IDS WG Meeting Minutes
April 20, 2023

This IDS WG Meeting was started at approximately 3:00 pm ET on April 20, 2023.

Attendees

Graydon Dodson	Lexmark
Smith Kennedy	HP
Alan Sukert	
Mike Trent	Xerox
Brian Volkoff	Ricoh
Bill Wagner	TIC

Agenda Items

1. The topics to be covered during this meeting were:
   - Latest status on the HCD iTC and the HCD Interpretation Team (HIT)
   - Special topic on the new National Cybersecurity Strategy.
   - Round Table
2. Meeting began by stating the PWG Anti-Trust Policy which can be found at https://www.pwg.org/chair/membership_docs/pwg-antitrust-policy.pdf and the PWG Intellectual Property Policy which can be found at https://www.pwg.org/chair/membership_docs/pwg-ip-policy.pdf.
3. Al gave a quick status of the HCD iTC and the HIT
   - The last HCD iTC meeting was on April 10th. The key points covered were:
     - JBMIA had no update to provide.
     - NIAP provided no update on when it would provide an Endorsement for the HCD cPP.
     - The ND cPP/SD Version 3.0 was published on April 6th. The major changes included in Version 3.0 are:
       - TLS 1.3 is included and TLS 1.2 is removed (Note: Al is doing an assessment of Version 3.0 against the HCD cPP v1.0 and he found that TLS 1.2 is not removed in ND cPP v3.0)
       - Comments from the CCMC/CCDB were addressed
       - RfIs against v2.2e were included
       - AFL_FLR assurance requirements were included
       - The NIAP SSH Package with some curve restrictions was included
         - No SHA-3 support is included

     There was then a discussion of whether SHA-1 support was removed in v3.0. Turn out it was not. Because SHA1 and SHA2 support has to be removed by 2030 to comply with CNSA 2.0, the ND iTC plans to remove SHA1 in the next ND cPP release. The ND iTC will probably start by removing SHA1 from protocols. The ND iTC will also look at removing support for IKEv1, something the HCD iTC should look at doing also.

     There was also a question about when the HCD cPP will be certified. Typically, a new cPP is certified the first time a product is certified against that cPP. In the case of the HCD cPP, that will likely be by Lexmark under the Canadian Scheme. Per Graydon that may happen within the next month or two.

   Brian than ask about when TLS 1.3 might get into the HCD cPP. Al's view is that TLS 1.3 should not be in HCD cPP v1.0; it should be in the next version of the HCD cPP whether it is v1.1 or v2.0. As to the time frame, per Kwangwoo we could be talking at least 9-12 months at a minimum. Brian was

getting questions from Ricoh in Japan; he will tell them that they do not to hold up any existing certifications waiting from TLS 1.3.

4. Al then went through the current status of the HIT. Al went through a demonstration of the new HCD-IT repository under HCD iTC and the new Interpretation Team project for tracking the issues written against HCD cPP/SD v1.0. the HIT is using GitHub to manage the Request for Interpretation (RfI) process,, and as a result instead of an RFI form a GitHub issue is written for every RfI against the two documents. The issues are accessed through the HCD-IT repository, and each issue written is linked to the Interpretation Team project.

   The Interpretation Team project allows each Issue to be tracked through completion through the following phases:

   - **ToDo** – Awaiting initial action
   - **Awaiting Priority** – Awaiting assigning the issue a priority
   - **Awaiting Review** – Awaiting review of the issue by the HIT subteam assigned to the issue to determine if issue will be accepted
   - **In Progress** – Issue being address by the HIT and a TD or TR created
   - **Completion** – HIT action on the issue completed

   Al then went through the 7 issues that have already been generated against v1.0 of the HCD cPP and SD:

