

**IEEE P2600 Meeting #24
December 11-12, 2006
Peerless Systems, El Segundo CA**

Attendees

Chair: Don Wright, Lexmark
Vice Chair: Lee Farrell, Canon
Secretary/ Lead Editor (PPs): Brian Smithson, Ricoh
Lead Editor (Clauses): Jerry Thrasher, Lexmark

Hiromasa Akamatsu, Kyocera-Mita
Carmen Aubry, Océ
Nancy Chen, Okidata
Nick Del Re, Canon
Hiroshi Hosaka, Ricoh
Hiroki Kobayashi, Ricoh
Takanori Masui, Fuji-Xerox
Takeshi Nakamura, Kyocera-Mita
Ron Nevo, Sharp
Ken Ota, Konica Minolta
Glen Petrie, Epson
Alan Sukert, Xerox
Jay Treptow, Peerless
Randy Turner, Peerless
Hiroki Uchiyama, Ricoh
Shigeru Ueda, Canon
Brian Volkoff, HP
Jan Walter, Peerless
Lida Wang, Kyocera-Mita
Sameer Yami, Toshiba

In the following sections, names of speakers are indicated by [brackets].
The primary speaker for a session is noted at the beginning of the session
as a default; others are noted in place. Some editorial comments may
appear in these minutes, indicated by {braces}, inserted by the Secretary
for clarity.

Attendees.....	1
Administrivia [Wright]	2
Agenda review.....	2
Minutes and Agenda approvals	2
IEEE patent policy	2
Inappropriate topics review	3
Officers and Editors.....	3

Meeting schedule updates	3
TCG update [Volkoff]	4
INCITS CS1 update [Thrasher]	4
CCVF update [Sukert]	4
Action items from previous meeting [Wright]	5
Email issues [Wright]	5
Support of NIAP CIM requirements [Smithson]	5
Denial of Service threats [Smithson]	7
T.DOS.FAX threats in PP-C [Chen]	9
Unrolling PP threats [Smithson]	10
Unrolling Objectives [Smithson]	10
Functional differences in STs [Chen]	10
Sharp/IPA comments [Nevo]	14
SFR worksheet revision B [Smithson]	15
SFR Audit and Management requirements [Smithson]	17
Threat analysis recommendations [Aubry]	17
Compliance clause [Nevo]	18
Family of PPs proposal [Smithson]	18
Main document structure [Wright]	19
Main clauses 24a review [Thrasher]	19
Main clauses 24b review [Thrasher]	20
Comments database [Wright]	20
Next meeting [Wright]	21
Closing [Wright]	21

*** Commenced at 9:10 AM 12/11/2006 ***

Administrivia [Wright]

The following administrative items were reviewed:

Agenda review

Refer to meeting slides for detail

<http://grouper.ieee.org/groups/2600/presentations/P2600-Dec2006.ppt>

Minutes and Agenda approvals

The October 2006 minutes were approved without additional changes.

The December 2006 agenda was approved with no changes.

IEEE patent policy

Patent policy was reviewed. There were no patent disclosures made by attendees.

Note: A new patent policy will be instituted in April 2007.

Inappropriate topics review

Inappropriate topics criteria were reviewed. No issues were identified.

Refer to meeting slides for detail:

<http://grouper.ieee.org/groups/2600/presentations/P2600-Dec2006.ppt>

Officers and Editors

Officer elections took place at this meeting. The only nominations that had been received by the current Chair were for the current officers to continue their duties into the next working group year. No additional nominations were made at this meeting.

The current officers were elected by acclamation:

Chair: Don Wright, Lexmark.

Vice Chair: Lee Farrell, Canon.

Secretary: Brian Smithson, Ricoh.

Lead editors are unchanged:

Editor (clauses): Jerry Thrahser, Lexmark.

Editor (PPs): Brian Smithson, Ricoh.

Meeting schedule updates

Feb 22-23, 2007 (Thursday/Friday) with PWG and TCG, Wailea Beach Marriott Resort and Spa, Wailea (Maui), HI. Details are here:

<http://grouper.ieee.org/groups/2600/meetings.html>

- PWG meets on Mon-Tue Feb 19-20.
- For TCG members, there will be TCG HCWG meeting, on Wed. Feb. 21.

Apr 24-25, with PWG, IEEE Headquarters, Piscataway NJ

May 30-31, location open

- Handle comments from 1st re-circulation

Jul 11-12, location open, possibly HP in Roseville CA (nearest major airport is SMF Sacramento)

- Handle comments from 2nd re-circulation, if needed
- Cut-off for draft to RevCom is August 17th

Note: We may need to add some meeting dates and/or conference calls.

