

**IEEE P2600 Meeting #23**  
**October 23-24, 2006**  
**Lexmark, Lexington KY**

**Attendees**

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

Nancy Chen, Oki Data  
Nick Del Re, Canon  
David Freas, DAPS  
Satoshi Fujitani, Ricoh  
Tom Haapanen, Equitrac  
Harry Lewis, IBM  
Ron Nevo, Sharp  
Ken Ota, KonicaMinolta  
Glen Petrie, Epson  
Alan Sukert, Xerox  
Brian Volkoff, HP  
Bill Wagner, TIC  
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.

**\* Commenced at 9:15 AM 10/23/2006 \***

**Administrivia [Wright]**

The following administrative items were reviewed:

***Agenda review***

Refer to meeting slides for detail  
<http://grouper.ieee.org/groups/2600/presentations/P2600-Oct2006.ppt>

***Minutes and Agenda approvals***

The September 2006 minutes were approved without additional changes.  
The October 2006 agenda was approved with a few additions.

### ***IEEE patent policy***

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

### ***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-Oct2006.ppt>

### ***Officers and Editors***

No changes in Officers:

Chair: Don Wright, Lexmark.  
Vice Chair: Lee Farrell, Canon.  
Secretary: Brian Smithson, Ricoh.  
Editor (clauses): Jerry Thrahser, Lexmark.  
Editor (PPs): Brian Smithson, Ricoh.

**Note: We elect officers at the December meeting. If you are interested in nominating yourself for office, contact Don Wright.**

### ***Meeting schedule updates***

**Dec 11-12**, at Peerless, El Segundo, CA – ***expect two full days of meetings***. There will be a TCG meeting on Dec. 13 at a nearby HP facility.

*(2007 meeting dates/locations are still tentative)*

**Feb 22-23, 2007** with PWG, on Maui or other Hawaiian island. For TCG members, there will be TCG HCWG meeting, on Feb. 21.

- Finish draft if it hasn't been completed in December

**Apr 24-25**, location open (looking for East Coast, USA)

- Currently considering either Malwah, NJ (Sharp) or Piscataway NJ (IEEE)
- Handle comments from sponsor ballot

**May 30-31**, location open

- Handle comments from 1<sup>st</sup> re-circulation

**Jul 11-12**, location open

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

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>

## ICCC Update [Smithson]

(Web site for the conference: <http://www.7iccc.es/>)

- CCv3.1 final was announced, very few differences from CCv3.1 draft
- NIAP discussed what they had announced the week before, a policy change made necessary by budget cuts: They will not consider new evaluation projects unless they are (1) of interest to the NSA, and (2) target either medium or high robustness environments.
  - US government or the NSA? [Wright]
  - Announcement said the US government, but they say the NSA when they talk about it. NSA funds the NIAP CCEVS.
  - I asked NIAP for clarification but have not received a response [Freas]
  - Maybe if there is a lot of demand from other agencies, they will make exceptions.
  - One thing driving it is the pedigree of the software, where they have access to source for EAL5 and above, they need to give that more priority. [Cybuck]
  - Canada looks more attractive, and they also made a policy announcement, which we will talk about later.
- There was discussion about how costly, time consuming, and difficult it is to get CC certification. There were two camps: one wanted to make it easier, faster, and cheaper, and the other said that it was possible to get very good at integrating CC into the product development process and that changes to the CC are undesirable. I think that CCv3.1 will remain in force for some time.
- Were there presentations about better understanding or using CCv3.1? [Wright]
  - There was essentially nothing about writing PPs
  - There were a few things about writing STs, but not too much that was specific to CCv3.1 since it was so new
  - There were some good presentations about modeling security functional requirements, and about process for getting through evaluations, some of them I thought were very useful
- There was meeting of the CC Vendors Forum with the CC Development Board, which we will talk about later.
- When will the new CIM from NIAP be available? [Sukert]
  - I asked Audrey Dale, and she said it should have been in October (to coincide with the policy change) but is more likely to be November. Howard Cohen is working on it.