   - HCD-IT #1: The FCS_COP.1/KeyEnc Cryptographic operation (Key Encryption) SFR in HCD cPP v1.0 is inconsistent with TPM 2.0 Architecture specification section "26.6 Sensitive Area Encryption" – This was an issue generated by Graydon where in the FCS_COP.1/KeyEnc SFR the AES requirements only allow the CBC or GCM mode which does not match the TPM 2.0 specification that requires the CFB mode.. This issue was assigned to Brian, Jerry Colunga, Anantha and Joe McDonald from NSA to assess, since it might require changes to both the cPP and SD.
   - HCD-IT #2: Clarification is needed about algorithm verification of Root of Trust in the Test Assurance activities for the Secure Boot SFR – This issue was from Ohya-san to add a note to the Secure Boot test assurance activities saying that the algorithm verification for Root of Trust should be avoided, because authenticity check in Root of Trust should be performed by some kind of immutable code, so the algorithm verification tests should be difficult to perform. This issue was assigned to Jerry Colunga to assess.
   - HCD-IT #3: Extraneous "selection" in SFR FCS_CKM.4 Cryptographic key destruction in HCD cPP v1.0 – This issue was from Tom Benkart to remove an extraneous ‘selection’ in the last line of SFR FCS_CKM,4.1, This issue was rejected as a duplicate of one of the comments in HCD-IT #TBD.
   - HCD-IT NIAP APE_ECD.1-5 Evaluation Comments against the HCD #4: cPP – This is one of four issues related to NIAP assessment of the HCD cPP against the PP requirements of CC:2022 Part 3 as part of certification of the HCD cPP; these four issues must be addressed.

     This particular issue dealt with several comments related to Extended Component Definitions in Chapter D of the HCD cPP not properly using the existing CC Part 2 components as a model for presentation. All four of the NIAP assessment issues were assigned to Brian for initial assessment with the understanding he will need additional help given the extensive work required to address all the issues.
   - HCD-IT #5: NIAP APE_REQ.2-5 Evaluation Comments against the HCD cPP – This is the second of the NIAP assessment issues. This comment dealt with the general comment that incorrect conventions for assignments were used throughout the HCD cPP.

- HCD-IT #6: NIAP APE_REQ.2-8 Assessment Comments against the HCD cPP – This is the third of the NIAP assessment issues. This comment dealt with the general inconsistency as to whether an SFR with a refinement in it starts with "Refinement:" or not.
- HCD-IT #7: NIAP APE_REQ.2-7 Assessment of HCD cPP – This is the fourth of the NIAP assessment comments. This comment dealt with the general inconsistency with regards to whether or not "selection:" prompt is bolded.

One issue that came up in discussing the NIAP comments with the HIT was that the conventions for bolding, use of 'Refinement, etc. are in Section 5.1 of the HCD cPP. The question was whether these were the correct conventions to use; we didn't want Brian to spend the time to fix the comments using the wrong conventions and then have to do it all over again. We are asking NIAP to confirm what is in Section 5.1 are the correct conventions to use.

5. Al presented this week's special topics on the new US National Cybersecurity Strategy. The slides Al used can be found at https://ftp.pwg.org/pub/pwg/ids/Presentation/National Cybersecurity Strategy.pdf.

   Note that for the rest of these minutes the slides contain the full content of what was presented at the meeting; these minutes will only list the key points on each slide that Al singled out during his discussion of the strategy.

   The main items covered in the presentation were:

   - The new National Cybersecurity Strategy was published March 1, 2023 and can be found at https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

     It turns out that the Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, which we have talked about at previous IDS WG Meetings, and the work performed and reports created in response to that Executive Order laid the groundwork for this National Cybersecurity Strategy.

     The main goal of the National Cybersecurity Strategy is to explain how the US will:

     - Defend the homeland by protecting networks, systems, functions, and data;
     - Promote American prosperity by nurturing a secure, thriving digital economy and fostering strong domestic innovation;
     - Preserve peace and security by strengthening the ability of the United States — in concert with allies and partners — to deter and, if necessary, punish those who use cyber tools for malicious purposes; and
     - Expand American influence abroad to extend the key tenets of an open, interoperable, reliable, and secure Internet

     These are the typical types of goals one would expect from a national strategy like this.

