IDS WG Meeting Minutes
October 20, 2022

This IDS WG Meeting was started at approximately 3:00 pm ET on October 20, 2022.

Attendees

Matt Glockner	Lexmark
Jeremy Leber	Lexmark
Ira McDonald	High North
Alan Sukert	
Brian Volkoff	Ricoh
Bill Wagner	TIC
Steve Young	Canon

Agenda Items

1. The topics to be covered during this meeting were:
   - Review of the HCD iTC Meetings since our last IDS WG Meeting on 10/6/22
   - Follow-up to the review of the Security Page on the PWG web site at the request of the PWG Steering Committee (SC) done at the 9/22/22 and 10/6/22 IDS WG Meetings
   - Special topic on NIST SP 800-37Rev 2 – NIST Risk Management Framework (RMF)
   - 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 provided a quick summary of what was covered at the HCD iTC Meetings since the last IDS Workgroup meeting on 10/6/22:
   - The good news is that the HCD cPP is completed and all Final Draft comments have been addressed. The only thing that was left going into the 10/17/22 HCD iTC meeting was to correct the Revision information in the document.
   - For the HCD SD, all but four Final Draft comments had been addressed. We reviewed the four unresolved comments at the 10/17/22 HCD iTC Meeting and agreed on resolution for 3 of the 4 comments; the fourth comment required a change to the agreed resolution for that comment because the initial resolution was not completely correct. The NIAP representative came up with a proposed change off-line that is to be reviewed and agreed upon by the full HCD iTC via email no later that Friday Oct 21st. The proposed change will require a small modification to the Application Note in the HCD cPP for the FCS_KYP_EXT.1 SFR.
   - The current plan is to have both the "final" HCD cPP v1.0 and the HCD SD v1.0 ready for publishing by Oct 25th. At that time the HCD SD v1.0 will be sent to the Common Criteria Development Board (CCDB) for its review so that the HCD SD can be approved by the CCDB per the cPP Development Process at its next meeting which will be the week of November 6th. The HCD cPP v1.0 and HCD SD 1.0 should be published by Oct 28th and listed on the Common Criteria portal soon thereafter.
   - Ira mentioned that the ND cPP/SD v3.0 was submitted for final review on Oct 3rd, which comments due by Oct 30th. The plan of the ND iTC is to publish ND cPP/SD v3.0 sometime in 1Q 2023. Ira mentioned that there are several major changes in the new version, such as TLS 1.4 plus a very different SSH implementation. Al indicated he wants to look at the final draft ND cPP v3.0 to see what is changed so he can see what might need to be included in the next version of the HCD cPP.
     As an aside, Al indicated that there will be incremental and major updated to the HCD CPP and

HCD SD, with the next version being an incremental update. The HCD iTC, however, hasn't worked out yet what the intervals will be between incremental and major versions.

- One last point – once the HCD cPP and HCD SD are published it will be interesting to see what Position Statements are submitted and what they say. Th HCD iTC expects positive Position Statements from NIAP and the Japanese and Korean schemes; what will be interesting to see is what other schemes, especially the European schemes, do.

4. As a follow-up the review of the Security Page on the PWG web site at http://www.pwg.org/security the past two IDS WG meetings, Al was asked by Smith Kennedy at the 10/6/22 meeting to compare the Basic Security Features list of security features on the Security page to the list of Security Objectives in HCD cPP v1.0. The table below provides Al's comparison:

HCD cPP Security Objectives	PWG Security Site Basic Security Features
User Authorization	*Addressed in IETF STD92*[1]
User Identification and Authentication	Identification, authentication, and authorization
Access Control	Not addressed
Administrator Roles	*Addressed in IETF STD92*
Firmware/Software Update Verification	Automatic firmware/software updates
Self-test	Not addressed
Communications Protection	Network isolation and trust Protection of data in transit
Auditing	Protected audit logging and accounting
Storage Encryption	Protection of data at rest
Protection of Key Material	Not addressed
PSTN Fax-Network Separation	Not addressed
Image Overwrite	*Indirectly addressed in IETF STD92*
Wipe Data	*Indirectly addressed in IETF STD92*
Authentication Failures	*Addressed in IETF STD92*
Firmware Integrity	Process isolation and trust
Strong Cryptography	Confidentiality and data integrity

Note: Items in Italics were added during the meeting

The left column is the Security Objectives from the HCD cPP; the right column is from the list of Basic Security Features shown on the PWG Security page. The goal here was to map the bullets on the Basic Security Features to one or more of the HCD cPP Security Objectives by looking at the text of the bullet and the documents referenced and determine which, if any, of the HCD cPP Security Objectives applied.

The overall impression was that Mike Sweet, who created the list, did a good job of mapping to the Security Objectives in the HCD cPP without knowing what they were. A few notes on the discussion:

- Access control was deliberately not covered in the IPP standards developed the PWG IPP WG.
- Regarding Protection of Key Material, the assumption regarding IPP is that any encryption key or key material associated with operation of IPP are protected, so it is not an area of concern.

