Assessment Program:

The risks associated with non-compliance should be proportional to the rigor of the system design. Over-design can be costly, and under-design reduces confidence. Marketplace consequences, regulatory penalties, and effective recall processes can allow for less rigor in assessment. This is explored in "The ABCs of Conformity Assessment: NIST SP 2000-01" and "Conformity Assessment Considerations for Federal Agencies: NIST SP 2000-02."

Conformity Assessment in the United States:

Conformity assessment in the United States in unique. There is no national level coordinating organization, and there are numerous conformity assessment bodies, differing in size and scope. Approaches are sector-developed, and there is an overlap in coverage. Conformity assessment programs are tailored to meet specific private and public sector needs.

Federal agencies are supposed to first consider using industry standards in purchasing. They should reduce industry complexity where possible and leverage private-sector and public-sector programs. The foundational considerations for federal agency programs are: 1) engage

stakeholders by getting their input and leveraging their knowledge, 2) maximize transparency so that nobody is surprised by processes or requirements, and 3) leverage existing efforts.

There can be variations in requirements by different federal agencies. For example, OSHA requires that N95 masks used in the workplace are NIOSH-certified, and the FDA had somewhat different requirements. A couple years ago, FDA and NIOSH got together and shifted the conformity phase to NIOSH so that it's now a one-stop shop for manufacturers.

Another example is the Limited Access Death Master File. In the final rule establishing the certification program for access to the file, it was recognized that there need to be cybersecurity requirements on subscribers to prevent identity theft. The government crafted a model for this program that says if you're being inspected or audited for other purposes and they're looking for cybersecurity, that's the certification that is needed.

The Chair invited Board members to ask questions of Ms. Carnahan.

Mr. Scholl commented that one thing often overlooked in building conformity assessment programs is how to deal with a supplier that falls out of conformity.

The Chair commented that security is a non-functional property defined in part by the adversary. You cannot certify that a system is secure. So you are stuck with a set of choices about properties that presumably are subject to assessment and then you attempt to convince yourself that that assessment is correlated with the property you actually want, which is a system that is resilient and secure from attack.

Ms. Carnahan said that there are some good starts in conformity assessment programs for cybersecurity, including a program at the Department of Health and Human Services for certifying electronic health record systems. She is not proposing that the models she showed will work everywhere, and the government has to be clear about what the objective is.

The Chair added that the government must also not lose sight of the fact that a hostile adversary gets a vote in whether the objective is met.

The Chair recessed the meeting at 12:04 p.m. ET for a lunch break.

Telework Lessons and New Guidance

Sean Connelly, CISA, DHS; Jeff Greene, NIST

At 1:01 p.m. ET, the Chair welcomed Sean Connelly of DHS and Jeff Greene of NIST to provide lessons learned in the recent telework surge and new guidance.

Mr. Connelly began his presentation with some background on his work, including involvement in the Continuous Diagnostics and Mitigation (CDM) Program at the Cybersecurity and Infrastructure Security Agency (CISA) at DHS. He then offered some context to the Trusted Internet Connections (TIC) efforts taking place throughout the government:

- In September 2019, the Office of Management and Budget released Memorandum M-19-26, which tasks CISA with modernizing the TIC initiative. It calls for updated program guidance, use cases, and pilots. It requires that the program be agile and responsive, with a focus on strategy, architecture, and visibility.
- There have been several advancements in related IT Modernization Programs, including: 1) NIST SP 800-207 – Zero Trust Architecture, 2) GSA Enterprise Infrastructure Solutions

(EIS) Acquisition Vehicle, which encourages SD-WAN, zero trust, 5G/Internet of Things (IoT) and cloud-based security solutions, and 3) CISA efforts, including the National Cybersecurity Protection Services, which is piloting a Cloud Log Aggregation Warehouse (CLAW) for cloud telemetry, and the CDM program, which is piloting the monitoring of agency cloud environments.

- The key TIC 3.0 program documents include: 1) Program Guidebook, 2) Reference Architecture, 3) Security Capabilities Handbook, 4) TIC Use Case Handbook & Use Cases, and 5) SP Overlay Handbook & Overlays.
- In March of this year, OMB released Memo M-20-19, which seeks to harness technology to support mission continuity. It encourages agencies to leverage approved collaboration tools and capabilities, and it advises them to make risk-based security decisions.
- The TIC 3.0 Interim Telework Guidance was released in April of this year. It was developed to support OMB M-20-19 and the current telework surge. It addresses telework security challenges, is discretionary and not part of core TIC program guidance, and is valid for the 2020 calendar year only.

Security challenges of the surge in telework include:

- Workers are geographically dispersed and more reliant on mobile devices. The distributed workforce has caused agencies to implement more cloud-based, remote user, and teleconference solutions.
- The traditional perimeter security model is less applicable. Attacks are increasingly focused on end users, where traditional network controls are not located. Trust cannot be assumed.
- Trust zones are used to secure network components with similar protection requirements. Segmenting networks into trust zones and enforcing traffic zones helps prevent lateral network movement.
- The goal of zero trust architectures is to shrink the trust zone down as small as possible. Zero trust assumes all users and access requests are suspect. Trust is established and re-established by robust identity credential and access management (ICAM), access controls, network analysis, telemetry, and threat intelligence.
- Implementing zero trust architectures may involve extensive planning, designing, and procurement efforts. The TIC 3.0 Interim Telework Guidance accommodates traditional, micro-segmented, and zero trust architectures by providing agencies with the flexibility to place Policy Enforcement Points anywhere in their existing network architecture.

The TIC 3.0 Interim Telework Guidance applies to scenarios in which teleworkers access sanctioned cloud services. It broadly supports a wide spectrum of architectural implementations, and it provides security patterns and capabilities to support secure teleworking:

- In the traditional telework security pattern, capabilities are positioned in a centralized location. When you scale this out, there are greater costs and decreased performance, a.k.a., the "TIC tax." The guidance offers new ways to connect to cloud services.
- Policy Enforcement Point (PEP) capabilities apply to specific use cases. As architectures move towards a zero trust solution, there may be a greater reliance on authentication mechanisms to validate remote users and protect data. Universal security capabilities are enterprise-level and apply across use cases.

- The guidance is not part of the current core TIC 3.0 document set and does not support existing TIC 3.0 use cases. Traffic to the public internet should still be routed through TIC access points.
- An appendix to the telework guidance offers a sample chart with telework capabilities. Vendors can build an overlay where they map their capabilities to the TIC telework capabilities. Agencies should use overlays to understand coverage and gaps delivered by service provider's products and services.

The finalized TIC 3.0 program documents will be released this summer, but a remote user use case will not be included in this release.

Separately, CISA's National Cybersecurity Protection System (NCPS) program is evolving to ensure that security information about cloud-based traffic can be captured and analyzed. NCPS released draft Volume 1 of the Cloud Interface Reference Architecture and is actively working to develop Volume 2. Agencies should refer to the document for telemetry requirements.

The Chair invited Board members to ask questions of Mr. Connelly.

Mr. Venables commented that the service edge architecture works when users are mostly accessing cloud services, but when they are accessing a mix of internal and cloud services it doesn't work as well. He noted that zero trust architecture places a high premium on skills and asked whether agencies have the teams capable of running that kind of environment.

Mr. Connelly said that there is a range in the technical skill sets at agencies. At the pace providers are providing services, it is tough to keep up.