No schedule conflicts or issues were identified during this meeting. The most current P2600 meeting information is always available at <http://grouper.ieee.org/groups/2600/meetings.html>

TCG update [Volkoff]

(TCG web site: <http://www.trustedcomputinggroup.org/>)

- meeting in El Segundo on Wednesday (at HP)
- we have been discussing how to package the standard
 - to allow for robust capabilities
 - to give mfrs flexibility for various levels of implementation
- Sharp has joined
- next TCG member meeting is in Atlanta, end of January
 - HCWG considering meeting for multiple days

INCITS CS1 update [Thrasher]

(INCITS CS1 web site: <http://cs1.incits.org/>)

- No meeting since last update
- Next CS1 meeting is in January (in San Jose CA)
- CCV3.1 update for ISO 15408 is a new ballot proposal (not fast-tracking)

CCVF update [Sukert]

(No CCVF web site – yet :-)

- NIAP sent a survey to vendors
 - CCVF considering collecting a response from CCVF members, but has not yet decided
- survey was sent to vendors that had certs in the US [Cybuck]
 - NIAP no longer such a partnership
 - now just NSA (not NIST)
 - resources have been very limited
 - focus has been on government products not commercial
 - focus on medium+ (EAL4-5)
 - planning to charge for evaluations, is included in federal budget
 - should be published in the federal register
 - evaluation of PPs more difficult than STs
 - requires more senior people
 - recent e-mail about "low priority" on CIMs did not mean that they are not unimportant
 - DHS is working on a COTS strategy
 - working groups are not open to vendors
 - draft CIMs are "just about" final

- NIAP (and DAPS) are interested in US Govt profiles for MFPs, at least PP-A

Action items from previous meeting [Wright]

Main action items were updated on presentation slides:

<http://grouper.ieee.org/groups/2600/presentations/P2600-Dec2006.ppt>

Action item spreadsheet was reviewed and updated:

- Pre-meeting:
<http://grouper.ieee.org/groups/2600/actionitems/P2600-action-items-20061208.xls>
- During meeting:
<http://grouper.ieee.org/groups/2600/actionitems/P2600-action-items-20061211.xls>
- Post-meeting:
<http://grouper.ieee.org/groups/2600/actionitems/P2600-action-items-20061221.xls>

Email issues [Wright]

Support of NIAP CIM requirements [Smithson]

Refer to <http://grouper.ieee.org/groups/2600/email/msg00658.html>.

- new draft CIM is no more international friendly than old one
- are there parts of the CIM that are a problem? [Wright]
 - FIPS 140 [Chen]
 - some NIAP-specific SFRs [Smithson]
- P2600 should be international standard [Ueda]
- NIAP has extensions to SFRs that are not internationally acceptable [Aubry]
- whatever is inside CCv3.1 can be in P2600 [Wright]
 - outside of CCv3.1, NIAP reqts could be added to ST
- could we have an informative annex for NIAP requirements? [Wright]
 - then it would need to be evaluated by NIAP [Aubry]
 - the base certification could be done elsewhere, but then the additional requirements could be evaluated by NIAP [Thrasher]
 - this was discussed at ICCCC, do CCRA ST and then "top off" with US reqts in US [Thrasher]
 - such an appendix would need at least review by NIAP [Smithson]
 - yes, especially because NIAP CIM is not final and we would be evaluating before it is final [Cybuck]
 - there is already a process for delta evaluations in US [Cybuck]