Subsequently, I contacted Howard and he said that the draft is complete and is in internal review, but still no firm release date.

- Next ICCC is in Rome, and in 2008 it will be in Korea.

## **INCITS CS1 update [Thrasher]**

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

- Std for protection of personally identifiable information
  - It is based on PCI
  - held up awaiting copyright release from VISA
- CCv3.1 has entered into ISO process to be an update to 15408
  - not fast-tracking
  - 1 - 1.5 year process
  - first working draft
  - is the same thing that was presented at ICCC? [Wright]
    - appears to be final copy, definitely not 3.1 draft

## **CCVF update [Smithson/Thrasher]**

(No CCVF web site – yet :-)

- CCVF got an audience with the CC Development Board, and made their case for why vendors should have more input and earlier input into the CC development process. What they got was an agreement from the CCDB to consider the matter at their next meeting (in six months). They said they couldn't make a decision because not all of the CCDB members were present at this meeting. [Smithson]
- The CCVF came in with a list of things that they wanted to request as changes, but didn't get that far. Instead, they only got to discuss whether or not CCVF should be considered as a source of input along with the national scheme representatives.
- The CCDB seemed to like the idea only because it funneled all vendor input through one organization to resolve inter-vendor differences. [Smithson]
- There were a lot of people there. It was announced at a plenary, so many people found out about the CCVF who didn't know about it before, especially vendors outside of the US. [Smithson]
- It's a good source of information. We found out about the Canadian policy through CCVF. [Sukert]

## **Action items from previous meeting [Wright]**

Main action items were updated on presentation slides:

<http://grouper.ieee.org/groups/2600/presentations/P2600-Oct2006.ppt>

Action item spreadsheet was reviewed and updated:

- Pre-meeting:  
<http://grouper.ieee.org/groups/2600/actionitems/P2600-action-items-20061020.xls>
- During meeting:  
<http://grouper.ieee.org/groups/2600/actionitems/P2600-action-items-20061024.xls>
- Post-meeting:  
<http://grouper.ieee.org/groups/2600/actionitems/P2600-action-items-20061102.xls>

Some items generated additional discussion:

- ideas for benefits of funding PP evaluation
  - (see slides for some ideas already considered)
  - We may need to re-evaluate our approach because of the NIAP policy changes
    - Xerox is working on this with CSC to go through the Australian scheme [Sukert]
    - We talked with COACT and SAIC about this before the NIAP policy change, so we should now go back and talk to them again [Wright].
    - At ICCC, I spoke with the director of EWA Canada and they would be happy to evaluate our PPs. I mentioned our budgetary estimate of \$25K per PP, and he said that would be about right for them. They seem like a very competent lab, given several presentations they gave at ICCC. [Smithson]
    - Also at ICCC, there was some discussion about US government requirements being not mutually recognized. The NIAP response was to the effect “the US Government reserves the right to set its own requirements”, and that would indicate that the new CIM will not be very different from the old CIM. [Smithson]
- Some of the older action items having to do with conversion to CCv3 were marked complete in the action items list (with some notes that they do not include CIM requirements). The details of those action items are often obsolete, and so I suggest that we create new action items as needed. [Smithson]
- A.NO\_GENERAL\_PURPOSE is marked complete, and I propose that we can't make that assumption. It would require an environmental objective, and I don't think we can set such an objective on behalf of our customers. [Smithson]

- If other PPs make that assumption and that objective, why can't we? People have loaded Linux onto routers and used them for general purposes. [Wright]
- I can't defend the other PPs, but I think they assume that products like routers will be in a more protected network environment than an MFP in an open network and open physical environment. [Smithson]
- AI#240 "strength of function", I think we should not be so specific as proposing a password policy, we should leave it to the ST writer [Smithson]
  - But someone could use a weak password and still be compliant [Nevo]
  - Is there anything in the CIM that would require this? [Wright]
    - No, there are some policies that place requirements on passwords [Cybuck]
  - We could give some examples or suggestions in a PP app note, but not in an SFR [Smithson]
  - There are so many ways to define strong passwords, we could refer to them in an app note but should not pick one. If we set a minimum like four numerics or eight alphanumeric, that be so weak that specifying it does more damage than leaving it to the ST writer and ST evaluator to make a proper judgement [Smithson]
  - We can discuss during the SFR discussion [Wright]