The Chair commented that his impression of zero trust approaches, in general, is that they place a higher burden on the security at the client end and desktop compared to the more classic perimeter and firewall solution. Is there any magic for getting assurance that they're configured properly and that patches are up-to-date?

Mr. Connelly replied that that is a good question. What is considered the traditional security officer's responsibility?

Mr. Duvvur asked about data exfiltration and whether additional elements are required to address exposure opened up beyond the traditional approaches in an office environment.

Mr. Connelly said that they are still looking at that. There is a new attack vector they have to be cognizant of, which is one of the reasons they are rolling out the CLAW.

Mr. Greene took the floor to discuss cybersecurity considerations for telework and three publications ITL released in March of this year:

- An ITL bulletin titled "Security for Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Solutions," summarizes two existing special publications. It provides more concise information to IT managers, who were inundated with new demands as the telework surge began.
- A one-page tear sheet titled "Navigating the Conference Call Security Highway," provides tips for securing virtual meetings: 1) Use common sense; 2) Follow your organization's rules; and 3) Consider what security is necessary because not all calls are created equal. NIST released a video on this topic as well.

- A one-page tear sheet titled "Telework Security Overview and Tip Guide," offers an overview of telework security basics: 1) Use common sense; 2) Follow your organization's rules; 3) Use a VPN; 4) Secure your devices; 5) Pay attention to basic security; and 6) Watch for unusual activity.

Karen Scarfone, a NIST associate who worked on the "Security for Enterprise Telework" bulletin, added that the most noteworthy thing that had changed from previous, similar bulletins was a specific focus on zero trust architecture. It advises IT managers to plan telework-related security policies and controls based on a zero trust model and to develop a telework security policy that defines telework, remote access, and BYOD requirements.

The bulletin contains implementation recommendations. First, ensure that remote access servers are secured effectively and configured to enforce telework security policies. Second, secure organization-controlled telework client devices against common threats, and maintain their security regularly.

Mr. Greene added that the overriding recommendation for securing virtual meetings is to take a risk management approach.

The Chair recessed the meeting at 1:58 p.m. ET for a 2-minute break.

National Information Assurance Partnership (NIAP)
Mary Baish, Director, NIAP

At 2 p.m. ET, the Chair welcomed Mary Baish, Director of the National Information Assurance Partnership (NIAP).

Ms. Baish started her presentation with an overview of NIAP. In the early 1990s, the United States, Canada, and a number of countries in the European Union established the Common Criteria Recognition Arrangement (CCRA), which was released as a standard in 1996. National policy mandates the purchase of Common Criteria-evaluated, NIAP-certified commercial products for National Security Systems (NSS). NIAP authorities include NSD 42, CNSS Policy 11, CNSS Directive 502, and DoD Instruction 8500.01.

The NIAP mission is to validate evaluations of commercial off-the-shelf (COTS) IT products for National Security Systems (NSS) procurement; develop requirements specifications (Protection Profiles); and represent the United States in the 31-nation CCRA.

Protection Profiles (PPs) are meant to be testable and the tests repeatable. The profiles are based on technology type and are not implementation- or vendor-specific. They are written in collaboration with industry. They are standards-based, raise the security bar, and provide government users a basis for comparing products. Security is built into product lifecycles.

To initiate the NIAP evaluation process, a vendor goes to a COTS testing lab and selects the Protection Profile that is most applicable to the product. The lab tests the product, and the test results are then provided to NIAP for the final evaluation. If everything passes, validation documents are provided and posted to the NIAP website. The documents include a NIAP Certificate, Validation Report, Assurance Activity Report, Administrative Guide, and Final Security Target.

The NIAP evaluation confirms the security functionality of COTS products and allows product comparison by technology type. It adds assurance to an overall network security posture, sets baseline security requirements, and raises the bar for COTS product security functionality.

More than 900 evaluated product configurations are available for NSS procurement. NIAP collaborates with more than 200 vendors to develop Protection Profiles. Many evaluations are complete in 90 days.

Several U.S. government agencies and programs are impacted by the NIAP:
- CSfC: NIAP validated products are the building blocks of commercial systems used to protect classified information.
- DISA:
- DHS: The "Study on Mobile Device Security" recommends NIAP Protection Profiles and NIAP-validated apps for whole of government.
- DoD CIO: Memos, instructions, directives mandate NIAP PPs and NIAP-validated products for DoD.
- NIST evaluates the NIAP labs and works with NIAP.

In 2009, reforms began in the CCRA, largely spurred by the United States. An updated CCRA was signed in 2014 by all member nations.

More than 40 PPs have been developed, and there are more than 50 technology sectors represented in the technology communities that collaborate with NIAP. PP-based evaluations for mobility and network devices have increased. Interest in the technology communities continues to grow.

Ms. Baish outlined a number of recent and upcoming activities:
- A pilot related to automation was conducted recently with a report coming soon.
- They are working on other automation efforts and trying to automate the development of Common Criteria elements. Speed is always an issue when it comes to certification.
- A working group is looking at test automation in general.
- A working group is looking at Common Criteria in the cloud. How can NIAP evaluate products that run as a service in the cloud? The Common Criteria was written when most products were physical things. NIAP has already published a Protection Profile for mobile device management.
- They are working with NIST on entropy tests and certification.
- They are looking at incorporating threat-based cybersecurity.
- They are discussing the impact of the EU Cybersecurity Act and what changes will have to be made to the CCRA, if any.

The chair invited Board members to ask questions of Ms. Baish.

Mr. Venables asked whether any vendors are doing anything in the design and architecture process that helps them with a smoother or quicker path to certification.

Ms. Baish said there has been a lot of discussion in the CCRA about adding things along the lines of development accreditation.

The Chair asked if there is any connection in place or planned with the NIST SSDF.

Ms. Baish said there is attention being paid to the issue of secure software development now.

The Chair asked if there is any comment on the UK becoming a certificate-consuming nation.

Ms. Baish said that they announced the news that they were dropping their status to consumer last fall but she did not have any further comment on it.

The Chair noted that security against attack is a non-functional attribute of a system, which limits how far you can go in assurance. He asked whether there is basically a mutual recognition that the speed of certification trumped a higher level of assurance.

Ms. Baish said that a higher level can be achieved if the tech community writes it all down in the PP and explains the need for it. Even with products evaluated at a higher level of assurance, they were still finding a lot of problems. It was providing customers with a false sense of security and taking a long time. The CCRA reform tried to provide truth in advertising. They think openness is more important than being able to claim that they looked at all attacks for a particular product.

The Chair said it was clear that paying more for more testing wasn't really paying off in terms of higher actual security.

The Chair recessed the meeting at 2:47 p.m. ET for a brief break.

Public Comment, Summary of Day 1, and Board Discussions

At 3 p.m. ET, the Chair asked whether any public comment had been received.

Mr. Scholl reported that no public comment had been received.

The Chair opened the floor to Board members to discuss the day's presentations:

Certifications, Assessments, and Frameworks:

Doug Maughan commented that in addition to the certifications raised during the meeting, there are other requirements, such as FedRAMP and FISMA. He asked if there has been any published value assessments of those checklist-type requirements versus something like penetration testing. In other words, is the paper exercise worth the effort and does the technical exercise get us any further?

The Chair said that he tends toward the view that a properly done penetration test can be a good way to calibrate how secure development or secure operations or secure configuration was done. He said they may want to weigh in on CMMC in particular, but they should wait to hear from Katie Arrington on Day 2 of the meeting before making a decision.