- all of the US labs will re-evaluate a non-US evaluated ST
- how would the annex be validated? [Aubry]
 - I think it would be an informative annex, not part of the evaluation [Smithson]
- {there was quite a bit of discussion about this}
- In a “delta evaluation” would NIAP accept those CIM requirements which are standard CCv3.1 if were evaluated elsewhere? [Thrasher]
 - Not sure but they should, need to ask them [Cybuck]
- It is more than just SFRs, there is an issue with the concept of “robustness” [Aubry]
 - It has been the intention of NIAP to get other schemes to accept some of their requirements [Cybuck]
 - Do you mean the “special” requirements that are outside of CCv3.1? [Wright]
 - There are some semi-special requirements in the CIM which are CCv3.1 compliant but which are more restrictive than CC requires and perhaps more restrictive than we desire. [Smithson]
 - Some of those requirements are necessary to make those SFRs meaningful [Cybuck]
 - The other thing to look at is Medium Robustness, which now is modeled after EAL4+. In the old CIM, it was EAL3+. I don't think we want to require EAL4+, even those parts that are standard CCv3.1.
- So the decision is to have an informative annex which lists CIM requirements that we do not think should be in the normative part of the PP? [Thrasher]
 - I think the annex might be so large that it is almost a replication of the CIM itself. It may be better to include whatever of the CIM we think should be in the normative part so that it is easier to comply with the CIM if desired, but not go so far as to try to speak for NIAP by listing their requirements in our PP. [Smithson]
- What happens with other countries' requirements? Do we have an informative annex for Germany, one for Japan, etc.? [Petrie]
 - We're trying to go for the “common” part of Common Criteria [Smithson]
 - In three years, no other government has come forward with additional requirements [Wright]
 - That is because the P2600 is not known anywhere except the US [Aubry]
 - Other countries do not have anything like the CIM documents [Thrasher]

- Even within the US government, not everyone requires the CIM. They may have other requirements. They all superset the common criteria [Walter]
 - We have a representative from DAPS who says that he wants CIM compliance [Wright]
 - That's just one voice [Walter]
- There is a counter argument that the CIM isn't final and we'd be putting obsolete requirements in our PP annex [Thrasher]
 - Peter Cybuck said that the CIM drafts are very close to final [Wright]
- We are also assuming that CCv3.1 goes through the ISO process unchanged, maybe it will become CCv3.2 in order to become an ISO standard
- Are there any issues to discuss in the draft CIMs? [Wright]
 - They do not specify the dot-level SFRs in their appendix [Aubry]
- Decision [Wright]
 - We should not use non-CCv3.1 CIM requirements
 - Put them in an informative annex to make it easier for ST authors to use them if they would like to get NIAP to evaluate CIM compliance
 - We need to look at instruction-by-instruction [Smithson]

Denial of Service threats [Smithson]

Refer to <http://grouper.ieee.org/groups/2600/email/msg00666.html>.

- Problems with DoS threats
 - Difficult to distinguish from non-malicious activities
 - Difficult to mitigate
 - Difficult to test without a concise test case
 - Especially at EAL2-3 where testing is more black-box than architecture/code inspection
- Further evidence: we haven't really come up with any SFRs that fit our threat descriptions
- Looking at existing PPs, there are only two types of DoS that PPs currently address:
 - Resources (like memory) being used up by one process, mitigated by a resource management objective and SFR
 - Specific network resources, like connections, being used up, also mitigated by resource management
- So can't we make them more specific, like resource mgmt? [Wright]
 - If you're printing 50 copies of something, then you're not going to get any other printing done [Petrie]
 - You could say that while printing is taking place, you should be able to receive a fax, but then it is more like requiring multitasking [Smithson]
 - that's more of a design parameter [Petrie]

- if you want to use denial of service, you need to be specific [Nevo]
 - for example, if you want to address buffer overflow, you need a specific test case so the evaluator can test [Nevo]
 - another thing would be to ignore malformed or illegal commands [Nevo]
- you could have a policy that says that a user can't queue more than 50 pages [Petrie]
 - that would be a policy not a security requirement [Nevo]
- would this include things like SYN floods? [Wright]
 - what would the MFP do? [Nevo]
 - recover after the attack [Wright]
 - the other factor is protecting assets while under attack [Wright]
 - we already have threats covering protection of assets [Nevo]
- there are vulnerabilities where under high attack load, other vulnerabilities are enabled [Walter]
- there are many kinds that we don't address, like buffer overflows, and those are supposed to be caught by AVA vulnerability analysis [Smithson]
- if we put threats in the PP, they must be specific [Nevo]
- we have one that says if all ports are open, it's a denial of service attack, that is very specific, and there's a mitigation against it which is to have a timeout and close those ports [Wright]
 - no way to distinguish attack from unusual circumstance [Smithson]
 - no matter, it's still a denial of service with a mitigation [Wright]
 - sort-of mitigation, it doesn't prevent the denial of service [Smithson]
- you'd hope that these devices would be designed with that level of robustness, that they would time out connections that don't get used [Smithson]
 - if port 9100 is opened and not used, what should happen? [Smithson]
 - it should time out and be closed [Wright]
 - yes, and if it doesn't, then it's a bug, so how is that different from opening all ports? [Smithson]
 - if you see all ports being opened from one source, then it's an attack [Wright]
 - sources can be spoofed, or more commonly, a distributed denial of service is used [Smithson]
- we're talking about bugs that can be exploited [Smithson]
 - if we know about bugs like that, why shouldn't we document them and put them in as requirements? [Wright]
 - it's an endless list, and that's what ALC_FLR is for [Smithson]

