IDS WG Meeting Minutes
September 21, 2023

This IDS WG Meeting was started at approximately 3:00 pm ET on September 21, 2023.

Attendees

Graydon Dobson	Lexmark
Smith Kennedy	HP
Jeremy Leber	Lexmark
Alan Sukert	
Brian Volkoff	Ricoh

Agenda Items

1. The topics to be covered during this meeting were:
   - Latest updates on the HCD iTC and the HCD Interpretation Team (HIT)
   - Special Topic on Initial Public Review version of NIST Cybersecurity Framework 2.0
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 began discussing the results of the September 18th HCD Integration Team (HIT) Meeting:
   - Regarding Issues HIT-IT #4 – HIT IT #7, Brian had two questions related to the SFR style conventions in Section 5.1 that he needed clarified that he needed clarified before he could complete work on these four issues.
     - The first one was against SFR FCS_FCM.4.1. At the end of the SFR there is the requirement "] that meets the following: [**selection: *no standard***]." NIAP felt the [**selection: *no standard***] did not follow the conventions stated in Section 5.1 of the HCD cPP. The resolution to address this requirement that was to both NIAP and the Canadian Scheme was [***no standard***]. Brian will implement that solution.
     - The second question was about SFR FMT_MSA.3.2. The specific issue was that this SFR was stated as a Refinement of the version of the SFR in CC Part 2. NIAP's comment was that this was not a refinement of the CC Part 2 SFR and should not be labeled as a "Refinement".

       The CC Part 2 SFR FMT_MSA_3.2 states

       The TSF shall allow the [assignment: *the authorised identified roles*] to specify alternative initial values to override the default values when an object or information is created."

       The HCD cPP modified FMT_MSA.3.2 to read

       The TSF shall allow the [***selection: U.ADMIN, no role***] to specify alternative initial values to override the default values when an object or information is created.

       Now the main requirement of a Refinement to an SFR is that it must make the requirement stricter the original requirement being modified. In this case, the HCD cPP changed the assignment statement in the CC Part 2 version to a selection statement. It was argued by the Canadian Scheme member on the HIT that by doing that it did make the requirement stricter because a selection is a stricter requirement that an assignment, which in turn made what the HCD iTC did to FMT_MSA.3.2 in the HCD cPP is a true Refinement of the version in CC Part 2.

       The HIT members agreed to go with this interpretation in this case and in all similar situations where a selection replaces an assignment in an SFR will be considered a Refinement.
   - We next discussed an issue brought up by in an email discussion. The issue was that in working on issue HCD-IT #2, Jerry Colunga noticed multiple SFRs in the HCD cPP listed

FCS_COP.1/CMAC Cryptographic Operation (for keyed-hash message authentication) as a dependency. However, the HCD cPP defines in Section A.4.3 this SFR as FCS_COP.1/CMAC Cryptographic Operation (for cipher-based message authentication) and not as FCS_COP.1/CMAC Cryptographic Operation (for keyed-hash message authentication).

Jerry noted the SD specifies EAs for FCS_COP.1/CMAC Cryptographic Operation (for cipher-based message authentication).

After Al gave a brief history of how the FCS_COP.1/CMAC SFR was created, the HIT members agreed that this was clearly an editorial or a "cut and paste" error – the title of FCS_COP.1/CMAC in the various Dependency lists is wrong and needs to be changed to the correct title FCS_COP.1/CMAC Cryptographic Operation (for cipher-based message authentication). Al agreed to write up the formal Issue for this error.

- We then did a quick status of the remaining open Issues:
  - HCD-IT #1: Tom Benkart is working on the final text to give to Kwangwoo that he will give to our CCDB Liaison for CCDB review. The goal is to get CFB mode under AES for FCS_COP.1/KeyEnc in the CCDB "Crypto Spec".
  - HCD-IT #2: Since the various iTCs have no common file naming convention for the files containing the fixes for Issues documented by TDs, Jerry will come up with a file naming convention the HIT will use.
  - HCD-IT #8: Joe McDonald stated he needs more information on the path forward to properly address the threat of the data stored in NVM being removed from the device.
  - HCD-IT #9: Jerry will fix this issue as soon as he finishes HCD-IT #2.
  - HCD-IT #10: We will go through resolution of this issue on-line as a team at the beginning of the next HIR Meeting.
  - HCD-IT #11: Waiting on AL to complete his action to determine why the HCD PP only required plaintext keys to be destroyed and not all keys to be destroyed.
  - HCD-IT #12: Cory (the Canadian Scheme rep on the HIT) included a note in the Issue proposing updated to several of the threat definitions in the HCD cPP. Al gave everyone on the HIT the action to review Cory's threat definition updates before the next HIT Meeting.
  - HCD-IT #13: The solution to this issue was agreed upon by the HIT at the previous HIT Meeting.