## Email issues [Wright]

### *PP certification*

- NIAP policy based on budget
- Canada has new policy based on workload [Sukert]
  - If they get too many requests, then they will look at whether there is a Canadian customer and what EAL level is being requested [Sukert]
- other countries? may have language issues
- question asked of Audrey Dale: will NIAP recognize our P2600 profiles, or need to make US Govt profiles based on P2600? [Freas]
- Xerox looking at using CSC to do evals through Australia [Sukert]
- Cybuck will contact SAIC, BAH [Cybuck]
- Thrasher will contact COACT (they don't have international offices but may have some plans) [Thrasher]
- issues
  - English language support
  - need to support BRE/MRE CIM?

- FIPS 140 issues?

### ***Production printing [Lewis]***

- Alan, Harry, and Carmen working on this [Sukert]
- what is production printing?
  - some think it is enterprise mailroom
  - others think transaction printing
    - this one is more important
    - both roll-fed and high speed cut-fed
- asset value
  - books
  - personal data
    - this one is more important
- physical protection
  - higher level of security than general enterprise
  - a tightly controlled manufacturing facility
  - example: check-writing facility in CA, if a check was missing, nobody left the building [Petrie]
- but now, data feed may be coming in from outside
  - some customers are asking about the same network vulnerabilities that you see in other environments [Sukert]
  - concern is building among customers
  - not so much concern about hardcopy security
- biggest benchmark is production speed
  - makes decryption difficult at speed
  - also have issues with delete/overwrite
- short-run versus long-run
  - 98% of jobs are short run, but 98% of volume is long-run [Petrie]
  - these are more like digital press printing
- DAPS hasn't been asking for CC for production printing [Freas]
  - primarily a cost issue [Freas]
  - does DAPS do a lot of its own evaluation as part of its purchasing decision? [Smithson]
    - beginning to do more security eval [Freas]
  - what kind of printing does DAPS do? [Lewis]
    - manuals etc [Freas]
    - so it is more publishing than transaction printing
  - would some be military manuals that have confidential or secret information? [Wagner]
    - yes, there would be some of that [Freas]
- base on an existing profile, or a new one? [Wright]
  - probably not PP-D because of too many differences from SOHO [Smithson]
    - higher EAL
    - other differences in basic assumptions

- would need to have its own profile
- where would it fit in the hierarchy? [Freas]
  - between B and C? between C and D? [Wright]
  - not sure where, maybe off to the side [Smithson]

### ***Managed services [Sukert]***

- in managed services environments, you get a mix of environments to be supported
- question asked was: how would P2600 apply if you have one customer that has a variety of products
- is there confidential info that the management company will be able to access
- MS company has access to your network
- would this apply to an PP-A environment? [Thrasher]
  - could be, although more likely PP-B
  - could apply to A [Cybuck]
- can the customer change the counters? maybe this requires different roles [Volkoff]
- we have different roles, but I don't think they map very well to this [Smithson]
  - we have user, dev admin, sec admin, net admin, auditor, if we define these too narrowly then we might end up with a profile that doesn't fit a market [Smithson]
  - also, the way we group things, like address book is part of management data or user job logs are in the same category as audit logs, might cause us problems later [Smithson]
- adding a new actor "managed services" could be a solution [Petrie]
- do we need to do anything? [Wright]
  - consider this during discussion of CCv3.1 threats/objectives/SFRs/SARs