- if we define a threat, our understanding is that we must find an SFR [Ueda]
 - it is not a requirement, you can have an SAR, this is even covered in the CIM [Aubry]
- how can we resolve this? [Wright]
 - our recommendation is to remove DoS threats [Ueda]
 - can we try to describe these threats in prose, if not Common Criteria language, to distinguish that it's an attack? Then we could prescribe an appropriate mitigation [Wright]
 - if it's too specific and we codify the mitigation, such as close ports after N milliseconds, then we've given attackers the magic number of N-1 milliseconds to use in their attack [Smithson]
- how should evaluator test? [Ueda]
 - they could download attack scripts and run them [Wright]
 - do they use 5,000 packets, or 8,000 packets, or 100,000 packets? [Ueda]
 - the evaluator should be able to decide [Wright]
 - so it depends on the skill of the evaluator [Ueda]
- if we can't define it, mitigate it, or test it, the evaluator is going to reject it [Farrell]
 - we can look up SYN flood in wikipedia, and that says exactly what it is [Wright]
 - that's great for the main clauses of P2600, but not for PP [Smithson]
- {there was a great deal of additional discussion}
- homework for all to do for next {February} meeting
 - which T.DOS (and T.EA) threats are not testable
 - which T.DOS threats are never covered in other PPs or STs
 - what threats are not mitigatable
 - what other details are needed in the threat descriptions to make the scenario better understood - or to better understand the possible mitigations
 - what SFRs and SARs are applicable
 - **Note: please send comments to the mailing list as soon as possible so that we can discuss in advance of the February meeting**

T.DOS.FAX threats in PP-C [Chen]

- unlikely to have public-facing fax [Sukert]
- maybe in a hotel business center [Smithson]
- risk is low -- unlikely attack, low asset value [Sukert]
- decided: remove T.DOS.FAX.* from PP-C

Unrolling PP threats [Smithson]

Refer to <http://grouper.ieee.org/groups/2600/email/msg00641.html> .

- We have categorized threats in the PPs to make it easier to write the PPs
- However, we have ended up with same-named threats that have different meanings depending on the environment
- This can result in confusion, and it also makes it difficult to determine which objectives are intended to mitigate which sub-threats
- It has also resulted in some differences in description between clauses 1-9 and the PPs, because it has been necessary to write a combined threat description for the categorized threat, and that description can be different or at least inconsistent with the original threat descriptions
- Proposed:
 - Unroll threat categories and list each one individually in all PPs
- Why did we make this decision in the first place? [Wright]
 - It made the rationale tables in the PP shorter
- What is an example of same names / different meanings? [Wright]
 - T.TSF.CRED has a different meaning in each of PP-A, B, C, and D
- Any objections? [Wright]
 - {none}
- Approved. [Wright]

Unrolling Objectives [Smithson]

Refer to <http://grouper.ieee.org/groups/2600/email/msg00641.html> .

- Similarly, we have objectives with same names and different meanings in different environments
 - Example: O.GENUINE, O.NETWORK
- Objections? [Wright]
 - {none}
 - As long as the new names don't simply append the environment name, i.e. O.NETWORK.B [Thrasher]
- Approved [Wright]

Functional differences in STs [Chen]

Refer to <http://grouper.ieee.org/groups/2600/email/msg00660.html>.

- We define threats, objectives, and SFRs based on all functions of an MFP. However, if you want to use our PP for a device which doesn't have all functions, it could not comply because it does not fulfill the objectives.
- Didn't we talk about this a long time ago? I thought the rationale would be that when you write an ST, you'd say that a threat does

not apply because the functionality is not present in the device [Wright]

