# IDS Working Group

2010-12-09 Face to Face Meeting Minutes

## 1. Attendees

| | |
|---|---|
| Carmen Aubry * | Océ |
| Howard Cohen ** | NIAP |
| Peter Cybuck | Kyocera |
| Jim Donndelinger ** | Aerospace Corp. |
| Ken Elliott ** | Aerospace Corp. |
| Lee Farrell | independent |
| Shaun Gilmore ** | NIAP |
| Carol Houck ** | NIAP |
| Ira McDonald | High North / Samsung |
| Joe Murdock | Sharp |
| Fumio Nagasaka | Epson |
| Ron Nevo * | Samsung |
| Glen Petrie * | Epson |
| Brian Smithson * | Ricoh |
| Mike Sweet | Apple |
| Jerry Thrasher | Lexmark |
| Bill Wagner | TIC |
| Rick Yardumian | Canon |

* by telephone/LiveMeeting
** by telephone/LiveMeeting, until 12:00

## 2. Agenda

Joe Murdock opened the IDS meeting and provided the planned agenda topics:

11:00 – 11:05 Administrative Tasks
11:15 – 12:00 Supporting Documents for Common Criteria Evaluation (NIAP conference call)
12:00 – 13:00 Lunch
13:00 – 13:30 Supporting Documents for Common Criteria Evaluation
13:30 – 13:45 Review action items
13:45 – 14:00 Document status and Review
14:00 – 14:15 MPSA Survey results
14:15 – 15:00 Identification, Authentication and Authorization
15:00 – 15:15 Break
15:15 – 16:14 IDS Security Ticket
16:15 – 16:30 Wrap up and adjournment

## 3. Minutes Taker

Brian Smithson

## 4. PWG Operational Policy

It was noted that all attendees should be aware that the meeting is conducted under the PWG Membership and Intellectual Property rules. There were no objections.

## 5. Approve Minutes from previous meeting

No minutes were produced from previous meeting.

There were no objections.

## 6. Supporting Documents for Common Criteria Evaluation (NIAP conference call)

[Brian] Some members of the IEEE P2600 working group had been in contact with NIAP seeking their guidance on what to put in a Supporting Document (SD) specifically to support the evaluation of MFPs conforming to IEEE 2600.1 and/or 2600.2. They had been looking at some of the other development activities such as the OS PP and the Network Appliance PP, which has given them some indication of NIAP's direction. They are looking for more specifics on what to do for the HCD PP that would give NIAP the assurance that evaluations are consistent and reliable across multiple labs and CC schemes.

[Shaun] On this call, NIAP can speak at a high level about the end goal of the program and the PPs. More detailed technical discussions would be needed later in a series of calls to talk about specific requirements in the MFP PP and specific assurance activities.

The NAPP and USB PP have some additional assurance requirements associated with SFRs and more specificity in the SFRs themselves. NIAP wants very objective and repeatable assurance activities. Having high-level, open-ended requirements as we've seen in the past is not the direction we're going. More specific requirements are needed where that makes sense.

NIAP understands that with a large number of vendors and products, some flexibility is needed. To accommodate that, an "Appendix C" is used to specify appropriate optional requirements or refinements to requirements, but they are still very specific.

For example, instead of just saying that you do secure tunneling, the document will say how secure tunneling should be done. In general, the direction is to be more granular in requirements and more specific in assurance activities.

NIAP is willing to supply someone to work with the PWG-IDS to participate in a series of workshops toward that end for HCDs.

[Brian] In the NAPP, there are quite a few extensions to SFRs that are different from standard CC, and asked if that is the direction they are taking or if it is something to be avoided.

[Shaun] NIAP is not being strict with EALs or CC dependencies/selections/refinements. It is better to articulate the requirements in some pseudo English / CC language and then let NIAP determine how to express that in a way that is acceptable to the international community.

In the NAPP, there is a whole front matter section that describes threat environment in prose, for which NIAP thinks it can get international acceptance. The idea is to start there and not immediately try to fit into standard CC, and then adjust it toward standard CC if needed to achieve that acceptance.

NIAP is trying to drive change into the CC by practical example, and in some cases that will break the CC in order to drive that change.