### **JBMIA activities [Smithson]**

- JBMIA's P2600 study working group had a kickoff meeting on Oct 16
  - Participants were OKI DATA , Canon , KyoceraMita , KonicaMinolta , Sharp , SeikoEpson , ToshibaTEC , Panasonic , FujiXerox , Brother , NEC , Ricoh
  - WG leader is Mr.Uchiyama(Ricoh) , and WG sub-leaders are Mr.Masui(FujiXerox) and Mr.Iwasaki(Sharp).
- Most of participants aware about P2600 activity, but they were passive to that until recently.
- Some members think that they want to study P2600 PP through this activity, but plan is not to write a new PP but instead to feed their comments through their company representatives

- Will they have a person assigned for that, or use someone like you? [Wright]
  - No, each company will use its own representative in P2600, no designated liaison
- Next conference will be held on Oct 30; they meet every two weeks
- They expect to finish their work by the end of November
- I will be in Tokyo and could meet with them [Wright]
  - The invitation is still open for you to meet with them
- How will they wrap up in November if we have not wrapped up? [Wright]
  - It is not clear to me
- Since they have representatives already in P2600, why is this a separate study? [Wright]
  - Some of it is cultural, also some issues have been relayed through Ricoh and other companies, and some of it is distance and language, plus some companies have not participated at all
  - There is some concern that PP-B is too onerous [Canon]
  - Also some concern about lack of difference between PP-A and PP-B.
- Any action we need to take? [Wright]
  - We should publish information sooner than usual, not right before the December meeting
  - Also, if there is information we know is going to change, we could annotate it [Wagner]
- They are hoping to see a CCv3.1 compliant draft to review [Ohta]

## **TCG update [Volkoff]**

- standard will be behavior-based
- will not have MFD manufacturers open their architectures and follow TCG specs
- it will be based on interfaces
- we have spent time on service providers versus manufacturers versus IT administrators

## **Document structure [Wright]**

- IEEE editors have some issues with the current structure in which we have PPs as annexes which themselves have annexes and front matter
- they propose a different structure:
  - P2600 would contain existing clauses
  - compliance would not refer to the PPs
  - PPs would be separate standards (P2600.1, .2, etc)
  - would have their own front matter, etc
  - could be added asynchronously

- we could complete the clause work without waiting for PPs
- we refer to what is in the PPs in the clauses [Thrasher]
- we also define the four environments in the clauses, but we are now talking about another one [Smithson]
- we would need to resolve what is in which profile before P2600 was done
- annex E would be very tricky [Thrasher]
  - may need to remove it [Wright]
- so you could be compliant with P2600 and not a PP? [Yami]
  - yes, you could be compliant with P2600, or a PP, or both, you'd have all options, it really cleans up the structure quite a bit
- the main clauses could be approved/released earlier
  - there may be forward refs that need to be resolved [Farrell]
  - yes, or you could release them together as we have been planning to do
- can you add another PP without resubmitting P2600? [Farrell]
  - you could do an amendment, just an editorial instruction, you would still need to
- I thought that we would release the PPs with full front matter, but strip that off when it is an annex of the IEEE standard
  - That could be more confusing
  - Yes, especially if we refer to such items in the main body of the PPs [Smithson]
- Other than synchronizing the references, what other problems might there be?
  - I am concerned that if it is a standard, it may be in conflict with the PP standards [Smithson]
  - Would it matter if what was in P2600 was less specific than what is in the PPs?
- If the compliance clause was more specific than the PPs, could someone claim compliance to a P2600 PP and not to the main P2600 standard? [Smithson]
  - yes
- how do I state compliance? [Petrie]
  - For example, you could say a product is compliant with P2600 and is certified with P2600.1 or whatever
- Clause 5 is written around the PPs, but isn't otherwise very relevant to the main document [Sukert]
  - The PP could say that the environment is described in P2600 5.1, and if you add a PP, you could
- One way to solve some of these problems is what I was going to discuss later, which is to combine the four PPs into a "family of PPs" [Smithson]
  - there are a few examples of family PPs that are already certified