4. Al then presented his special topic for the day, which is a look at Initial Public Review version of NIST Cybersecurity Framework 2.0. The slides for this presentation can be found at https://ftp.pwg.org/pub/pwg/ids/Presentation/NIST Cybersecurity Framework v2.0.pdf.

   Al state that NIST Cybersecurity Framework 2.0 is very different from NIST Cybersecurity Framework 1.0; the principal differences were the inclusion of categories and subcategories related to the cybersecurity protection of the supply chain and the inclusion of a new core function – the Govern function. It also turned out a lot of the subcategories in NIST Cybersecurity Framework 1.0 were moved around to different core functions and/or categories.

   a. The potential uses of : NIST Cybersecurity Framework 2.0 are to:
      - Create and use Framework Profiles to understand, assess, and communicate the organization's current or target cybersecurity posture in terms of the Framework Core's cybersecurity outcomes, and prioritize outcomes for achieving the target cybersecurity posture
      - Assess the organization's achievement of cybersecurity outcomes
      - Characterize cybersecurity risk management outcomes with Framework Tiers
      - Improve cybersecurity communication with internal and external stakeholders
      - Manage cybersecurity risk throughout supply chains

Al noted the inclusion of the supply chain risks here

b. As was the case in NIST Cybersecurity Framework 1.0, NIST Cybersecurity Framework 2.0 is comprised of three core components::

- **Framework Core** - a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors
- **Framework Implementation Tiers ("Tiers") -** Describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the Framework (e.g., risk and threat aware, repeatable, and adaptive)
- **Framework Profile ("Profile")**: represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories

Slide 3 has more details about these components.

c. Regarding Framework Profiles, they are used to understand, assess, prioritize, and tailor the sector- and technology-neutral Core outcomes (i.e., Functions, Categories, and Subcategories) based on an organization's mission objectives, stakeholder expectations, threat environment, and requirements and leading practices – consider a profile a snapshot in time of where an organization is with respect to the various framework core functions.

- A *Current Profile* that covers the Core's outcomes that an organization is currently achieving (or attempting to achieve) and characterizes how or to what extent each outcome is being achieved
- A *Target Profile* that covers the desired outcomes that an organization has selected and prioritized from the Core for achieving its cybersecurity risk management objectives.

  In other words, a Current Profile gives you a snapshot of where you are and a Target Profile is snapshot of where you want to be.

Slide 5 lists several ways in which a Framework Profiles can be used. Among them are:

- Compare current cybersecurity practices to sector-specific standards and regulatory requirements
- Set cybersecurity goals for the organization, identify gaps between current practices and the goals, and plan how to address the gaps in a cost-effective manner
- Assess progress toward achieving the organization's cybersecurity goals
- Determine where the organization may have cybersecurity gaps with respect to an emerging threat or a new technology
- Express the organization's cybersecurity requirements and expectations to suppliers, partners, and other third parties

d. Regarding Framework "Tiers", they are very similar to Capability Maturity Model maturity levels Al used to work with when he first stared at Xerox back in 1995. Slides 6-8 define the four Tier levels in the NIST Cybersecurity Framework. The four levels are

- Tier 1: Partial – generally characterized by ad-hoc or lack of process and procedures related to risk management and cybersecurity
- Tier 2: Risk Informed: Risk management procedures are in place; There is an awareness of cybersecurity risks at the organizational level, but an organization-wide approach to managing cybersecurity risks has not been established
- Tier 3: Repeatable: Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed; Is an organization-wide approach to managing cybersecurity risks
- Tier 4: Adaptive: An organization-wide approach to managing cybersecurity risks that uses risk-informed policies, processes, and procedures to address potential cybersecurity events;

Organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators

Slide 10 lists ways the formulation of these Tiers can be used. Among them are:

- Help set the overall tone for how cybersecurity risks will be managed within the organization, and determine the effort required to reach a selected Tier
- Capture an organization's outcomes over a range, from Partial (Tier 1) to Adaptive (Tier 4)
- Reflect a progression from informal, ad hoc responses to approaches that are agile, risk-informed, and continuously improving

e. The Frame Core is made up of 6 Core Functions:

- **Govern (GO) -** Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy
- **Identify (ID)** – Help determine the current cybersecurity risk to the organization
- **Protect (PR)** – Use safeguards to prevent or reduce cybersecurity risk
- **Detect (DE)** – Find and analyze possible cybersecurity attacks and compromises
- **Respond (RS)** – Take action regarding a detected cybersecurity incident
- **Recover** – Restore assets and operations that were impacted by a cybersecurity incident

Each Core Function is composed of a number of categories and subcategories. Slides 11 and 12 list the Categories for each of the 6 core functions.