- It was on the list of things to talk about with NIAP when we met with them in Washington DC. I don't remember them telling us that it could not be done [Aubry]
- Several companies – Ricoh, Sharp, Canon, etc. – visited the Japanese scheme IPA late last week and IPA said that they could not accept an ST unless it addressed all of the threats listed in the PP. [Smithson]
 - That was their interpretation of reading the document, and they were hoping that it would be clarified in the document. [Petrie]
 - That's not what I heard, what did IPA say? [Smithson]
 - They said that it needed to be explicitly stated [Petrie]
- Regarding NIAP, they said look at the PKE PP for how to address it. [Wright]
 - Their answer at the time was that if the function isn't there, then it does not need to be addressed [Cybuck]
- JBMIA people discussed this issue, and our opinion was that if a fax security function is in the PP and your device does not have a fax function, then it must have a fax [Ueda]
 - Are there SFRs that are so specific? [Wright]
 - Network [Nevo]
 - Hard drive [Smithson]
- Which PP is the one that NIAP referred us to? [Wright]
 - It is the Family of PPs for PKE components, which is a Family PP that I used as an example of how we would not want to write our Family of PPs. It defines sixteen components and two EALs which can be combined to form any of thousands of virtual PPs, and the name of the PP would be created algorithmically. [Smithson]

(Note: it is this one --
http://www.commoncriteriaportal.org/public/files/ppfiles/PP_VID3004-PP.pdf)
- There is a French PP that is an example of functions that are explicitly stated, and the German scheme accepted this one. [Aubry]

Note: it is this one --
<http://www.commoncriteriaportal.org/public/files/ppfiles/pp0601.pdf>
- We had the same problem in IPP. It was called “conditionally mandatory feature” [Walter]
- You should stipulate that up front in the document. [Walter]
 - Yes, but there is no clear mapping from threat to objective to SFR [Thrasher]

- We may end up needing to do that anyway because SFRs apply to certain objects that we should specify [Smithson]
- Another problem is that IPA opinion may be different from NIAP [Ueda]
 - Did IPA say that you need to make a separate PP for each function? [Thrasher]
 - JBMIA proposed that we have a family PP for each environment. Each PP would address eight or so functions [Smithson]
 - This destroys the single family PP that you proposed? [Thrasher]
 - Yes, I would withdraw that proposal given this information [Smithson]
 - This is also what NIAP said, they proposed that we use the PKE family of profiles as an example of how to do it [Smithson]
- It's more than just the macro-level functions like print, scan, and fax. There are also functions like hard drive and network, and they can be combined in many dimensions. [Wright]
- I started writing a prototype of a family of PPs by function for environment A [Smithson]
 - Note: it is here --
<http://grouper.ieee.org/groups/2600/presentations/EISegundo2006/ppf-a-demo-24a.doc>
 - At the beginning, it describes the family and not a specific TOE. I defined TOEs for print, scan, copy, fax, non-volatile storage, network, and document server.
- How do you use this? [Wright]
 - For a particular device, you'd pick the PPs which apply and state that your ST complies with that list of PPs. They are individually named. [Smithson]
- Is there a way to mandate that you must have at least one of print, scan, fax, or copy? [Thrasher]
 - I didn't put anything about that in the document except that the names for each PP include "for Hardcopy Devices" [Smithson]
- This seems way overly complex [Wright]
 - It was overly complex before [Smithson]
- It seems like the ST writer could simply ignore SFRs that don't apply. [Wright]
 - Yes, but this tells them what exactly to do. Otherwise, they need to trace back from SFR to threat or from threat to SFR. I think we'll need to state these requirements clearly one way or another, and this brings those requirements into collections that can be used very easily [Smithson]

- Wouldn't we accomplish the same by having tables that say "these SFRs don't apply if you don't have fax, and these other SFRs don't apply if you don't have network"? [Wright]
 - We'll have those too. But there are some problems with the way it is written because the TOE overview and security problem definition describe all functions. I don't think it's a large step to clarify it. [Smithson]
- We can separate the issue of whether to explicitly state it versus having a family of PPs [Farrell]
 - Except that I think the IPA and NIAP are asking for family of PPs. [Smithson]
 - But the example you showed had applicability written into each SFR [Wright]
 - Perhaps we could do that, it would avoid writing multiple copies of SFRs. [Smithson]
 - You could do it as an app note [Wright]
 - May need to be more than an app note, because I think an app note is the equivalent of informative. [Smithson]
- So the question needs to go back to IPA to see if explicit statement is acceptable or is a family of PPs required [Wright]
 - We should ask NIAP also [Smithson]
- So what is "non-volatile storage"? Is it a little flash memory on the controller? [Farrell]
 - I tried to specify that it needed to be non-volatile document storage [Smithson]
- If you look at CC part 1, the way to comply with a PP is either strict or demonstrable, and despite my best efforts, I could not make demonstrable fit in our situation. [Smithson]
 - Demonstrable needs to be "more restrictive". The only way I could think to do that would be to have an alternate SFR, for example in the case of a fax, which says "Do not have a fax". [Smithson]
- Look at the draft Medium Robustness CIM, page 43, for a description of PP conformance [Cybuck]
 - I thought that Exact conformance was no longer part of CCv3? [Smithson]
 - It says that this text is taken from CCv3.1 [Wright]
 - We're claiming Demonstrable, which says it must be a non-strict superset of the claims of the PP [Wright]
 - The conformance rationale should demonstrate how each requirement is represented in the ST [Aubry]
 - We should still check with the schemes [Farrell]
- The problem will be if we have access control requirements for scan, but a device does not have scan [Aubry]
 - We don't break that out [Wright]