[1] STD 92, RFC 8011 on Internet Printing Protocol/1.1: Model and Semantics

- STD 92 covers the areas of User Authorization, Administrator Roles, and Authentication Failure. As a result, these areas did not need to be addressed in any standards created by he PWG IPP WG.
- Ira indicated that STD 92 also indirectly covers Image Overwrite and Data Wiping.
- The remaining two areas - Self-test and PSTN Fax-Network Separation – are ones that are unique to devices like HCDs and would not be expected to be covered in an IPP standard.

5. Al then presented this week's special topic on the NIST Risk Management Framework (RMF). The slides Al used can be found at https://ftp.pwg.org/pub/pwg/ids/Presentation/NIST Risk Management Framework.pdf.

   The main items covered in the presentation were:

- Al started by saying that he found out about the NIST RMF from an article on Cybersecurity of the Digital Thread for Additive Manufacturing for 3D Printing he was using for his presentation at this years International Common Criteria Conference (ICCC), and decided to learn more about it.
- NIST RMF is documented in NIST SP 800-37 Rev 2 NIST Risk Management Framework for Information Systems and Organizations. It was published in December 2018. NIST RMF is closely associated with the NIST Cybersecurity Framework that was discussed at a prior IDS WG meeting; in fact, elements of the NIST Cybersecurity Framework are included in the NIST RMF as references to the various tasks.
- NIST RMF is mandatory for Federal information systems, but can be used by non-Federal entities like businesses, industry, and academia.
- The purpose of the NIST RMF is to provide guidelines for managing security and privacy risks and applying the Risk Management Framework (RMF) to (Federal) information systems and organizations. The slide set lists several reasons why these guidelines were developed.
- The slides provide several key definitions that are important to understanding the elements of the NIST RMF. A couple of the key ones are:
  - **Authorization Package**: The essential information that an authorizing official uses to determine whether to authorize the operation of an information system or the provision of a designated set of common controls. At a minimum, the authorization package includes an executive summary, system security plan, privacy plan, security control assessment, privacy control assessment, and any relevant plans of action and milestones.

    Note that **Authorization** in this context deals with a senior manager authorizing some type of task in the NIST RMF to be performed.
  - **Control Assessment**: The testing or evaluation of the controls in an information system or an organization to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security or privacy requirements for the system or the organization. "Control" in this context is one of the security and privacy controls from NIST SP 800-53 Rev 5, Security and Privacy Controls for Information Systems and Organizations.
  - **Privacy Control**: The administrative, technical, and physical safeguards employed within an agency to ensure compliance with applicable privacy requirements and manage privacy risks. It is interesting that no definition of the term "Privacy" itself was provided; the NIST Definition of Privacy in SP800-130: Assurance that the confidentiality of, and access to, certain information about an entity is protected.
  - **Risk**: A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

  - **Risk Assessment**: The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of a system.
  - **Security**: A condition that results from the establishment and maintenance of protective measures that enable an organization to perform its mission or critical functions despite risks posed by threats to its use of systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the organization's risk management approach. As a group, we found this definition of 'Security' to be awkward as best. A better definition of 'Security' from NIST SP 800-160v2r1 (as taken from ISO/IEEE 15288:2015) is "Protection against intentional subversion or forced failure. A composite of four attributes – confidentiality, integrity, availability, and accountability – plus aspects of a fifth, usability, all of which have the related issue of their assurance".

- The NIST RMF consists of the following 7 steps:
  - **Prepare** to execute the RMF from an organization- and a system-level perspective by establishing a context and priorities for managing security and privacy risk
  - **Categorize** the system and the information processed, stored, and transmitted by the system based on an analysis of the impact of loss
  - **Select** an initial set of controls for the system and tailor the controls as needed to reduce risk to an acceptable level based on an assessment of risk
  - **Implement** the controls and describe how the controls are employed within the system and its environment of operation
  - **Assess** the controls to determine if the controls are implemented correctly, operating as intended, and producing the desired outcomes with respect to satisfying the security and privacy requirements
  - **Authorize** the system or common controls based on a determination that the risk to organizational operations and assets, individuals, other organizations, and the Nation is acceptable
  - **Monitor** the system and the associated controls on an ongoing basis to include assessing control effectiveness, documenting changes to the system and environment of operation, conducting risk assessments and impact analyses, and reporting the security and privacy posture of the system

Each step has one or more Tasks associated with it. Al ran briefly through the Tasks for each step. Some highlights of the Tasks are:

- For the **Prepare** step, the tasks revolve around planning for the risk management process. That includes tasks such as (1) assigning Project Management Roles, (2) establishing, documenting, and publishing organizationally-tailored control baselines and/or Cybersecurity Framework Profiles and (3) developing and implementing risk management and continuous monitoring strategies.