Mr. Scholl said that he had reached out to confirm Ms. Arrington's schedule and was waiting to hear back. The other schedule change is that the NIST Program Updates session, scheduled from 11:45 a.m. to 12:15 p.m. on Thursday, might have to be cut short to allow time for Jim Olthoff, Associate Director for Lab Programs at NIST, to pop in and say hi.

The Chair said that Mr. Venable's earlier comment about a connection between NIAP or Common Criteria and the SSDF was a good one.

Mr. Venables said it is worth continuing to press on that issue over time. There has been too little examining of what can be done in the software lifecycle and design practices to improve

security and the verifiability of security. There is probably some middle ground to encourage framework standards, adoption, and architectural practices that make assurance easier.

Ms. Hallawell asked if there are ways to make Common Criteria easier. Some of the most innovative companies don't have the resources to do a Common Criteria certification. Has anyone done any analysis on of all the companies out there and how many are Common Criteria certified?

The Chair said that the United States reduced the evaluation level that was mandatory for U.S. government acquisition. It was controversial in the international community, but apparently, they somehow resolved it. When Ms. Baish talked about conducting evaluations in 90 days instead of 3 years, that represents a significant change. Looking at architecture or development practices had really never been part of Common Criteria as widely used. Could that be added in without driving the cost back up? It might be worthwhile to weigh in on Common Criteria and development and encourage them to look at it.

Mr. Venables said he thinks it is definitely worth mentioning the intersection of frameworks and the certification process.

The Chair encouraged everyone to think overnight about what they want to say with regard to that topic and also CMMC.

Standards and Racially Insensitive Terminology:

Mr. Venables said that his company has started a focused effort in removing racially insensitive terminology, such as *black list* and *white list*, from standards. He asked whether it is the ISPAB's role to recommend that NIST make a pervasive change across the standards.

The Chair agreed that it would be a great recommendation.

Dr. Romine said that the NIST community stakeholders have not been silent on this issue. They have received feedback with strong encouragement to take action, and they have already begun to scan the guidance documents and standards that they participate in to identify potentially incendiary or loaded words, with the expectation that they have already committed to making changes. That said, he would encourage the Board to encourage NIST to take swift and decisive action on the issue.

Mr. Groman moved that a succinct letter be drafted congratulating NIST on its efforts on the initiative to date and encouraging them to continue moving forward.

The Chair asked Mr. Venables if he wished to draft the letter.

Mr. Venables said he would draft the letter. The Internet Engineering Task Force drafted similar language the year before, and he would pass it around to the Board members.

The Chair thanked NIST for being engaged on the matter and thanked the new Board members for being vocal about it.

The Chair recessed the meeting at 3:22 p.m. ET.

Thursday, June 25, 2020

National Initiative for Cybersecurity Education (NICE) Update

Rodney Petersen, Director, National Initiative for Cybersecurity Education, NIST

[Prior to the official start of Day 2 of the meeting, there was a brief discussion about potentially adjusting the schedule to accommodate Board members on the West Coast if a virtual platform is used again in the future.]

At 9 a.m. ET, the Chair opened the meeting and welcomed Rodney Petersen, Director of the National Initiative for Cybersecurity Education (NICE) at NIST.

Mr. Petersen said he was pleased to hear that a few new members had joined the Board. NICE is working closely with two or three of the organizations represented on the Board. IBM has been very active in education and workforce activities, beginning with Ginni Rometty, who serves on the President's Workforce Policy Advisement Board. An IBM staff member currently chairs the NICE Cybersecurity Apprenticeship subgroup. NICE also works actively with companies in the financial sector.

NICE Overview:

Mr. Petersen presented an overview of NICE, beginning with the introduction of three student interns, who are working remotely this summer: Joseph Mercado is a rising junior at Cal State University, San Bernardino, where he is studying business; Frauke Steinmeir holds a master's degree in education and has gone back to earn an associate's degree in cybersecurity at San Antonio College; Matthew Scarborough holds a bachelor's degree and has gone back for an associate's degree from Clark State in Ohio.

The mission of NICE is to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development. Training is an increasingly important topic, and workforce development is a new area of emphasis.

NICE is in the process of updating its Strategic Plan. The vision and mission will remain largely the same, and the values statement will be somewhat consolidated where there is overlap. For example, seeking evidence and measuring results are very similar values. Mr. Petersen said he is proud that NICE is all about challenging assumptions, stimulating innovation, and embracing change. For better or worse, the pandemic has forced K-12 schools to rethink their learning models, and that may help stimulate innovation.

Key to what NICE does is fostering communication, collaboration, and resource sharing. In the IT and cybersecurity workforces, women and minorities are under-represented. There is a lot of opportunity to increase representation in the field, including diversity not only of ethnicity and gender but also of thought and approach.

In updating the Strategic Plan, NICE is developing new goals and objectives. The current plan has three goals: 1) Accelerate Learning and Skills Development: Inspire a sense of urgency in both the public and private sectors to address the shortage of skilled cybersecurity workers; 2) Nurture a Diverse Learning Community: Strengthen education and training across the ecosystem to emphasize learning, measure outcomes, and diversify the cybersecurity workforce; and 3) Guide Career Development and Workforce Planning: Support employers to address market demands and enhance recruitment, hiring, development, and retention of the cybersecurity workforce.

NICE funds CompTIA and Burning Glass to develop CyberSeek.org, which offers analytics around workforce demand and identifies the number and type of open positions. Approximately 1 million people are employed in cybersecurity, and there are a half million open positions. Most important is the interactive Jobs Heat Map that identifies the number of positions available, types of positions, and job titles.

There are two annual events where NICE brings public sector and private sector partners together: The annual NICE Conference and Expo coming up in November and the annual NICE K12 Cybersecurity Education Conference coming up in December. It was decided that this year's conferences will be moved to a virtual format.

NICE Cybersecurity Workforce Framework:

The NICE Cybersecurity Workforce Framework (a.k.a., NIST SP 800-181) is going through a review and update. It is currently organized in a hierarchical way, with seven workforce categories, 33 specialty areas, and 52 work roles. Work roles are not intended to be the same as job titles. The greatest changes to the Framework probably will be made in the specialty areas, both over the next year and in the coming years.

With the Federal Cybersecurity Workforce Assessment Act, Congress required federal departments and agencies to inventory how many people are doing these work roles in some capacity. Then they had to identify where we are falling short and where there are critical gaps that we need to prioritize in hiring, retention, or partnerships. They will be repeating that process in the next year.

NICE kicked off the Framework review and update process last November with a request for comment. The program received more than 500 distinct comments. The plan is to issue a draft for comment by mid-July with a final draft ready for announcement during the NICE Conference and Expo in November.

The NICE Framework's core authoring team is made up of Mr. Petersen, NICE Deputy Director Bill Newhouse, NICE Program Manager Danielle Santos, the Office of the CIO at DoD, the Chief Human Capital Office at DHS, CISA, and the Employment and Training Administration at DoL. They hope to make it easier to use by private sector employers.