- Network connection would be a problem, because we have access controls that apply to network connections and also to local interfaces, so we can't throw out the access control SFR [Smithson]
- Conclusion: look at how we can be very clear about compliance if you do not have certain functions [Wright]

Sharp/IPA comments [Nevo]

Refer to <http://grouper.ieee.org/groups/2600/email/msg00672.html>

- We have discussed some of these already [Wright]
- field emissions was not clear to IPA, they did not understand that we meant only those emissions from cables and not from the whole device
 - it was unclear to people that we do not mean tempest-like requirements
 - the threat description in the clauses is very clear [Wright]
 - look at the description in the PPs, it is shorter because it is a threat category description [Thrasher]
 - it would help if we use full descriptions and not the short descriptions when we unroll threats [Thrasher]
- need to be more specific what we mean by “availability”
 - if we include paper as an asset, you would need a password to refill paper [Ueda]
 - no, we are not protecting paper as an asset in the PPs [Wright]
 - “timely manner” was questioned – it is subjective, and does not give enough guidance to evaluators [Cybuck]
 - Actually, “availability” is defined in the PP but is never used in the PP after that [Smithson]
 - It's not listed as an asset in the PP [Thrasher]
 - But if it is not an asset, then why have DoS threat? [Aubry]
 - add TOE availability to 1.2.3.3, clarify that it does not apply to external factors like fires, floods...
 - add EA to 1.2.3.3
- question: if someone turns off a security function, is the device no longer P2600 compliant? [Ueda]
 - it is still compliant, you can't control what someone does when the device is employed [Wright]
 - can anyone turn off those functions? [Ueda]
 - that is a matter of TSF access controls [Thrasher]
- definition of RESOURCE (for T.RESOURCE.COPY/PEER) needs to change, because it refers to unauthorized usage in the PPs but refers to physical resources in the clauses [Smithson]
 - it is only an accounting issue [Ueda]

- but it is important as a security function when accounting for usage is important to the customer or manufacturer, such as a lease based on usage or an environment like a university where usage is billed back to users [Sukert]
- physical versus IT: it says that we are protecting hardcopy form of user documents, and we should remove hardcopy from that definition
 - we are protecting that using PIN printing [Sukert]
 - but we still do not protect the paper output [Nevo]
 - T.UD.PHY.OUTPUT refers to paper [Aubry]
 - People interpret this as requiring a metal box locking up the output tray [Cybuck]
 - Our definition includes the “original document”, which we do not protect in any form, so we should definitely change that part at least [Smithson]
 - the rest of the definition needs to be more clear [Nevo]
 - “PHY” really indicates that it refers to physical documents [Smithson]
 - I disagree. The specific threats that we’re dealing with important to customers, and we are really protecting the paper output [Sukert]
 - no, we are protecting the electronic document from being taken by requiring a PIN before it is released on paper [Nevo]
 - but if you did have a locked mailbox mechanism, even if it is controlled by an IT function, then you would be protecting the paper and if we remove that from the threat definition, then you might fail the evaluation with that solution [Smithson]
 - yes, either PIN printing or a locked mailbox is a solution [Wright]
 - conclusion: remove the reference to hardcopy ORIGINAL documents; hardcopy output remains within scope [Wright]

SFR worksheet revision B [Smithson]

Refer to these documents:

<http://grouper.ieee.org/groups/2600/presentations/EISegundo2006/SFRworksheetsheet24b.xls>,

<http://grouper.ieee.org/groups/2600/presentations/EISegundo2006/sfr-notes.txt>

- At Lexington, I proposed a list of SFRs, and we looked at a number of additions at that meeting
- I looked at those additions, and upon further investigation, most of them were not such good ideas {details provided in the second document, linked above}