   - Slides 3 and 4 described the current landscape that the National Cybersecurity Strategy was built around. The key conditions that Al emphasized were:

     - Rise of the open internet has allowed US competitors and advisories to engage in pernicious economic espionage and malicious cyber activities such as cyber-attacks, cyber-enabled economic espionage and trillions of dollars of intellectual property theft , causing significant economic disruption and harm to individuals, commercial and non-commercial interests, and governments across the world – in fact the open internet is a key thread throughout the strategy
     - Public and private entities have struggled to secure their systems as adversaries increase the frequency and sophistication of their malicious cyber activities

     As a result, the strategy must recognize that:

- Must impose costs if it hopes to deter malicious cyber actors and prevent further escalation – making sure malicious actors pay for their actions is a critical element of any cybersecurity strategy
- Must retain the promise of an open, interoperable, reliable, and secure Internet to strengthen and extend our values and protect and ensure economic security for American workers and companies
- The US is vulnerable to peacetime cyber-attacks against critical infrastructure, and the risk is growing that these countries will conduct cyber-attacks against the United States during a crisis short of war – vulnerability of infrastructure is another theme throughout the strategy
- These adversaries are continually developing new and more effective cyber weapons – our enemies are continually getting better so we have to get better as stopping them

- The National Cybersecurity Strategy is made up of four Pillars:
  - **Protect the American People, the Homeland, and the American Way of Life**

    Will require a series of coordinated actions focused on protecting government networks, protecting critical infrastructure, and combating cybercrime
  - **Promote American Prosperity**

    Need to demonstrate a coherent and comprehensive approach to address challenges that threaten our national security in this increasingly digitized world – the key here is the fact that the strategy has to apply to "a digitized world"
  - **Preserve Peace through Strength**

    Need to issue transformative policies that reflect today's new reality where Cyberspace is no longer treated as a separate category of policy or activity disjointed from other elements of national power
  - **Advance American Influence**

    Need to maintain an active international leadership posture to advance American influence and to address an expanding array of threats and challenges to its interests in cyberspace

  Each Pillar has a set of high-level Steps and methods for achieving those pillars that the remaining slides described and which will be summarized below.

  a. Pillar I: **Protect the American People, the Homeland, and the American Way of Life**

     The objective of Pillar 1 is to manage cybersecurity risks to increase the security and resilience of the Nation's information and information systems. Pillar has 3 Steps as follows:

     - Step 1 - **Secure Federal Networks and Information** by**:**
       - **FURTHER CENTRALIZE MANAGEMENT AND OVERSIGHT OF FEDERAL CIVILIAN CYBERSECURITY** through
         - Further enabling the Department of Homeland Security (DHS) to secure Federal department and agency networks, with the exception of national security systems
         - Deploying centralized capabilities, tools, and services through DHS where appropriate, and improve oversight and compliance with applicable laws, policies, standards, and directives
       - **ALIGN RISK MANAGEMENT AND INFORMATION TECHNOLOGY ACTIVITIES** through
         - Department and agency leaders empowering and holding their CIOs accountable to align cybersecurity risk management decisions and IT budgeting and procurement decisions
         - The Administration, through OMB and DHS, guiding and directing risk management actions across Federal civilian departments and agencies, and CIOs will be empowered to take a proactive leadership role in assuring IT

procurement decisions assign the proper priority to securing networks and data - risk management is another theme that goes across the entire strategy

- **IMPROVE FEDERAL SUPPLY CHAIN RISK MANAGEMENT** through
  - Integrating supply chain risk management into agency procurement and risk management processes in accordance with federal requirements that are consistent with industry best practices
  - Ensure, where appropriate, that Federal contractors receive and use all relevant and shareable threat and vulnerability information

  It is important that the strategy covers supply chain risk management as well as sharing threat intelligence with Federal contractors in the strategy; you will see involvement of Federal contractors a lot in this strategy.