In its work to update the NICE Framework, the program has found that:

- The term "Cybersecurity Workforce" is not inclusive of the range of "cybersecurity work" that the NICE Framework is intended to cover. A better term is "a workforce skilled in cybersecurity."
- The term "Workforce Framework" is not inclusive of other stakeholders such as education and training providers.
- "Work Roles" continue to be a critical component of the Framework. The program received comments suggesting adding additional work roles as well as removing one work role for every one added. There was also feedback about the lack of references to control systems, SCADA, etc.
- There is interest in adding "Job Titles," which is not necessarily the same as "Work Roles."
- "Competencies" are an attractive addition but are proving difficult to articulate and relate to the current structure. Employers increasingly want to hire people based on competencies.

- "Cyber" is misunderstood and potentially misapplied. It is used as a prefix, as shorthand for "cyberspace," and shorthand for "cybersecurity." One example is the DoD Cyber Workforce Framework, where the intent is to focus on cyberspace.
- There is a need for greater harmonization with the NIST Cybersecurity Framework, NIST Privacy Framework, and other NIST publications that talk about cybersecurity work.
- There is a desire to reconcile differences with "Knowledge Units" (criteria) for becoming a National Center of Academic Excellence in Cybersecurity. We are not necessarily using the same language, and we want to make sure the CAE models the NICE Framework.
- It is important to leave open the opportunity for international adoption of the Framework. We know that other countries want to adopt the Framework, and we want to try to deemphasize the drivers that make the Framework U.S.-only.

Several tentative conclusions have been reached regarding the updated NICE Framework. The scope will cover the Security of Cyberspace, and the new title will be the NICE Cybersecurity Competencies Framework. Components will include: 1) Categories, which will be reframed and reduced while Specialty Areas are eliminated; 2) Work Roles, which will be replaced with Specialty Area labels to avoid confusion with job titles; 3) Tasks, knowledge, skills, and abilities, which are under further review – unlike much of the structure of the Framework, KSAs need to be dynamic and fluid; and 4) Competencies.

They have found that they need to build and encourage the building of tools and resources – and convey awareness of existing tools – to bring the Framework to life.

The draft NICE Strategic Plan revised goals:

- Expand application and use of the NICE Framework.
- Promote the discovery of cybersecurity careers and multiple pathways: A lot of young people, parents, and others have misconceptions about the field, and the Strategic Plan will seek to help demystify cybersecurity careers.
- Transform learning to build and sustain a diverse and skilled workforce: This builds on advancements in online learning and new ways to do hands-on training. It also encompasses interoperable learning records.
- Modernizing the talent management process to address employer needs: The issue of competencies becomes increasingly important.

The Chair invited Board members to ask questions of Mr. Petersen.

Mr. Venables commented that in the financial sector they have observed a shortage of cybersecurity workers, but the real problem is the need for greater productivity from the cybersecurity workforce already in place. He asked about the NICE Framework's relevance to training people on how to be more productive.

Mr. Petersen replied that NICE recognizes that training and education do not end when someone gets a job. The Workforce Policy Advisory Board is committed to trying to reinforce the importance of employers providing ongoing training. The automation issue is of particular interest, as work roles or tasks become obsolete.

Mr. Venables said that they have found that one of the sources of people leaving is the lack of automation and tools A universal weakness is people not being trained on how to think about how to automate, how to structure process, and how to do continuous improvement. They have

been sending a lot of their people to non-cybersecurity training on things like site reliability, engineering processes, and automation.

Mr. Petersen agreed that it's not just about technical competencies but also about soft skills and critical thinking skills. Students are not always given that type of training.

Dr. Romine asked whether there is an appreciation gap for those who have operational roles in cybersecurity. If someone is successful in this role, there is no event to illustrate it.

Mr. Venables said that his company has introduced different types of metrics, including the notion of a control pressure index, which measures how they are successfully defending their systems. Most organizations see a lot of scans and intrusion attempts, most of which are not significant. Some are interesting, and some make it through one line of defense, some maybe get to the second line of defense. For malware, there can typically be eight levels of controls. The index measures what percentage are making it to the first level and then the second level, etc. It is a way of illustrating the effort that's going on to push back against those attacks.

Mr. Duvvur said that, increasingly, service providers are taking on a lot of the work in terms of building controls directly into the cloud. All of the operational procedures to ensure secure workloads, etc. are more or less engrained in the clouds themselves. The velocity will start to increase over time as there's a shared model. Regulators are still going to come after the bank client at the end of the day, but it starts to assuage some of those concerns and drives a bit more velocity through that lifecycle.

The Chair said that when he thinks of security integrated into other jobs, he thinks of software developers. At his previous employer, there were a few thousand people who were directly in cybersecurity jobs and several tens of thousands who were writing software and had to write it securely. Similarly, with site reliability engineers, they have to have enough security competence and skills to do that part of their job securely.

Mr. Maughan asked about White House and NSF activities regarding the Future of Work initiative and how involved NICE is. The Future of Work is very much about upskilling, reskilling, and how to reach under-represented communities.

Mr. Petersen said they are actively following the efforts, and the NSF has always been a good partner. The work NIST is doing in AI is closely connected to what the NSF is doing. They are talking about the cybersecurity dimensions of that work. One of the notions in the NICE Strategic Plan is of a multidisciplinary approach - that this is not just for computer science and engineering, and every discipline has a cybersecurity component.

Mr. Groman commented that the privacy field is about 10-15 years behind cybersecurity in terms of career paths, talent, and skills. He can come up with dozens of examples where not having the established privacy team to support and work with the cybersecurity team leads to bad outcomes for both. They want to be able to build up the cadre of privacy professionals across the federal government and private sector. If anything, he has seen attrition.

Mr. Petersen said that it is kind of a follow-on to the NIST Privacy Framework. They are not intending to have a combined framework but instead trying to model each framework after the other and look for areas of overlap and areas of distinction.

Dr. Romine pointed out that the meeting had run quite a bit over time, which he said was fine because the conversation was spirited and useful.

Mr. Groman said that he should have started his comment by saying congratulations because the NICE program is outstanding. It's everything they dreamed of, and they want to expand it. He would love to see something similar occur on the privacy risk side.

Positioning, Navigation, and Timing (PNT) Profile Development
Jim McCarthy, NIST

At 9:58 a.m. ET, the Chair welcomed Jim McCarthy of NIST to the meeting to discuss the development of a PNT profile per Executive Order 13905, "Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing (PNT) Services."

Mr. McCarthy began his presentation with some background on the PNT profile development initiative. The executive order, issued February 12, 2020, directed the government to foster the responsible use of PNT services by critical infrastructure owners and operators.

NIST is leading the effort to develop a single, cybersecurity-based, foundational PNT profile, with a deadline of February 12, 2021. This will lay the groundwork for other agencies to create sector-specific profiles for things like navigation systems for aviation, industrial control systems, etc. The goal is to ensure that any disruption would have a minimal impact. NIST's outreach and engagement efforts are directed not just at federal agencies but also at the private sector.

The focus is on critical infrastructure – owner/operators of the electrical power grid, communication infrastructure, businesses in the transportation, agriculture, weather, and emergency response sectors, among others. Some of these businesses have the sophistication and resources to assess and mitigate the risk, and others don't.

Patricia Hatter asked whether NIST is reaching directly out to companies.

Mr. McCarthy said that the GovDelivery system is one of the outreach mechanisms being used. There is a list of nearly 10,000 members on the system. Based on feedback and responses, they are providing mechanisms for people to contact them. They are also reaching out via social media and webinars.

NIST issued a Request for Information on May 27 seeking information from PNT tech vendors, users of PNT services, and other key stakeholders. They have not yet started working on the profile, but they have started working on its super structure.