- FMT_MOF.1 required only by CIM – use only if our CIM analysis calls for it
- FMT_MSA.3 is a dependent requirement – put it in
- FMT_REV.1 does not apply to our situation – leave it out
- FCS_COP.1 for O.NETWORK seemed OK to use, but...
 - Why include it if we already have an SFR to protect network data? [Aubry]
 - Does it harm anything to include it? [Sukert]
 - It adds complexity and evaluation steps; in general we should not use redundant or unnecessary SFRs [Aubry]
 - FCS_COP refers to a way to achieve an objective, and was removed from CCv3.0 but put back in v3.1. Trusted channel more clearly addresses the objective without specifying the way to achieve it [Smithson]
 - If it's required for CIM, then it should be in the CIM annex [Wright]
 - I am going to check with CSC about this anyway [Sukert]
- FDP_UCT.1 and FDP_UIT.1 apply to complex crypto operations, and we already have FTP_ITC.1 – leave it out
- FTP_TRP.1 is for trusted paths to users, not to other devices (or users who are intermediated by devices) – leave it out
- FRU_FLT.1 and FPT_FLS.1 requires more than we intended with O.RESILIENT – leave them out
- FTP_ITC.1 for O.GENUINE seems reasonable to require for applets and software loads, but...
 - We haven't expanded O.GENUINE to include applets and software loads, and I wonder if this is the best objective name for that
 - Why are we requiring trusted channels? [Volkoff]
 - Confidentiality [Aubry]
 - Not integrity? [Volkoff]
 - If we can validate the image, do we care if it came over a trusted channel? [Wright]
 - Conclusion: rejected – leave it out – but we still need to work on the definition of O.GENUINE with regard to applets and software loads
- Explicitly stated SFR for O.FAXONLY is a good solution for an ST (although IPA said they'd reject such an SFR), but in any case it is too specific for the PP – leave it out
- FPR_UNL.1 for O.FAXONLY is part of the Privacy class, not appropriate for our objective – leave it out.

Note: final disposition is represented in this updated document:
<http://grouper.ieee.org/groups/2600/presentations/EISegundo2006/sfr-notes-24b.txt>

SFR Audit and Management requirements [Smithson]

- A brief description of the content of audit_notes and mgmt_notes was given, but we did not review them in detail.

Note: here are those documents --

<http://grouper.ieee.org/groups/2600/presentations/EISegundo2006/audit-notes.txt>

http://grouper.ieee.org/groups/2600/presentations/EISegundo2006/management_notes.txt

- However...
 - Japanese interpretation of “unspecified” audit means that “minimal” is followed plus perhaps additional requirements [Ueda]
 - That is different from what I thought, which was that “unspecified” meant that the specific set of requirements could be created without regard to the “minimal” set. [Smithson]
 - There are threats that we mitigate using O.MONITOR, and if we specify O.MONITOR then we must include them in audit [Aubry]
 - Need to look at where we are specifying O.MONITOR and make sure that we either audit those items or remove the objective. [Smithson]

Threat analysis recommendations [Aubry]

Refer to <http://grouper.ieee.org/groups/2600/email/msg00663.html> and <http://grouper.ieee.org/groups/2600/presentations/EISegundo2006/ThreatsAnalysisWorksheet-24c-asset.xls>

- I could not rationalize threat analysis with some decisions made during meetings
- We need to be able explain the reasoning for why we chose to include/disclude items in the PP
- I added an asset value for each asset category in each environment
- we need to explain items that were in the “red” category which we did not include, and also items that were in the “green” category which we did include [Wright]
- we have some rationale that was discussed in meetings, but others do not know what that is [Thrasher]
- you can create a mathematical process, but then you apply common sense and judgement [Wright]
- this spreadsheet will never see the light of day, it is not part of the standard [Thrasher]
 - but the risk ratings are in clause 7 [Smithson]
 - but not the numbers [Thrasher]
 - this is related to asset valuation methodology [Wright]

- what we need to do is look at the asset values that I've chosen for each environment and see if you agree, then we run the numbers and see how they come out [Aubry]
- should we put this in an annex?
 - Someone coming into this newly would benefit from it [Petrie]
 - We put the STRIDE/DREAD things into the annex, but there is no science to it [Thrasher]
 - Where did the calculations come from? [Wright]
 - I had some rationale for the formulae, but I do not think they came from Microsoft's threat analysis book [Smithson]
- Is there an action item to update annex E? [Wright]
 - We are removing the PP assignment portion from annex E [Thrasher]
 - So it would go in the "introduction to PPs" [Wright]
- {there was a long discussion about T.DOS.PRT.DELETE in particular and why it was not included in the PPs}