[Brian] The threat environment and prescriptive security functional requirements could be rather dynamic, such as if new attacks are developed or specific techniques like a hashing algorithm become broken, and asked if that sort of thing should be in an SD which made the PP more specific while not requiring the PP to be updated. The SD could change more frequently. His concern was that if such things were in the PP, the PP may need to change every year.

[Shaun] Yearly updates wouldn't be a bad idea, and that it didn't matter if it was in a PP or an SD, because you need that information. They both go through the same process to be recognized. We can debate which one is easier for the user, but you'll need both of them.

[Ira] The HCD PP was an IEEE standard and it is not possible to update it on a yearly cycle, and the SD would be an open standard from the PWG with a much lighter process that makes it possible to make an update in as little as four months.

[Shaun] The IEEE model isn't going to work, and the IEEE PP will be sunsetted at some point. If it can't be updated in two years, then it's not a useful framework to work from. We don't want to retrofit or interpret things in an SD simply because the IEEE PP doesn't allow changes. The HCD vendor community will need to change from the IEEE model to a more responsive development framework, whatever that may be. There may be an interim period where we do need to do something with the IEEE PP, but not for the long term.

[Brian] The vendor community had discovered the difficulty of having a long approval process and expensive copyright situation, and agrees that we need to do something differently in the future. However, the durable part of the current PPs could be the base principles of what security areas need to be covered in HCDs, and the specificity and dynamism could be provided by the SDs. That could give the current PPs a longer lifetime. IEEE standards need to be revised or reaffirmed every five years anyway, so that could be when the PPs are rewritten. At that point, we would have a great deal of practical experience actually evaluating products and seeing if they really worked out. Right now, NIAP is speculating that HCD evaluations against the IEEE PPs are not consistent or reliable across multiple labs and schemes even though only one HCD has completed such an evaluation at this time. We shouldn't try to rush to make changes before we have some actual experience with evaluation.

[Shaun] NIAP understands that, and they aren't really focused on any problems with MFPs but instead are dealing with the larger issues of CC evaluations. MFPs evaluations may or may not work with the EAL model, but that's not the point. They need to fit in the overall landscape of where we're going. We're not certain if working from the current HCD PPs will work as a framework for creating more specificity in SDs.

[Brian] If the PP doesn't contain nearly enough detail, then all of the meat would be in the SDs and that could prove cumbersome for vendors and confusing for customers. It is also possible that the PP might not cover something in the PP that is really needed, in which case we would have a greater need for a new PP.

[Carmen] Most HCD evaluations are done outside of the US scheme, and asked if NIAP would mind if other schemes participated in this development such as European schemes or the Japanese scheme.

[Shaun] NIAP wants to be open to international participation, although they are reluctant to open it too broadly at first until they have a strawman in place. If mutual recognition is important, which it certainly is for this technology, then it makes sense to open up to other schemes for commenting and development.

[Carmen] In the NAPP, there is a requirement for software updates, which is not a problem for HCDs, but asked how that can be reconciled with the CC's notion that a software update breaks the CC certification of a product. At the last ICCC, there was talk about predictive assurance. Are the two related?

[Shaun] We're hoping that in the next generation of the CC, there will be a way for vendors to update their products. Products have that capability and do get updated, so ignoring it in the CC doesn't make sense. The technical aspects of how to do a secure update are good to have in a PP, but it is true that there is a conflict between updates and the current CC.

[Ron] What is the timeframe for developing SDs, for replacing the PP, for everything?

[Shaun] We have some PPs at EAL2 out there now. There will be some date on which we don't want to have any PPs associated strictly with an EAL, but we haven't set a date for that. It depends on how quickly we can develop standardized PPs. It is taking some time to do that, so it is certainly not in the next year. It may be two or more years out.

[Ron] We have products in evaluation, and it can take a long time to complete them. We want to make sure that our investment is preserved.

[Shaun] Even after we make a change in policy, we allow evaluations that are underway or about to start, and after that we allow maintenance for a couple of years. Policies aren't retroactive.

[Ron] How will NIAP convince DoD agencies to not ask for more that EAL2?