The remaining slides detail the Categories and associated subcategories for each of the core functions. Al did not go through all of the Category/Subcategory slides in detail during the meeting so only the highlights will be presented in these minutes. See the complete slides in the link above to see the details for all the category/subcategory pairs.

i. Govern Function

Al noted that many of the categories and subcategories in the Govern function came from other categories and subcategories in NIST Cybersecurity Framework 1.0.

Al noted nothing of significance on Slide 13 (Organizational Context Category). Slides 14 and 15 were significant because they included the Cybersecurity Supply Chain Risk Management Category and its associated subcategories which are all new and a major focus of NIST Cybersecurity Framework 2.0. Some of the interesting subcategories for this category are:

- Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle
- Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties
- The risks posed by a supplier, their products and services, and other third parties are identified, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship
- Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships

Al noted that based on his experience when he worked quality assurance for GE back in the 80s it is very important to make sure suppliers and third parties have the same quality and risk management focus as the main contractor.

The remaining Categories and Subcategories for the Govern Function in Slides 16-18 involved establishing cybersecurity roles and responsibilities; organizational cybersecurity

policies, processes and procedures; supply chain cybersecurity risk management and review of organizational cybersecurity risk management activities.

ii. Identity Function

Al noted in the first category, Asset Management, on Slide 19 the importance of maintaining inventories of all assets, including not just the hardware but all the software and firmware. Al also emphasized the subcategory "Systems, hardware, software, and services are managed throughout their life cycle".

A lot of the Categories/Subcategories that we formerly in the Identity Function in NIST Cybersecurity Framework 1.0 were denoted as "Dropped" in NIST Cybersecurity Framework 2.0. Smith asked if that meant they were really dropped; Al indicated it was really a poor choice of words, for they were in fact just moved to a different Function.

The subcategories associated with risk assessment in Slides 21 and 22 are the core of the Identity function. It was interesting, though, that the Improvement category that included a "Lessons :Learned" subcategory on Slide 23 was part of the Identity Function.

iii. Protect Function

Like the Identity Function, much of what used to be in the Protect Function in NIST Cybersecurity Framework 1.0 was moved to other functions in NIST Cybersecurity Framework 2.0. What was left did include some important Categories such as Identity Management, Authentication, and Access Control on Slides 24 and 25 and Data Security on Slide 27.

Data Security included two important categories from an IDS perspective – "The confidentiality, integrity, and availability of data-at-rest are protected" and "The confidentiality, integrity, and availability of data-in-transit are protected".

One other interesting subcategory Al pointed out under the Protect Function was under the Platform Security category – "Secure software development practices are integrated and their performance is monitored throughout the software development life cycle'. Al was glad the Framework explicitly called out for this.

Finally, Al pointed out under the Technology Infrastructure Resilience category the importance of "Networks and environments are protected from unauthorized logical access and usage" subcategory

iv. Detect Function

In the Continuous Monitoring category there are key subcategories like "Networks and network services are monitored to find potentially adverse events" and "Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events".

Outside of the Continuous Monitoring and Adverse Event Analysis categories, most of what was in the Detect category in NIST Cybersecurity Framework 1.0 was moved to other functions in NIST Cybersecurity Framework 2.0.

v. Response Function

Al did not discuss in any detail the categories/subcategories under the Response function in Slides 34 and 35 except to say that they are the types of things one would expect in a "Response" category – implementing incident response plans and analyzing incidents to determine root cause(s).

vi. Recover Function

Slides 36 and 37 cover the categories/subcategories under the Recover function. Basically, they involve implementing incident recovery plans and communicating the statis on the recovery effort.

5. **Actions:** None

Next Steps

The next IDS WG Meeting will be October 5, 2023 at 3:00P ET / 12:00N PT. Main topics will be the latest status of the HCD iTC and HIT and likely a special topic on a TBD topic