The RFI includes eight requests:

- Describe public or private sector need for and/or dependency on the use of PNT services or any combination of these service.
- Identify and describe any impacts to public or private sector operations if PNT services are disrupted or manipulated. What is the risk to the system itself? Can you articulate the risk to the system?
- Identify standards, guidance, industry practices and sector-specific requirements referenced in association with managing public or private sector cybersecurity risk to PNT services.
- Identify and describe any processes or procedures employed by the public or private sector to manage cybersecurity risk to PNT services.

- Identify and describe any approaches or technologies employed to detect disruption or manipulation of PNT services. What are you using to detect disruption?
- Identify any processes or procedures employed in the public or private sector to manage the risk that disruption or manipulation to PNT services pose: This is focused on the business risk. If there are consumers of their products, what would be the downstream effects to their user base?
- Identify and describe any approaches, practices and/or technologies used by the public or private sector to recover or respond to PNT disruptions: Do you have a response plan in place? How quickly can you recover?
- Any other comments or suggestions?

Stakeholders can submit responses to NIST via the website and they will be posted publicly. The PNT profile development process aims to be open, transparent, and collaborative. The profile will provide guidance to organizations on how to: 1) Identify systems dependent on PNT; 2) Identify appropriate PNT sources; 3) Detect disturbances and manipulation of PNT services; and 4) Manage the risks to these systems.

The NIST Cybersecurity Framework is the perfect tool to use for this project. It is a living document that has a common and accessible language. It is adaptable, risk-based, guided by perspectives, and meant to be paired with other documents. There are a number of sectors that have used it in developing their own profiles, including the manufacturing, financial services, and maritime sectors.

The RFI response period opened May 27, and a pre-recorded outreach webinar was made available June 4. They expect to issue the PNT profile draft annotated outline and host a status update webinar later this summer, with an initial analysis of responses anticipated in August. In the fall, they plan to issue a draft PNT Profile for public comments and host a status update webinar, which will give them at least 4 months to adjudicate comments before the final deadline of February 12, 2021.

Section 4i of the EO gives the Secretary of Commerce 180 days (i.e., a deadline of August 8) to "make available a GNSS-independent source of Coordinated Universal Time to support the needs of critical infrastructure owners and operators for the public and private sectors to access." They have a fiber optic connection in place and it's up to any entity to sign up for that particular service. They are in the process of testing that now. They are working with outside stakeholders to deliver GNSS-independent UTC with accuracy required for critical infrastructure. The first inquiries were to develop timing delivery over optical fiber, and they will work with interested parties to explore other technologies as well. The Boulder and Gaithersburg offices of NIST are both working on the project.

Mr. Venables asked how delivery over optical fiber is going to make it to critical infrastructure.

Mr. McCarthy said that it will be an enrollment process. Owners and operators will sign up for it.

Mr. Scholl added that the "clock people" at NIST are going to provide a timing calibration service. They are going to run dedicated fiber from the Boulder and Gaithersburg campuses. They would then offer organizations calibration services to ensure that what they're offering downstream is accurate and correct down to a certain level of fidelity.

Mr. Venables asked about the plan to communicate this out to the critical infrastructure sectors and whether it goes out through the sector-specific agencies or sector coordinating councils.

Mr. Scholl said that it will go out through all of that and there are many other agencies that are working on other pieces of the initiative. Some of the outreach will be done by the Time and Frequency Division once they have the services up.

The Chair said that it might be interesting to get a brief update from the Time and Frequency Division. He was wondering if you have to run dedicated fiber to every user or if there is some infrastructure in place he's not aware of.

Mr. Scholl said that they have other time measurement services they offer besides the time over fiber service. They are first out of the gate with the time over fiber services, but there is a lot of work being done in other agencies, including DHS.

Mr. McCarthy asked everyone to contact NIST by email or Twitter with questions or comments.

The Chair recessed the meeting at 10:35 a.m. ET for a 10-minute break.

NIST Cryptographic Conformance Testing Update

Michael Cooper, Manager, Security Testing, Validation, and Measurement, NIST

At 10:47 a.m. ET, the Chair asked about the plan for hearing from the CMMC office.

Mr. Scholl said that they would hear from Mike Cooper, Manager of Security Testing, Validation, and Measurement at NIST, instead. If Katie Arrington or her deputy joined the meeting later, he would call another audible.

The Chair said that he was definitely hoping to hear an update from CMMC, but if the speakers weren't there, the meeting should proceed with the alternative plan.

Mr. Cooper started his presentation with an overview of the work his group does. They are focused on testing capabilities and the appropriate testing and verification processes for crypto and several other security areas.

Cryptographic Algorithm Validation Program (CAVP):

Over the past 20 years or so, they have used a desktop-based tool called the crypto algorithm validation system, which was a purpose-built C, C++ desktop application. They are just about ready to retire it. For the past few years, they have been working on a web-based automated crypto validation system and are using it almost entirely now.

Mr. Cooper provided an overview of ACVP. He said he is probably using the wrong acronym because ACVP specifies the protocol itself, which is the specific schema that's necessary to transfer data back and forth between a client and a server. NIST developed the protocol and the server. The testing labs and the vendors take the clients and integrate them with their own crypto modules so that they can talk to the NIST server. Once they do that, the testing process is 95% automated. They purposely left in a small manual step at the end to review the validation certificate to make sure that there's no language problem or miscommunication on it.

Automated Cryptographic Validation Testing System (ACVTS):

The ACTVS is ahead of CAVS in that CAVS was always a little behind with the algorithms produced by the crypto team. ACVTS has a test for every algorithm.

They had to work with all the labs to make sure they could show the capability to use the system. A publicly available system, called Demo, tests each new release and maintains backward compatibility with previous versions. Industry can use it free of charge to test their construction. Client-side code is open-source, and they are working on the server-side code.

Since this is automated, you either pass or fail, and there's no ability for a laboratory to add value necessarily to the testing process. Many vendors asked to test our own code. They came up with the capability for a vendor to be identified as a first-party lab to test its own software and verify its functionality. Two or three vendors are already acting as their own first-party labs for testing their algorithms.

Cryptographic Module Validation Program (CMVP):

With CMVP, the module is the container that all the algorithms go in, and it is a security boundary within the system that protects the integrity of the crypto implementation. They continue to run a much more manual process around CMVP.

FIPS-140:

The first iteration of FIPS-140 came out in 1994. The current version is FIPS-140-2, which is 19 years old. As of last year, the secretary of commerce approved FIPS-140-3, which points to ISO 19790. ISO 19790 is the actual set of requirements, and a subordinate document, ISO 24759, is the derived test requirements.

They are working with NIAP, which is a user of their program output and often helps NIST with guidance as well as the user group forums.

Most of the documents they had to prepare align with the ISO standard. There's an ISO standard A-F that's an appendix to ISO 19790. SP 800-140 basically references the derived test requirements. They wrote each one with the intent that NIST could add clarity or override the international standard if absolutely necessary.

They published the relevant special publications in March and are working on the implementation guidance. They have an old application called Cryptic, which the laboratories use to compile their test report and submit it to NIST. They are working on a web-based submission capability and hope to have that completed by September.

Entropy Testing:

A new area they are diving into is entropy and entropy standards in the SP 800-90 series. Many vendors either purchase IP from another company or get their entropy source through some other method. When they ask for details about how the entropy is created, they have a tough time getting an answer from the module vendors. If this could be a separate validation and they could get the other entropy source vendor to produce its own validation, then it could be referenced by any of the modules that use it as a separate item.