[Carol] We're working with the DoD agencies, and when we find out from a lab or vendor that some agency is asking for a higher EAL, we will go there and find out why and get them to lower or change their policy. It is like the IEEE work, it takes a long time. We are working on it on a case-by-case basis. We're making slow progress, with Army, Navy, Air Force, not yet the Marines, in the past three or four months. We have most of the CIO-level people engaged and perhaps agreed, but it takes a while for that to filter down.

[Brian] Other countries and commercial enterprises misunderstand EAL to be a measure of security, and not of assurance. For example, I was in Canada and they often refer to CC as "EAL certification". Can

NIAP have any impact outside of the US DoD agencies? I am concerned that if we change everything to EAL2, some will ask us “why did you lower the security on your products?”.

[Shaun] That’s an example of why EAL2 isn’t a good solution. We’re using it in the interim, but ultimately we to break the tie between acquisition decisions and straight EAL. It will be a long process to disassociate those things because it has been that way for so long. EAL2 is an interim stop until we get to the point of having supporting documents and mutually recognized PPs that may have a combination of EALs and may have requirements that aren’t even captured by the CC. We want a PP per technology, not a technology having PPs at different EALs.

[Ira] Is it true that the NAPP does not apply to MFPs?

[Shaun] Yes, but they may share some requirements. The NAPP could apply to many technologies so we wanted to scope it down. But where a product uses remote login or IPsec tunneling or something like that, they may have identical or very similar requirements to the NAPP.

[Brian] I sat in on the NAPP deployment/configuration subgroup, and they talked about deriving some requirements from the Consensus Audit Guidelines, otherwise known as the SANS Top 20 Network Controls. Is that something that came from NIAP?

[Shaun] It is certainly something that they should take into consideration. They should look into the 800-53 controls, 1253 controls, SANS controls, DISA STIGs, other schemes PPs that have been developed for network devices.

[Pete] We discussed in a previous conference call a couple of policies that might address data at rest or some other issues. Is that still under consideration?

[Shaun] It’s still under consideration. We don’t have a very good policy for data at rest or data overwrite. We have a disk encryption PP, a USB PP, and an initiative for file encryption. From that we should be able to make a general policy about data at rest, but we don’t have one yet.

[Brian] How soon can we start having the technical sessions so we can get started?

[Carol] We need to identify who to assign. We have many requirements and few people.

[Shaun] Probably mid to late January before we can assign a person.

[Brian] Would it be useful to have a face-to-face during RSA week in mid February?

[Shaun] Yes, there will be many of us out there.

[Carol] Some of the other schemes will be there too. Would you make the arrangements?

[Brian] We can probably use the Ricoh Tech Portal in San Francisco that we used for the CCVF meeting last year. It was too small for that meeting, but would be fine for this one.

[New action item]

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 70 | 12/9/2010 | 1/14/2011 | | | Brian Smithson | admin | | Make arrangements for F2F meeting with NIAP/other schemes at Ricoh SF during RSA week | | |

[Ron] We also have a PWG F2F meeting in the first week of February, so we could prepare.

[Brian] It would be good to have a few teleconferences before our F2F so we can hit the ground running and be productive.

[Ira] We could have a teleconference with NIAP in late January and again during the PWG F2F in early February.

## 7. Review Action Items

NOTE: The most recent Action Item spreadsheet is available at: ftp://ftp.pwg.org/pub/pwg/ids/ActionItems/ . Changes made during this meeting are indicated by red text.