- **STRENGTHEN FEDERAL CONTRACTOR CYBERSECURITY** through
  - Assessing the security of its data by reviewing contractor risk management practices and adequately testing, hunting, censoring, and responding to incidents on contractor systems
  - Ensuring, where appropriate, that Federal contractors receive and use all relevant and shareable threat and vulnerability information

  Again, see the emphasis in involving Federal contractors in the strategy.

- **ENSURE THE GOVERNMENT LEADS IN BEST AND INNOVATIVE PRACTICES through**
  - Ensuring the systems it owns and operates meet the standards and cybersecurity best practices it recommends to industry
  - Being a leader in developing and implementing standards and best practices in new and emerging areas such as quantum computing

  Involvement in generating standards and meeting standards and best practices is both key themes that appear throughout the strategy.

- **Step 2 - Support Critical Infrastructure** by**:**
  - **REFINE ROLES AND RESPONSIBILITIES** through
    - Clarifying the roles and responsibilities of Federal agencies and the expectations on the private sector related to cybersecurity risk management and incident response
    - Identify and bridge existing gaps in responsibilities and coordination among Federal and non-Federal incident response efforts and promote more routine training, exercises, and coordination

      This is pretty straightforward

  - **PRIORITIZE ACTIONS ACCORDING TO IDENTIFIED NATIONAL RISKS** through
    - Working with the private sector to manage risks to critical infrastructure at the greatest risk
    - Prioritizing risk-reduction activities across seven key areas: national security, energy and power, banking and finance, health and safety, communications, information technology, and transportation

    The seven key areas listed are ones we have seen in the news recently, which solidifies why they were chosen as areas that should be emphasized for risk-reduction.

- **LEVERAGE INFORMATION AND COMMUNICATIONS TECHNOLOGY PROVIDERS AS CYBERSECURITY ENABLERS** through
  - Strengthening efforts to share information with ICT providers to enable them to respond to and remediate known malicious cyber activity at the network level
  - Promoting an adaptable, sustainable, and secure technology supply chain that supports security based on best practices and standards
  - Encouraging industry-driven certification regimes that ensure solutions can adapt in a rapidly evolving market and threat landscape

  It is important that ICT providers are involved, Also, the last bullet is one that the Common Criteria is keenly aware of – to be more agile to better adapt as the threat landscape changes.

- **PROTECT OUR DEMOCRACY** through
  - When requested, providing technical and risk management services, support training and exercising, maintain situational awareness of threats to this sector, and improve the sharing of threat intelligence
  - Coordinating the development of cybersecurity standards and guidance to safeguard the electoral process and the tools that deliver a secure system

  Given what happened on Jan 6, 2021, one would expect protection of elections and election security to be a key tenant of this strategy.

- **INCENTIVIZE CYBERSECURITY INVESTMENTS** through
  - Working with private and public sector entities to promote understanding of cybersecurity risk so they make more informed risk-management decisions, invest in appropriate security measures, and realize benefits from those investments

- **PRIORITIZE NATIONAL RESEARCH AND DEVELOPMENT INVESTMENTS** through
  - Updating the National Critical Infrastructure Security and Resilience Research and Development Plan to set priorities for addressing cybersecurity risks to critical infrastructure
  - Aligning investments to the priorities, which will focus on building new cybersecurity approaches that use emerging technologies, improving information-sharing and risk management related to cross-sector interdependencies, and building resilience to large-scale or long-duration disruptions

- **IMPROVE TRANSPORTATION AND MARITIME CYBERSECURITY** through
  - Clarifying maritime cybersecurity roles and responsibilities; promote enhanced mechanisms for international coordination and information sharing; and accelerate the development of next-generation cyber-resilient maritime infrastructure
  - Assuring the uninterrupted transport of goods in the face of all threats that can hold this inherently international infrastructure at risk through cyber means

  We sometimes forget the importance of shipping. However, given the experience from the Pandemic and the affect the clogged ports had on the supply chain and shortages in grocery stores, making sure our transportation, including maritime shipping, is secure is a critical task.

- **IMPROVE SPACE CYBERSECURITY** through
  - Enhancing efforts to protect our space assets and support infrastructure from evolving cyber threats
  - Working with industry and international partners to strengthen the cyber resilience of existing and future space systems

  The strategy even has to account for any future space involvement.