They are working on an application now. There are some automated tests that are performed, but there is still an evaluation of the process for how you make the claim that you've got enough entropy based on your source.

The crypto module testing automation is something they have always strived for. There is an NCCoE project in development. They have worked with many different vendors and are developing a workshop targeted for September 1.

A lot of the testing that goes on within a particular company could be used as an output. NIST has never established what artifacts and evidence would be necessary for them to accept the testing done within a company's boundaries. If they're doing some sort of code analysis or if they've got a certain process built into their development techniques, those could be leveraged as evidence that they meet the requirements in FIPS-140.

NIST Crypto Testing Outreach:

They have been working with industry in several different forums, including RSA and the ICMC. The next ICMC, rescheduled to August, is planned for both a live and virtual format. They also work with the CMUF, an industry-led group of representatives from all the labs and many of the companies they interact with on a regular basis. Over the last several years, they have also been interacting much more with NIAP and Common Criteria.

The Chair said that the move to more automation and more reliance on vendor testing artifacts sounds great. He asked about the population they're dealing with.

Mr. Cooper said they have dealt with about 650 vendors. They average 550-600 modules a year. They have six reviewers who do all of the validations, which is why they need more automation.

The Chair asked why people routinely don't flip the switch on the mode of crypto used.

Mr. Cooper said that many companies have come up with the idea of a FIPS method of managing their crypto libraries. Most of the time, they're developing for an international market and they've got cryptography built into their library that covers a span of possible operational locations beyond the U.S. government. By putting in this FIPS mode, you're in essence trying to restrict the usage of algorithms down to only those that are approved by NIST. That is difficult in that there are many algorithms outside of the NIST-approved set of algorithms that are necessary for normal operations. Is it riskier to operate outside of FIPS mode? Maybe not. All of those same algorithms are tested and validated using CAVP, so all you're switching between is a restricted or a wider set of algorithms. The hard part is if some application says, instead of using AES to do this function I'm going to use this other algorithm. You would never know because you don't have the FIPS switch flipped.

The Chair said that it strikes him as clearly good practice to move toward automation and reliance on more integration in the developer task flow and developer product model.

The Chair recessed the meeting at 11:20 a.m. ET for a 5-minute break.

NIST Program Updates

Matthew Scholl, NIST; Kevin Stine, NIST

At 11:30 a.m. ET, the Chair welcomed Matthew Scholl and Kevin Stine, both of NIST, to provide updates on NIST programs.

[Mr. Scholl reported that there were several thunderstorms in areas participants were located, and some connectivity was lost temporarily because of power outages.]

Mr. Stine opened the presentation by following up on the previous day's discussion about diversity and inclusivity in the context of terminology used in the technology space. NIST takes the issue very seriously and has taken a number of concrete steps, including an initial inventory of the existing security and privacy publications. They will take a hard look at documents as they move through their lifecycle from early development into draft and into final. They have identified an extensive list of publications that have one or more uses of negative terms and are in the process of initiating updates. In most cases, they are likely to be errata updates.

Ms. Hatter asked Mr. Stine to review the recommendations.

Mr. Stine said that there is an IETF RFC that has provided several alternative word pairings for both *whitelist/blacklist* and *master/slave*. There seems to be growing industry consensus to replace *whitelist/blacklist* with *allow list/block list*.

Mr. Scholl added that they have been working internally with staff to ensure that decisions for replacement terms are well-informed. They are concerned about terminology that might have qualitative implications not only about race but also about gender and other areas of inclusivity.

The Chair noted that Mr. Venables had drafted language for a letter and sent it around to Board members overnight.

Strategic Planning at ITL:

Mr. Stine turned to a presentation of strategic planning efforts within ITL. They have tried to focus the discussion around three core questions: Do they have their priorities right? Are they missing anything? Are there areas that do not need to be prioritized or emphasized as much as they are today?

They have identified several priority areas, including: metrics, education, training and workforce development, privacy, cryptography, identity and access management, trustworthy platforms and trustworthy network, emerging technologies, stakeholder engagement, standards, and the ITL workforce.

Ms. Hallawell commented that cybersecurity in both the private and public sectors needs to be better integrated into wider parts of the IT organization. She asked how NIST looks at the broader fabric of how cybersecurity is to become more entwined.

Mr. Stine said that ITL absolutely looks at cybersecurity and privacy in the context of the broader IT organization and in the broader enterprise risk management context. In the priority area of trustworthy platforms or trusted platforms, they include secure software development work.

Mr. Scholl added that a big emphasis of the trustworthy platforms arena is to have security capability or resilience capability become inherent in IT as much as possible.

Mr. Stine said that he and Mr. Scholl represent only two out of seven divisions in the ITL, and their view has been informed significantly by experts across all of the relevant areas.

Mr. Scholl added that they have had social scientists and usability experts also work with them. More emphasis needs to be made on expertise in hardware security as well. They will be working with the material scientists and manufacturing experts across NIST.

Questions about Data Governance and Privacy:

Mr. Groman asked where guidance around data governing, tagging, and inventorying fits in. The chief data officers in the government must work with the CISOs and CIOs, but the technical capabilities that allow a government agency to understand its data are not there.

Mr. Scholl said this is a very complicated question. They have been looking at it through a very narrow lens of cybersecurity. They have another research organization within the laboratory, the Information Access Division, that looks at some of these data governance issues. They draft best practices and methods around data indexing and ways to put together large, disparate data sets at volume and velocity.

Mr. Groman said that one of the big challenges in the private sector comes in the context of mergers. There are cases where a parent company buys a smaller company, the smaller company says here's our data, and then they discover that they have 52 million social security numbers and no one knows why. The new PII Inventory Tool scans privacy documents and creates a list, but if your privacy documents were wrong, you're not going to have an inventory of your PII or your data.

Mr. Stine said that the topic of data and data protections will span all of the priority areas. There is a growing emphasis on data security at the NCCoE, which is working on a number of projects on data confidentiality or data integrity. They have been discussing with industry partners a more foundational, data-focused project.

Mr. Gattoni said that data is one of the three things he is responsible for at CISA. The chief data officer works for him and struggles with a lot of the same challenges. They have started with the very functional approach of cataloging and looking at the feature sets of data tools on the market. What they are really stumbling into is the grand logistics challenge of an agency where data is the currency in trade. Data treatment and cleaning and prep was always an ancillary task of analysts as part of their normal operations. It needs to be treated as an entirely different function.

Mr. Groman said that before starting a risk assessment of privacy, the first thing is to know what data you have. Until we can do that well, the other pieces can't be done well.

Ms. Hatter pointed out that there is so much infrastructure technical debt because companies just don't have time when they make acquisitions – they have to keep moving forward.

Mr. Stine briefly turned the conversation to an introduction of Jim Olthoff, Associate Director for Lab Programs at NIST, who had just joined the meeting for a quick word.

Mr. Olthoff said he wanted to take the opportunity to thank everybody for engaging during the meeting. ISPAB is one of the most important advisory committees they have. This area is critically important to the country and is an important part of what NIST works on. They need the Board's input.

Mr. Stine thanked Mr. Olthoff for the statement of support.

Mr. Groman said that what is missing in the data governance problem is the technology.

Mr. Scholl said there might be an opportunity to leverage work in AI or machine learning.