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 33 | 12/10/2009 | | | | Randy Turner | SHV | | Randy Turner will contact Symantec (when appropriate) to encourage discussion with the PWG about a SHV. | H | No longer blocked waiting for AI #32 so we can send market rationale to Symantec. Need a volunteer to take over on this task. |
| 34 | 12/10/2009 | | | | Randy Turner | Remediation | | Randy Turner will investigate Symantec's products and their method(s) to "remediate noncompliant endpoints." | H | Symantec wants an NDA, but PWG cannot do an NDA; will do a generic version; should we invite Symantec to a PWG IDS teleconference? Need a volunteer to take over on this task. |
| 44 | 3/11/2010 | | | | Jerry Thrasher Ira McDonald Brian Smithson | NEA Binding | | Recast the NEA Binding document as a TCG TNC Binding document | | Make it a TCG document, not an IETF NEA document |
| 58 | 6/11/2010 | 8/3/2010 | | | Joe Murdock and Ira McDonald | SCCM | | Create a first draft SCCM binding spec based on the NAP binding spec | H | MS is releasing R3 of SCCM and also a beta of "R-next", while at the same time adding power management; WIMS group may also be interested. On hold due to priorities. |
| 66 | 10/20/2010 | | | | Brian Smithson Joe Murdock Ira McDonald | admin | | Create a project charter for creating IEEE 2600.1 Supporting Documents | H | With no requirements specification. Wait for NIAP guidance in mid to late January. |
| 67 | 10/28/2010 | | | | Joe Murdock Ira McDonald | auth | | Write IDS-Identification-Authentication-and-Authorization-Framework specification | P | |
| 68 | 12/2/2010 | | | | Joe Murdock | auth | | Define IAA Security Ticket (per October 2010 F2F) | P | |
| 69 | 12/2/2010 | | | | Michael Sweet | log format | | Write HCD Logging specification | P | |

[Ira] Regarding the Support Documents project charter, we should expect guidance from NIAP in mid to late January before writing the charter so that we don't get the SC to approve something and then find we need to turn around and change it.

## 8. Document Status

HCD-Assessment-Attributes

- ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-idsattributes10-20100930.pdf
- Stable (needs a binding prototype)

HCD-NAP Binding

- ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-napsoh10-20100930.pdf
- Stable

HCD-TNC Binding

- Initial Draft still under development

HCD-NAC Business Case White Paper

- ftp://ftp.pwg.org/pub/pwg/ids/white/tb-ids-hcd-nac-business-case-20100422.pdf
- Final

HCD-Remediation

- ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-remediation10-20100930.pdf
- Initial Draft

HCD-NAP-SCCM Binding

- Mapping Spreadsheet:
  - ftp://ftp.pwg.org/pub/pwg/ids/white/IDS-NAP-SCCM-Mapping_20090917.xls
- Specification on hold

HCD-Log

- White Papers:
  - ftp://ftp.pwg.org/pub/pwg/ids/white/ids-logging-20100608.pdf
  - ftp://ftp.pwg.org/pub/pwg/ids/white/IEEE2600.1_audit_events.pdf
- Specification:
- ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-log10-20101018-rev.pdf
- Initial Draft

IDS-Identification-Authentication-Authorization

- White Papers:
  - ftp://ftp.pwg.org/pub/pwg/ids/white/ids-authorize-20100608.pdf
- Mind Map:

  - ftp://ftp.pwg.org/pub/pwg/ids/white/ids-iaa-framework-2010-12-03.xmind
- Specification (outline only):
  - ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-iaa10-20101202.pdf
  - ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-iaa10-20101202.docx

## 9. New HCD-ATR attribute

[Joe] Should we add a security log destination attribute to ensure that there is a location to archive logs?

[Ira] Yes, to ensure that there is a central location.

[Brian] How are you going to do a health validation on something that is outside of the HCD?

[Ira] You could validate that it is a correct URI scheme and that it is DNS-resolvable.

[Joe] Site policy could control what are acceptable values.

[Ira] As is done with IPP, we could make some policy like it can be https or sftp and not sent in the clear.

[Mike] There is no URI scheme for syslog. One was started three years ago but didn't get finished.

[Brian] IEEE 2600.1 doesn't require an external log. It requires a log, which can be internal, external, or both. I think this is the first instance in which one of these attributes makes a functional requirement that 2600.1 doesn't also require.

[Joe] Well, we require syslog.

[Mike] It could be internal or external, and site policy could refine it further. The URI could point to something local.

[Brian] Should it be multivalued?

[Ira] Yes. And the first one would be primary and the only one that is required to be non-empty.

[Brian] Would a flag be sufficient? One that says "audit is enabled"? We do something like that for admin passwords – just a flag that says you've changed it to something other than default, but there is no assessment of strength of function.