  There are also "system-level" tasks for the **Prepare**" step such as (1) identifying the proper stakeholders, (2) identifying the assets that need protection, (3) conducting a system-level risk assessment and update the risk assessment results on an ongoing basis, (4) defining the security and privacy requirements for the system and the environment of operation and (5) allocating security and privacy requirements to the system and to the environment of operation. Al noted that this last task is very similar to what is done in a CC certification, where security objectives are allocated between the TOE and the operational environment the TOE will be operating in.

- For the **Categorize**" step, which Al indicated is a somewhat unusual one, the three tasks are (1) document the characteristics of the system, (2) categorize the system and document the security categorization results and (3) review and approve the security categorization results and decision. Al noted the NIST SP doesn't get into much detail as to what categorization scheme is to be used here.
- For the **Select** step, tasks include items such as (1) selecting the controls (from NIST SP 800-53) for the system and the environment of operation, (2) tailoring, allocating and documenting the security and privacy controls to the system and to the environment of operation, (3) developing and implementing a system-level continuous monitoring strategy, and (4) reviewing and approving the security and privacy plans for the system and the environment of operation.
- For the **Implement** step, the two tasks are (1) implement the controls in the security and privacy plans and (2) document changes to planned control implementations based on the "as-implemented" state of controls.
- For the **Assess** step, the tasks revolve around assessment of the security and privacy controls. The tasks include (1) selecting the appropriate assessor or assessment team for the type of control assessment to be conducted (Al noted that in a "prior life" he was an assessor for the SEI Capability Maturity Model), (2) developing, reviewing, and approving plans to assess implemented controls, (3) doing the assessment of the controls per the plan, (4) documenting the assessment results and (5) conduct initial remedial actions to the findings of the assessment. These are standard tasks associated with any type of assessment.
- For the **Authorize** step, keep in mind the discussion of what 'Authorize' means in the context of the NIST RMF. So, the tasks for this step involve (1) assembling the Authorization Package defined above, (2) identifying the risks, (3), developing the response to each identified risk and (4) determining and authorizing which risks are deemed to be acceptable risks. This is the true 'Risk Management' step in the NIST RMF.
- Finally, the **Monitor** step involves the "closed loop" aspect of the process of continuous monitoring of the controls defined earlier and the management of the risks defined in the **Authorize** step. The tasks for this step include (1) monitoring the information system and its environment of operation for changes that impact the security and privacy posture of the system, (2) assessing the controls implemented within and inherited by the system in accordance with the continuous monitoring strategy, (3) responding to risk based on the results of ongoing monitoring activities, risk assessments, and outstanding items in plans of action and milestones, (4) reviewing the security and privacy posture of the system on an ongoing basis to determine whether the risk remains acceptable and (5) implementing a system disposal strategy and execute required actions when a system is removed from operation. Al noted that this last task is the same as the "decommissioning" of HCDs for which developing the requirements took several weeks to iron out by the HCD iTC.

Al's general impression of the NIST RMF is that it is much more bureaucratic and much more management-oriented than the Cybersecurity Framework is. But that is understandable, since risk management is, by definition, a management-oriented activity.

The NIST list of publications related to the NIST RMF: https://csrc.nist.gov/Projects/risk-management/publications

6. Round Table:

Ira mentioned a couple of upcoming events:

- Post Quantum Cryptography Workshops in November 2022
  - PQNet Conference (Academia, Industry, Standards) at 9am-TBD US EST on 27-28 November 2022 (using Zoom and Slack). For registration, please use the google form of this website: https://pqnet.org/

  - US NIST 4th PQC Standardization Conference (Academia, Industry, Government, Standards, other) at 10am-3pm US EST on 29 November 2022 to 1 December 2022.For registration, please visit this website ($35 registration fee): https://csrc.nist.gov/Events/2022/fourth-pqc-standardization-conference

- ASTM International Conference on Additive Manufacturing, October 31 – November 4, 2022, Orlando FL
- CCUF Fall 2022 Workshop, November 10, 11 & 14, 2022, Toledo Spain
- International Common Criteria Conference, November 15-17, Toledo Spain

7. **Actions:** None

Next Steps

- Since Al will be in Orlando FL in two weeks (November 3rd) giving a paper with Paul Tykodi at the ASTM ICAM 2022 Conference, there will be no IDS WG Meeting that week.
- The next PWG Face to Face Meetings will be November 15-17, 2022. The IDS Session will likely be on November 17th from 10A – 12N ET.
- The next IDS WG Meeting will be December 1, 2022 at 3:00P ET / 12:00N PT. Main topics will be (1) the latest status on the HCD iTC, (2) a post-mortem on the IDS Face to Face Meeting and (3) Al will briefly go through his ASTM ICAM 2022 and ICCC presentations and share important topics that came out of the Fall 2022 Common Criteria User's Forum (CCUF) Workshop and ICCC 2022.