- **Step 3 - Combat Cybercrime and Improve Incident Reporting** by**:**
  - **IMPROVE INCIDENT REPORTING AND RESPONSE** through
    - Encouraging reporting of intrusions and theft of data by all victims, especially critical infrastructure partners
  - **MODERNIZE ELECTRONIC SURVEILLANCE AND COMPUTER CRIME LAWS** through
    - Working with the Congress to update electronic surveillance and computer crime statutes to enhance law enforcement's capabilities to lawfully gather necessary evidence of criminal activity, disrupt criminal infrastructure through civil injunctions, and impose appropriate consequences upon malicious cyber actors

    This is an area that has been in the news a lot lately and one law enforcement wants badly. As seen below, methods related to law enforcement occur frequently in this strategy.
  - **REDUCE THREATS FROM TRANSNATIONAL CRIMINAL ORGANIZATIONS IN CYBERSPACE** through
    - Advocating for law enforcement to have effective legal tools to investigate and prosecute transnational criminal groups and modernized organized crime statutes for use against computer hacking
  - **IMPROVE APPREHENSION OF CRIMINALS LOCATED ABROAD** through
    - Identify gaps and potential mechanisms for bringing foreign based cyber criminals to justice
    - Increase diplomatic and other efforts with countries to promote cooperation with legitimate extradition requests
    - Push other nations to expedite their assistance in investigations and to comply with any bilateral or multilateral agreements or obligations

    All reasonable things to want to do.
  - **STRENGTHEN PARTNER NATIONS' LAW ENFORCEMENT CAPACITY TO COMBAT CRIMINAL CYBER ACTIVITY** through
    - Continue building cybercrime-fighting capacity that facilitates stronger international law enforcement cooperation
    - Improve international cooperation in investigating malicious cyber activity, including developing solutions to potential barriers to gathering and sharing evidence
    - Lead in developing interoperable and mutually beneficial systems to encourage efficient cross-border information exchange for law enforcement purposes and reduce barriers to coordination
    - Urge effective use of existing international tools like the UN Convention Against Transnational Organized Crime

Given President Biden's history, working with our international partners was going to be an integral part of this strategy, and you will see it throughout the four Pillars.

b. Pillar II: **Promote American Prosperity**

The objective of Pillar II is to preserve United States influence in the technological ecosystem and the development of cyberspace as an open engine of economic growth, innovation, and efficiency. Pillar II has 3 Steps as follows:

- Step 1 - **Secure Federal Networks and Information** by**:**
  - **Foster a Vibrant and Resilient Digital Economy** through
    - Working across stakeholder groups, including the private sector and civil society, to promote best practices and develop strategies to overcome market barriers to the adoption of secure technologies
    - Improving awareness and transparency of cybersecurity practices to build market demand for more secure products and services
    - Collaborating with international partners to promote open, industry-driven standards with government support, as appropriate, and risk-based approaches to address cybersecurity challenges

      Note again the common themes here of promoting best practices and promoting standards.
  - **PRIORITIZE INNOVATION**
    - Promoting implementation and continuous updating of standards and best practices that deter and prevent current and evolving threats and hazards in all domains of the cyber ecosystem
    - Eliminating policy barriers that inhibit a robust cybersecurity industry from developing, sharing, and building innovative capabilities to reduce cyber threats

    Eliminating barriers shows several other times also.
  - **INVEST IN NEXT GENERATION INFRASTRUCTURE**
    - Facilitating the accelerated development and rollout of next-generation telecommunications and information communications infrastructure in the US
    - Working with the private sector to facilitate the evolution and security of 5G, examine technological and spectrum-based solutions, and lay the groundwork for innovation beyond next-generation advancements
    - Examining the use of emerging technologies, such as artificial intelligence and quantum computing, while addressing risks inherent in their use and application
    - Collaborating with the private sector and civil society to understand trends in technology advancement