Mr. Maughan mentioned that those kinds of discussions are happening in both the AI Working Group and the Big Data Working Group within NITRD.

Mr. Scholl added that one of the concerns about these data sets, especially if they are going to be used to draw inferences, is identifying the biases that are potentially inherent in the data when it was gathered.

Mr. Stine said that if the Board wished, they could have a data-focused session.

Risk Management and Cybersecurity:

Mr. Stine said they have a long-standing risk management program, and it is an area that will continue to grow. With tools like the Privacy Framework and the Cybersecurity Framework, increasingly the common thread is how to anchor these in broader ERM activities.

They have issued some guidelines recently, particularly NISTR 8286, on integrating cybersecurity and enterprise risk management. That publication was released for public comment, and a second draft for comment is anticipated soon. There has been a very positive response, mostly from ERM practitioners.

Ms. Hatter noted that she has been on three public company boards, and the risk management element – cybersecurity issues, privacy issues – should be much more centerstage. However, most people on boards don't have any background in this. When you try to bring up these topics, it is like throwing Jell-O against the wall. The normal board member doesn't know how to frame it, so they can't give it any context. Maybe there is some way to get things board-ready or plug into some framework that maybe the legal department or CFOs relate to.

Mr. Stine said that this aligns with integrating cybersecurity and ERM. One objective should be to reduce the demand on board members – present cybersecurity risk in a way that will resonate with them, using the language and tools that they are already using to manage broader enterprise risk.

Tactical Items:

Mr. Scholl turned to a couple tactical items. The 800-53 REV-5 draft is closed for comments. There are no baselines in it – it is a control catalog. The baselines will be in a second document. Also, they are going to be approaching cybersecurity metrics from two angles. Are there foundation units like bit strength that they can use to understand the security capabilities? Do they have common understandings of different tests, assessments, and observations that are done? They need to come up with new metrics looking at cryptographic strength in light of quantum machines.

Mr. Stine said that they recently issued two IoT documents: NISTR 8259 and a companion document, 8259A. 8259A provides six core cybersecurity capabilities for connected devices. 8259 is the root document, discussing foundational activities for manufacturers to consider.

In response to a question about this being comparable to – or different from – activities coming out of the EU and UK, Mr. Stine said he thinks it is comparable. The six core capability baseline activities were in some ways developed with collaboration from abroad, and they took into account a number of existing baselines from other organizations, including some international entities.

The Chair thanked the presenters and recessed the meeting for a 34-minute lunch break.

Solarium Report Implementation

Nick Leiserson, Office of Rep. James R. Langevin (RI-02)

At 1 p.m. ET, the Chair welcomed Nick Leiserson, legislative director for Rep. James R. Langevin of Rhode Island.

Mr. Leiserson began with some background on Congressman James Langevin. Rep. Langevin chairs the Intelligence and Emerging Threats and Capabilities Subcommittee for the Armed Services Committee. He also serves on the Cybersecurity, Infrastructure Protection, and Innovation Subcommittee for the Homeland Security Committee. He is one of four legislators who serve on the Solarium Commission.

The Solarium Commission was created by the National Defense Authorization Act in August 2018. It includes four sitting members of Congress, four deputy secretary-level officials from the executive branch, and six individuals from the private sector. The commission has two overarching goals: 1) to develop a strategy for the United States in cyberspace to protect against cyber-attacks of significant consequence; and 2) to develop an implementation plan for the government to achieve the vision of that strategy.

The commission's report was published on March 11, and it was one of the last public events to take place in Washington, D.C. this year. There has been one remote hearing with the Senate Homeland Security and Governmental Affairs Committee, and another is scheduled tentatively for July with the House Committee on Homeland Security.

Layered Cyber Deterrence:

The report emphasizes deterrence in cyberspace, with the caveat that it is not deterrence in the nuclear sense of the word. They call it "layered cyber deterrence," and they are focusing on three areas. The first is about shaping the behaviors of adversaries using norms of responsible state behavior in cyberspace and using bodies like United Nations experts to help delineate what responsible states do in cyberspace. The second area is about resilience, both by increasing the cost to adversaries of exploiting a system and by reducing the benefit they gain if they are successful. The third area is about cost imposition on adversaries.

Compared to the 2015 DoD Cyber Strategy, the biggest evolution is the emphasis on a whole-of-nation approach. One of the things that was apparent to the commission was that there isn't a lot of consistent language in cyber strategies across agencies.

Pillars for Guiding Implementation:

The report outlines six pillars to guide implementation. The first pillar is about transforming government and governmental reform. The report recommends, among other things, creating a statutorily backed position of a National Cyber Director within the Executive Office of the President. It also recommends strengthening CISA and reforming Congressional committees so that there aren't 80-100 different committees and subcommittees that have some claim of jurisdiction over cyber.

The second pillar is about shaping norms of international behavior. It recommends creating a stand-alone Bureau of Cyberspace Security and Emerging Technologies at the Department of State, headed by a full assistant secretary.

Jumping ahead to the sixth pillar, the report deals with preserving the military instrument of power, reviewing U.S. Cyber Command and working on the DoD cyber workforce.

The third, fourth, and fifth pillars address resilience. Pillar three deals with how we look at resilience, and it recommends creating a continuity of the economy plan. The need for continuity of economy planning has become increasingly apparent in the time of COVID-19. The idea is to mitigate the consequence of a successful threat actor's exploit. Pillar three also recommends establishing a statutorily defined national risk management cycle with responsibilities for the different sector-specific agencies.

Pillar four is focused on increasing cybersecurity across the entire ecosystem and the need for a better measurement of cybersecurity. It recommends changes to the Sarbanes-Oxley Act and corporate governance. The commission is trying to use business incentives and translate cybersecurity outcomes into dollars and cents to help organizations account for risk. A key recommendation is the creation of a Bureau of Cyber Statistics to maintain incident data.

Pillar five is about working more closely with systemically important critical infrastructure. It focuses on operational collaboration between the government and providers to better understand specific threats. The report recommends better operational collaboration, such as joint analytical work or involvement in defensive cyber campaign planning.

Short-Term and Medium-Term Priorities:

All in all, there are about 80 recommendations in the report, and 55 have a legislative component. A number of amendments to the current Senate National Defense Authorization bill were filed to implement some of the recommendations. Another short-term priority is establishing a National Cyber Director at the White House. Medium-term priorities include creating a Bureau of Cyber Statistics. Continuity of the economy planning and creating a joint collaborative environment for analysis are also high priorities. Other recommendations, like Congressional reform, are less likely to happen any time soon.

In response to a question about the reaction in Congress and the Administration, Mr. Leiserson said the response from Congress has been quite positive in general. The Administration is expected to file its response to the report with Congress soon.

Mr. Maughan asked what kind of cross-communication took place between the Solarium Commission and the Moonshot Initiative.

Mr. Leiserson said there was significant cross-communication. Rep. Langevin briefed the Moonshot group last year on the Solarium's ongoing deliberations. One of their recommendations is to fund some of the Moonshot initiatives. There was also cross pollination with the National Security Commission on Artificial Intelligence. A tri-commission meeting on workforce development issues met last week with people from the Solarium Commission, the National Security Commission on AI, and the National Commission on Public Service.

The Chair asked if there had been any international reaction.

Mr. Leiserson said there were a couple of international trips that commission staff went on. There are several references throughout the report to the United Kingdom's National Cyber Security Center, which the commissioners found to be an innovative organization. A fair bit of the pillar five recommendations on CISA were inspired by the work of NCSC.