- you would write an ST that is compliant with one of the four security options that are provided for in the family PP, like P2600 PP level A
- by combining them, you would also solve some of Glen's issues about boilerplate that has small differences between different PPs [Smithson]
- also, you could pull clause 5, annex E, and those tables in clause 7, out of P2600 and put it in the one family PP where they are really used, without having to duplicate all of that information in each PP [Smithson]
- how would the eval labs deal with it? [Wright]
  - it could be a little easier than dealing with four PPs that have subtle differences [Smithson]
  - one existing family PP has four security levels for a class of products, which are concentric or hierarchical like ours [Smithson]
  - another one has components and EAL levels that can be mixed and matched to form any of thousands of virtual PPs – I don't suggest we do that [Smithson]
- you could still have that as a separate standard
  - yes, I think this would actually help solve some of the problems introduced by the IEEE's suggested restructuring [Smithson]
- you would only need to get the PP evaluated once [Farrell]
- how would that work if you have one PP at EAL3, two at EAL2, and one at EAL1, and you could mix like a Chinese menu, how would it be evaluated?
  - I think we would pick them explicitly, PP-A at EAL3, PP-B and PP-C at EAL2, and PP-D at EAL1, so there are only four choices [Smithson]
  - We would need to unroll our rolled-up threat descriptions, but I think that has other benefits, and then we would say which ones apply to which environments, which objectives apply to which threats, which SFRs, which SARs, etc. [Smithson]
- When we get to my SFR/SAR proposal, I rolled all four environments into one analysis because it was easier to look at that way, so I can see how that part would work already [Smithson]
- Also, from a document management perspective, having a single document makes all of that introductory information easier to manage without the small amounts of drift that we have experienced with separate PPs [Smithson]
- Wouldn't we still want to have the definitions of the environments mentioned in the main P2600 document?

- Yes, it is needed because we describe mitigation techniques and threats in the context of those environments [Sukert]
    - But we could still duplicate that part in a family PP
- Could you put the main document in each PP and have no main? [Petrie]
  - It makes more sense to have them independent documents [Farrell]
  - The main stuff is not even part of the profile [Thrasher]
  - It would be difficult for evaluators to deal with
- Agreed to restructure P2600 main document plus one or more P2600.n PP standards
  - main document may be recommended practice or standard (not decided yet)
  - if standard, it could only require PP compliance, or it could have its own compliance requirements (not decided yet)
  - could release early or at the same time as the PPs (not decided yet)

## Compliance clause [Nevo]

Refer to

<http://grouper.ieee.org/groups/2600/presentations/lexington2006/MFD%20Compliance%20Clause-23a.doc>

- Ron created a document with compliance requirements in two sections, section A for manufacturers and section B for IT professionals [Wright]
- I think Ron did a good job, but the concept is wrong. About half of the items are implementation-specific requirements and the other half are redundant requirements that are already in the PPs [Smithson]
  - For example, item #1 requiring MAC/IP filtering to protect against DOS attacks is one specific way to do it, but there are other possible firewall approaches that would be precluded by compliance with this requirement [Smithson]
  - For the other example, #2 is fully covered by the PP and so it seems like there is no need to have it repeated here, and there is some risk that we would have some conflicting wording [Smithson]
- These are necessary for compliance? [Wagner]
  - Yes [Wright]
- Would it be presented this way, or with references to earlier portions of the text? [Wagner]
  - This would be a clause 10 [Wright]
  - Also, we would need to specify which environment it applies to