    Note the references here to AI and quantum computing which are becoming big areas of importance. Also notice the mention of security of 5G, which is a big issue in mobile communications.
  - **PROMOTE THE FREE FLOW OF DATA ACROSS BORDERS**
    - Continuing to lead by example and push back against unjustifiable barriers to the free flow of data and digital trade
    - Continuing to work with international counterparts to promote open, industry driven standards, innovative products, and risk-based approaches that permit global innovation and the free flow of data

- **MAINTAIN UNITED STATES LEADERSHIP IN EMERGING TECHNOLOGIES**
  - Making a concerted effort to protect cutting edge technologies, including from theft by our adversaries, support those technologies' maturation, and, where possible, reduce United States companies' barriers to market entry
  - Promoting US cybersecurity innovation worldwide through trade-related engagement, raising awareness of innovative American cybersecurity tools and services, exposing and countering repressive regimes use of such tools and services to undermine human rights, and reducing barriers to a robust global cybersecurity market

  Protecting theft of US technologies will show up later in Pillar II.

- **PROMOTE FULL-LIFECYCLE CYBERSECURITY**
  - Promoting full-lifecycle cybersecurity, pressing for strong, default security settings, adaptable, upgradeable products, and other best practices built in at the time of product delivery
  - Promoting foundational engineering practices to reduce systemic fragility and develop designs that degrade and recover effectively when successfully attacked
  - Promoting regular testing and exercising of the cybersecurity and resilience of products and systems during development using best practices from forward-leaning industries
  - Pushing the promotion and use of coordinated vulnerability disclosure, crowd-sourced testing, and other innovative assessments that improve resiliency ahead of exploitation or attack
  - Evaluating how to improve the end-to-end lifecycle for digital identity management, including over-reliance on Social Security numbers

  It was nice to see the strategy place importance of promoting a secure lifecycle. The last bullet was interesting in promoting a digital identification in place of Social Security numbers; it would be great if that would actually happen.

- **Step 2. Foster and Protect United States Ingenuity** by**:**
  - **UPDATE MECHANISMS TO REVIEW FOREIGN INVESTMENT AND OPERATION IN THE UNITED STATES**
    - Formalizing and streamlining the review of Federal Communications Commission referrals for telecommunications licenses
    - Facilitating a transparent process to increase the efficiency of this review
  - **MAINTAIN A STRONG AND BALANCED INTELLECTUAL PROPERTY PROTECTION SYSTEM**
    - Continuing to help foster a global intellectual property rights system that provides incentives for innovation through the protection and enforcement of intellectual property rights
    - Promoting protection of sensitive emerging technologies and trade secrets
    - Preventing adversarial nation states from gaining unfair advantage at the expense of American research and development

    The last bullet is critical for IP protection.

- **PROTECT THE CONFIDENTIALITY AND INTEGRITY OF AMERICAN IDEAS**
  - Working against the illicit appropriation of public and private sector technology and technical knowledge by foreign competitors, while maintaining an investor-friendly climate

- **Step 3. Develop a Superior Cybersecurity Workforce** by**:**
  - **BUILD AND SUSTAIN THE TALENT PIPELINE**
    - Continuing to invest in and enhance programs that build the domestic talent pipeline, from primary through postsecondary education
    - Leveraging the President's proposed merit-based immigration reforms to ensure that the United States has the most competitive technology sector
  - **EXPAND RE-SKILLING AND EDUCATIONAL OPPORTUNITIES FOR AMERICA'S WORKERS**
    - Working with the Congress to promote and reinvigorate educational and training opportunities to develop a robust cybersecurity workforce
  - **ENHANCE THE FEDERAL CYBERSECURITY WORKFORCE**
    - Continuing to use the National Initiative for Cybersecurity Education (NICE) Framework to support policies allowing for a standardized approach for identifying, hiring, developing, and retaining a talented cybersecurity workforce
    - Exploring appropriate options to establish distributed cybersecurity personnel under the management of DHS
    - Promoting appropriate financial compensation for the US Government workforce, as well as unique training and operational opportunities
  - **USE EXECUTIVE AUTHORITY TO HIGHLIGHT AND REWARD TALENT**
    - Promoting and magnify excellence by highlighting cybersecurity educators and cybersecurity professionals
    - Leveraging public-private collaboration to develop and circulate the NICE Framework, which provides a standardized approach for identifying cybersecurity workforce gap
    - Implementing actions to prepare, grow, and sustain a workforce that can defend and bolster America's critical infrastructure and innovation base