Final Words, Recommendations, and Discussions

The Chair asked for feedback from Board members on items from the day's discussions to be considered for recommendation or action.

Mr. Scholl reminded everyone that there had been discussions about data governance, the NICE Framework and research into extending it into the privacy arena, and different types of industry metrics that are used to accentuate the positive.

The Chair said he had hoped to hear an update from the CMMC office and what they were doing – or not doing – in response to concerns the Board expressed last August and issues that Mr. Kendall raised the previous day. There possibly is a need to make an observation or a recommendation with regard to CMMC, but he does not think that can be done without an updated presentation. At a minimum, they should try again at the next meeting to hear an update. It is very unfortunate that the presentation at this meeting was canceled.

Mr. Scholl apologized and said he would follow-up and figure out what happened. He added that another issue is cybersecurity education. How do you drive more value from the job roles and functions in the NICE Framework?

The Chair agreed and said that there certainly is a need for more cybersecurity practitioners, but the question is: Are we trying to inspect quality in, or are we working to build systems that are both ready to use and ready to use securely?

Removing Negative Terminology from Standards:

The Chair turned to language drafted by Mr. Venables on a recommendation for reviewing terminology in standards for considerations of sensitivity and diversity.

Ms. Hallawell asked if the Board could promote industry support for replacing insensitive language while promoting government action in that arena.

Mr. Gattoni said that NIST can inform CISA about sector engagement on the issue. It is a mission-oriented issue that CISA can take on with its stakeholder engagement division and entities like the sector coordinating councils.

The Chair added that the Board can make a statement that this is a best practice that should be adhered to both by government and industry and then make specific recommendations targeted at government.

Mr. Scholl said it would be useful if changes were coordinated among agencies and different policies didn't end up using different terms.

The Chair asked if someone wanted to move that the Board approve the language drafted by Mr. Venables to be amended as discussed.

Mr. Groman moved that a concise letter be written on the topic.

Ms. Hallowell seconded the motion.

The Chair called a vote, which was unanimous in favor of the motion.

NIAP, Common Criteria, and Best Practices for Software Assurance:

The Chair noted that the Board discussed sending a recommendation to NIAP about reflecting best practices for software assurance as described by the new NIST SSDF. It is worthwhile to go on record that it would be desirable to try even it's a long shot.

Ms. Hallawell said her overall concern with Common Criteria is that relatively few vendors go through the process because it is expensive and time-consuming. Having a secure software development lifecycle component should be part of any such testing, but the Board should be clear on its motivation. A broader point is whether we can move towards a more accessible method by which vendors can say they're building in better security. It might not be as rigorous as the SSDF or Common Criteria, but it might be useful.

The Chair said that when this battle came up in the past, a concern of the U.S. government was that some of the Common Criteria countries didn't have the capability of evaluating effectively. On the other hand, there are things that are low-cost/high-benefit, even if they don't work against all possible attacks.

Mr. Groman asked for clarification on the proposed recommendation.

The Chair said that they would be recommending consideration of some basic secure software development practice requirements that complement the security features that are already required. NIST just published a white paper on secure development practices, and the recommendation is that NIAP ought to look at it, figure out what cost-effective practices they can readily integrate into their evaluation process, and then move forward with doing that.

The Chair asked if someone wanted to make a motion on a letter to NIAP.

Several Board members expressed some uncertainty about the details of the SSDF.

The Chair said they would come back to that topic at a later date. In the meantime, it might be good to receive another briefing on SSDF.

Appreciation for Departing Board Members:

Mr. Scholl extended his thanks, admiration, and appreciation to Ms. Hatter and Mr. Boyer for their expertise and advice.

Ms. Hatter said that it has been fascinating to see technology from the government perspective. She tells her colleagues to have faith in this part of the government and the technology people who are keeping the wheels on the bus turning. It has been an eye-opening experience for her and she has enjoyed it.

Mr. Boyer said that it has been an honor to serve on the Board for the past 8 years. It has been fascinating to see the inner workings of how government approaches security. NISTS's role has grown, and that is a testament to all the phenomenal work they do and leadership they provide. On the industry side, there is a ton of respect for the work that NIST does and the expertise it brings.

Mr. Romine said that the Board members have made a difference, and he hopes the relationships will be ongoing. Their advice and input has been extremely important and valuable, and NIST is grateful for their candor, even when it wasn't laudatory.

Mr. Groman said he was going to miss them both. They brought a great perspective to the work in government.

The Chair thanked Ms. Hatter and Mr. Boyer for their service, contributions, sense of humor, and leadership.

Mr. Scholl asked everyone to submit feedback on the virtual meeting format. The next meeting is scheduled for October 14, and plans are moving ahead for either an in-person or virtual meeting.

The Chair asked for a motion to adjourn.

A motion was made to adjourn.

With no objections, the Chair adjourned the meeting at 2:33 p.m. ET.

List of Attendees

Last Name	First Name	Affiliation	Role
Brewer	Jeff	NIST	DFO
Romine	Chuck	NIST	Presenter
Kendall	Frank	CSIS	Presenter
Carnahan	Lisa	NIST	Presenter
Connelly	Sean	DHS	Presenter
Greene	Jeff	NIST	Presenter
Baish	Mary	NSA	Presenter
Petersen	Rodney	NIST	Presenter
McCarthy	Jim	NIST	Presenter
Cooper	Michael	NIST	Presenter
Scholl	Matthew	NIST	Presenter
Stine	Kevin	NIST	Presenter
Scarfone	Karen	Scarfone CyberSec.	Presenter
Leiserson	Nick	Rep. Langevin (R.I.)	Presenter
Salisbury	Warren	NIST	Staff
Carlson	Caron	NIST	Staff
Aisenberg	Michael	Mitre	Visitor
Bhardwaj	Kulbhushan	GlobalLogic	Visitor
Delak	Katya	NIST	Visitor
Friedman	Sara	Inside Cybersecurity	Visitor
Geller	Eric	Politico	Visitor
Hatzes	Laura	Exeter Gov. Services	Visitor
Heyman	Matthew	Impresa Mgt. Sol.	Visitor
Ignaszewski	Katie	IBM	Visitor
Johnson	Derek	FCW	Visitor
Kerman	Sara	NIST	Visitor

McConnell	Andrew	Exeter Gov. Services	Visitor
Mercado	Joseph	NICE, NIST	Visitor
Miller	Jason	Fed News Network	Visitor
Reardanz	Penelope	USG	Visitor
Riley	Christina	Satelles, Inc.	Visitor
Santos	Danielle	NIST	Visitor
Shostack	Adam	Shostack & Assoc.	Visitor
Snyder	Julie	Mitre	Visitor
Souppaya	Murugiah	NIST	Visitor
Steinmeier	Frauke	NICE, NIST	Visitor
Weber	Barry	Assured SPC	Visitor
Williams	Lauren	FCW	Visitor
Williquette	Joel		Visitor
Tabassi	Elham	NIST	Visitor
Rojo	Virginia		Visitor
Sedgewick	Adam	NIST	Visitor
Scarborough	Matthew	NIST	Visitor
Monitz	Jenny	DHS	Visitor
Megas	Kat	NIST	Visitor
Ross	Ron	NIST	Visitor
Vespestad	Kirk		Visitor
Name Unknown	Listed as phone #		Visitor
Name Unknown	Listed as guest		Visitor