Compliance clause [Nevo]

Refer to

<http://grouper.ieee.org/groups/2600/presentations/EISegundo2006/MFD%20Compliance%20Clause-24a.pdf>

- This is an example of the compliance clause, only for environment A at this time
- It uses description from PP (A) plus examples from main body
- If we split the PPs out from P2600, then we need to express this without using common criteria nomenclature [Wright]
 - Main body of P2600 doesn't use CC terminology [Thrasher]
 - shouldn't use PP nomenclature, just the descriptive title is OK [Wright]
- one problem is that the PP text includes terms that may not be defined in the main clause, like "unauthorized user"
 - this is clause 10 of P2600, so any new terms that are used should be defined in clause 3 [Thrasher]
- Ron will make these for B,C,D then turn over to Jerry for inclusion in main draft [Wright]

Family of PPs proposal [Smithson]

- This proposal was for a single Family of PPs document that would cover all four environments. The family would be of one sub-PP for each environment. Given the need to distinguish subset functions, possibly using a Family of PPs for that purpose, this proposal was withdrawn.

Main document structure [Wright]

- potential structure
 - main clauses 1-10
 - guide to PP is p2600.1
 - PP-A is p2600.2
 - PP-B is p2600.3 etc
 - others can be added asynchronously
- alternative
 - place the guide material in each PP as an appendix
- the only problem I can see with the separate guide is that it won't be published along with the PPs on commoncriteriaportal.org, but then again, other PPs don't come with guides either [Smithson]
- the advantage of this is that we can add environments independent of the other documents [Wright]
 - this approach completely uncouples the main documents from the PPs [Thrasher]
 - we would still want to consider updating the main document if we add an environment [Smithson]
 - if the new environment added threats, we should update those in the main document also [Thrasher]
 - we're not required to do so, but it might make sense to do it [Wright]
- any objections?
 - Do we need to wait on this pending the design decision on the PPs, family or whatever? [Farrell]
 - This is independent of that [Wright]
 - But what about the family PP approach that Smithson was proposing? [Farrell]
 - I think that proposal is withdrawn, and we'll only need to decide on the design of PPs for each environment [Smithson]
- We need to create PARs for p2600.x
- We also need to reword main doc
 - I have defined what I think needs to be done [Thrasher]
- For the PARs, we'll need to describe more about the environment than just "A" or "B" etc [Wright]
-

Main clauses 24a review [Thrasher]

Refer to

http://grouper.ieee.org/groups/2600/drafts/FullSpec/IEEE_P2600_v24a.pdf

- This version contains editorial changes from last meeting
- {accepted}

- There are some discrepancies in the definitions of UFD, MD, and TSF data [Chen]
 - We need to check out UFD, MD, and TSF defs and threats
- We also need to add T.DOS.FAX threats to PP threat table (when moved to Guide to PPs)

Main clauses 24b review [Thrasher]

Refer to

http://grouper.ieee.org/groups/2600/drafts/FullSpec/IEEE_P2600_v24b.pdf

- This version contains comments that indicate where I think we'll need to make changes to restructure P2600 according to the structure proposed earlier today
- {accepted}
- For the "guide to PPs", Thrasher will extract text into an IEEE template [Wright]
- We also need to recruit an author for Guide to PPs. Glen Petrie of Epson is considering it. [Wright]

Comments database [Wright]

Refer to comments received:

http://grouper.ieee.org/groups/2600/comment-tracking/P2600_2006-12-Comments-V1.pdf

and disposition after review:

http://grouper.ieee.org/groups/2600/comment-tracking/P2600_2006-12-Comments-V2.pdf

- {We discussed each comment, many of which were duplicates, and resolved comments as shown in the disposition document referenced above. Here are the action items:}
 - remove references to blank paper/toner/etc from PPs
 - Sukert to ask evaluator about having unused terminology defined in a PP (like "auditor" in PP-C or "maintenance port" in PP-D)
 - external environment is an asset?
 - need to consider external environment as a customer's asset, sometimes their most important asset [Aubry]
 - someone to write up rough objective and asset
 - also get PP example from Carmen
 - look at T.UD.ACC.HACK interfaces (on sfr worksheet) -- should be different interfaces than normal

Next meeting [Wright]

- **Two full days** in Maui. For more information, refer to:
<http://grouper.ieee.org/groups/2600/meetings.html>.

Closing [Wright]

See you in Maui!

** Adjourned at 6:25 PM, 12/12/2006 **