    All four of these tasks under Step 3 and their methods are what one would expect to be proposed to build a cybersecurity workforce within the US.

c. Pillar III: **Preserve Peace Through Strength**

The objective of Pillar III is to identify, counter, disrupt, degrade, and deter behavior in cyberspace that is destabilizing and contrary to national interests, while preserving United States overmatch in and through cyberspace. Pillar III has 2 steps as follows:

- Step 1 - **Enhance Cyber Stability through Norms of Responsible State Behavior** by**:**
  - **ENCOURAGE UNIVERSAL ADHERENCE TO CYBER NORMS**
    - Encouraging other nations to publicly affirm International law and voluntary non-binding norms of responsible state behavior in cyberspace) through enhanced outreach and engagement in multilateral fora

      At the time of the meeting Al didn't know what "fora" meant. Turns out it is the plural of forum.

Step 2. Attribute and Deter Unacceptable Behavior in Cyberspace by**:**

- **LEAD WITH OBJECTIVE, COLLABORATIVE INTELLIGENCE**
  - Leading the world in the use of all-source cyber intelligence to drive the identification and attribution of malicious cyber activity that threatens United States national interests
  - Sharing Objective and actionable intelligence across the United States Government and with key partners to identify hostile foreign nation states, and non-nation state cyber programs, intentions, capabilities, research and development efforts, tactics, and operational activities

  Again, emphasized the themes of collaboration and sharing of intelligence

- **IMPOSE CONSEQUENCES**
  - Developing swift and transparent consequences, which we will impose consistent with our obligations and commitments to deter future bad behavior
  - Conducting interagency policy planning for the time periods leading up to, during, and after the imposition of consequences to ensure a timely and consistent process for responding to and deterring malicious cyber activities
  - Working with partners when appropriate to impose consequences against malicious cyber actors in response to their activities against our nation and interests

  Emphasizes that a key to a good cybersecurity strategy is having strong consequences to any malicious actor that even attempts to perform a cybersecurity attack against the US.

- **BUILD A CYBER DETERRENCE INITIATIVE**
  - Launching an international Cyber Deterrence Initiative to build broader coalition of like-minded states and develop tailored strategies to ensure adversaries understand the consequences of their malicious cyber behavior
  - Working with like-minded states to coordinate and support each other's responses to significant malicious cyber incidents, including through intelligence sharing, buttressing of attribution claims, public statements of support for responsive actions taken, and joint imposition of consequences against malign actors

  Like so many tasks before, this strategy relies heavily on international cooperation.

- **COUNTER MALIGN CYBER INFLUENCE AND INFORMATION OPERATIONS**
  - Using all appropriate tools of national power to expose and counter the flood of online malign influence and information campaigns and non-state propaganda and disinformation

  Al was glad to see that the strategy included a task to fight misinformation.

d. Pillar IV: **Advance American Influence**

The objective of Pillar IV is to preserve the long-term openness, interoperability, security, and reliability of the Internet, which supports and is reinforced by United States interests. Pillar IV has 2 steps as follows:

- Step 1 - **Promote an Open, Interoperable, Reliable, and Secure Internet** by**:**
  - **PROTECT AND PROMOTE INTERNET FREEDOM**
    - Encourage other countries to advance Internet freedom through venues such as the Freedom Online Coalition, of which the United States is a founding member

Note: 'Internet Freedom' in this context is defined as online exercise of human rights and fundamental freedoms — such as the freedoms of expression, association, peaceful assembly, religion or belief, and privacy rights online — regardless of frontiers or medium. By extension, Internet freedom also supports the free flow of information online that enhances international trade and commerce, fosters innovation, and strengthens both national and international security

This task just emphasized the major theme of the strategy of ensuring an open, free internet.