[New action item]

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 71 | 12/9/2010 | | | | Joe Murdock | ATR | | propose by email a multivalued attribute for log location (a URI) to be added to HCD-ATR | | |

## 10. MPSA Survey Results

Refer to the presentation slides ftp://ftp.pwg.org/pub/pwg/ids/Presentation/2010-12-09_IDS_F2Fv3.pdf

## 11. IA&A and IDS Security Ticket

Refer to ftp://ftp.pwg.org/pub/pwg/ids/white/Cloud-and-Mobile-Authentication-2010-10-20.xmind

[Joe] There has been no change in the mindmap since the last face-to-face.

Refer to ftp://ftp.pwg.org/pub/pwg/ids/white/ids-iaa-framework-2010-12-03.xmind

[Joe] Two mindmaps have been combined into one. The only other change is that a SAML block has been added.
Document security is an issue that keeps coming up. It is for access control, not rights management.
What we're working on now is the MFP security ticket for IPP Everywhere and the cloud.
These are only recommendations, no new protocols; the only new thing is the security ticket.
The security ticket would be SAML or WS-Federation or policy request.

[Ira] If we have a conformance section, which we will, then we will have requirements and not just recommendations.

[New action item]

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 72 | 12/9/2010 | | | | Joe Murdock | IA&A | | direction is not "recommendations only", it is "requirements and recommendations" (pointing to existing standards) because there will be a conformance section | | |

[Joe] An outline has been posted for IA&A. There is no content. We are looking for authors of sections.

[Ira] We need a common requirements document to avoid making requirements in separate documents, over and over, which will ultimately drift from one another. It makes more sense to have one overarching requirements document for IDS security.
We can't go into Last Call unless we have an approved external requirements document, or by SC caveat, an embedded section that has rationale, use cases, and derived design requirements. We'd need one of those for every spec.

[Bill] It would be challenging to have one requirements document for all topics.

[Ira] The idea is that we'll have one common requirements document that covers most requirements, and then individual specs can point to that document and add a few unique requirements.

[New action item]

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 73 | 12/9/2010 | | | | Joe Murdock Ira McDonald Ron Nevo | reqts spec | | start an IDS common requirements spec to include out-of-scope and terminology sections | | |

Refer to ftp://ftp.pwg.org/pub/pwg/ids/white/ids-security-2010-12-08.xsd

[Joe] The MFP security ticket is a transportable container of security configuration for user, device, and service.

[Jerry] How do you protect the integrity of the ticket?

[Ira] IPP requires secure connection.

[Jerry] What about protecting it at rest?

[Ira] Grab the security ticket, and sign it. That protects it at rest.

[New action item]

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 74 | 12/9/2010 | | | | Joe Murdock | security tkt | | add a digital signature to the security ticket | | |

## 12. Summary of New Action Items and Open Issues

### 12.1 New action items

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 70 | 12/9/2010 | 1/14/2011 | | | Brian Smithson | admin | | Make arrangements for F2F meeting with NIAP/other schemes at Ricoh SF during RSA week | | |
| 71 | 12/9/2010 | | | | Joe Murdock | ATR | | propose by email a multivalued attribute for log location (a URI) to be added to HCD-ATR | | |
| 72 | 12/9/2010 | | | | Joe Murdock | IA&A | | direction is not "recommendations only", it is "requirements and recommendations" (pointing to existing standards) because there will be a conformance section | | |
| 73 | 12/9/2010 | | | | Joe Murdock Ira McDonald Ron Nevo | reqts spec | | start an IDS common requirements spec to include out-of-scope and terminology sections | | |
| 74 | 12/9/2010 | | | | Joe Murdock | security tkt | | add a digital signature to the security ticket | | |

### 12.2 New issues

No new issues.

### 12.3 Old issues

1. How are administrators notified of remediation issues? Does the HCD ever initiate a notification, or is it always the remediation server that initiates notification? Does this same issue apply to policy servers?
2. What is a “fatal” error? Under what circumstances (if any) do we require the HCD to be shut down?

## 13. Wrap up and adjournment

The next IDS conference call is on Thursday, January 13, 2011, starting at 1PM EDT.

IDS meeting adjourned.