- **WORK WITH LIKE-MINDED COUNTRIES, INDUSTRY, ACADEMIA, AND CIVIL SOCIETY**
  - Continue to work with like-minded countries, industry, civil society, and other stakeholders to advance human rights and Internet freedom globally and to counter authoritarian efforts to censor and influence Internet development
  - Continue to support civil society through integrated support for technology development, digital safety training, policy advocacy, and research

You see how this strategy mirrors the goals of the Biden administration.

- **PROMOTE A MULTI-STAKEHOLDER MODEL OF INTERNET GOVERNANCE**
  - Continue to actively participate in global efforts to ensure that the multi-stakeholder model of Internet governance (characterized by transparent, bottom-up, consensus-driven processes) prevails against attempts to create state-centric frameworks that would undermine openness and freedom, hinder innovation, and jeopardize the functionality of the Internet
  - Will defend the open, interoperable nature of the Internet in multilateral and international fora through active engagement in key organizations, such as the Internet Governance Forum, the United Nations, and the International Telecommunication Union

Multi-stakeholder model is a new term Al hadn't heard before.

- **PROMOTE INTEROPERABLE AND RELIABLE COMMUNICATIONS INFRASTRUCTURE AND INTERNET CONNECTIVITY**
  - Promote communications infrastructure and Internet connectivity that is open, interoperable, reliable, and secure
  - Support and promote open, industry-led standards activities based on sound technological principles

No additional comments beyond just reinforcing open internet.

- **PROMOTE AND MAINTAIN MARKETS FOR UNITED STATES INGENUITY WORLDWIDE**
  - Continue to promote markets for American ingenuity overseas, including for emerging technologies that can lower the cost of security
  - Advise on infrastructure deployments, innovation, risk management, policy, and standards to further the global Internet's reach and to ensure interoperability, security, and stability
  - Work with international partners, government, industry, civil society, technologists, and academics to improve the adoption and awareness of cybersecurity best practices worldwide

Another instance of pushing standards and best practices as part of the strategy.

Step 2. Build International Cyber Capacity by**:**

- **ENHANCE CYBER CAPACITY BUILDING EFFORTS**
  - Work to strengthen the capacity and interoperability of our allies and partners to improve our ability to optimize our combined skills, resources, capabilities, and perspectives against shared threats
  - Continue to address the building blocks for organizing national efforts on cybersecurity
  - Aggressively expand efforts to share automated and actionable cyber threat information, enhance cybersecurity coordination, and promote analytical and technical exchanges
  - Work to reduce the impact and influence of transnational cybercrime and terrorist activities by partnering with and strengthening the security and law enforcement capabilities of our partners to build their cyber capacity

  This set of tasks kind of sums up everything that came before it.

After Al finished his presentation Smith asked a very important question – how does the PWG fit into this National Cybersecurity Strategy. The group had a nice discussion of the question and felt thar the PWG's work on developing IPP standards certainly was aligned with the strategy's emphasis in standards as a key component. Also, the IDS WG's support of the work on the HCD iTC to develop the HCD cPP/SD falls into this "standards" emphasis of the strategy. However, the group agreed that this is a question that the Steering Committee and the IPP and IDS WGs should address individually. Al agreed that this would be a topic at the next IDS WG meeting.

6. There was no Round Table at today's meeting.
7. **Actions:** None

Next Steps

- The next IDS WG Meeting will be May 4, 2023 at 3:00P ET / 12:00N PT. Main topics will review of slide for the IDS Session at the May PWG Face-to-Face, the latest status of the HCD iTC and HIT, the role of the IDS WG in the National Cybersecurity Strategy (and Cybersecurity in general) and maybe a special topic on a topic TBD if time permits.
- The IDS Session at the May PWG Face-to-Face will be on May 18, 2023 at 10:00A ET / 7:00A PT.