- Originally, I envisioned a table that referenced earlier text for each environment [Wagner]
  - We would need to wrap some text around it, putting “shalls” in as needed [Wright]
- Using #1 as an example, even though MAC filtering is a good idea in all environments, we might say that is mandatory in environment A, and leave it as a recommendation in other environments [Haapanen]
- The problem I have with this is that we’re specifying MAC filtering and non-whitelisted addresses which implies that you have whitelists, and precludes the use of other firewalling techniques that don’t necessarily use MAC addresses or use blacklists or whatever. There are many possible ways to reduce DoS attacks, and we are requiring only one of them [Smithson]
  - This is the only thing we have in the whole document that relates to filtering [Nevo]
  - We could leave this in the mitigation techniques, but rewrite the compliance requirement to be more generic, such as MAC address filtering or similar firewalling technique for reducing DoS attacks [Wright]
- If we made it more like an objective to reduce DoS attacks by preventing unauthorized connections, then it would be OK. We don’t have such an objective in the PPs now – maybe we should – but to require specific techniques means that we are creating a technical specification for how to build MFPs [Smithson]
  - In general, we’re better off to describe the result and not the means, unless you’re trying to make things interoperable, but we’re not doing that in P2600 [Wright]
- If we keep it at an objective level, then I think those objectives should go into the protection profile unless there is some kind of objective which cannot by its nature be included in a protection profile. I read through this list and didn’t see one like that, and haven’t thought of any either [Smithson]
  - What about #2 “network interface will recover in a timely manner after a DoS attack”? That’s an objective which could be written into a compliance clause [Wright]
  - Yes, and that’s already in the PP – O.RESILIENT. [Smithson]
  - #3 could be rewritten without specifying “priority” as a mechanism, because multiprocessing or other techniques could be used [Wright]
- If we make a change here, shouldn’t we go back and change the original document? [Nevo]
- The other thing you could do is state the general objective in the compliance clause, and reference suggested mitigations [Wright]

- What if we took the list of objectives out of the PPs and put them here, saying “these are the compliance requirements”? [Smithson]
  - Is that a 100% match? [Wright]
  - It should be. What we have here is about half are implementation specifics that I don’t think we should require, and the other half are PP objectives. [Smithson]
- If we copy the objectives into a compliance clause, how is that going to be better than just leaving them in the PPs? [Farrell]
  - What we could do is reference mitigation techniques. “You shall do this, and see xxx, yyy, and zzz for specific techniques”. [Smithson]
- Here, you have more detail than in the PP objectives. [Nevo]
  - The additional information would be the reference to examples [Wright]
  - We would need to remove CC-specific language [Wright]
- What would be here that would not be in the PPs? {Wagner}
  - There would not be any references to techniques in the PPs [Wright]
- So you could claim compliance by fulfilling the objectives of the PP for your target environment, and optionally you could get CC certified by fulfilling the SFRs that support those objectives in the PP [Smithson]
- Agreed to this approach: restate the PP objectives (not in CC terminology) and provide references to example mitigation techniques. [Wright]
- What about the IT manager’s requirements? [Nevo]
  - I’m not sure that there’s any value in saying that an HCD has been installed in accordance with P2600 [Wright]
  - Do we want our standard to cover IT environments? [Smithson]
    - We said we do, in the PAR [Wright]
  - We have environmental objectives, like have a nice network and manage it and train your users [Smithson]
  - This might be an area where we have additional objectives that may not be appropriate in a PP [Smithson]
    - They all should be in the PP [Wright]
  - For example, O.PROTECT says what feature should be present, but doesn’t tell the IT professional that it should be enabled [Wright]
    - There is an assumption that IT professionals will configure it according to manufacturer’s guidance [Nevo]
    - For which we have an objective, OE.TRAIN [Smithson]
    - We tell them they must be trained, but not to do it, maybe we need an OE.ADMIN [Wright]

## Basic Robustness CIM mapping to PP-C [Chen]

Refer to

<http://grouper.ieee.org/groups/2600/presentations/lexington2006/Basic%20Robustness%20CIM%20mapping%20to%20PP-C%20Requirements.xls>

- (walked through the document)
- Some discussion points:
  - How will the mapping change based on the CIM for CCv3.1?
  - Should we worry about CIM compliance if NIAP isn't going to certify because of their budget problems?
  - Shouldn't we get a head start and do similar mapping for PP-A and PP-B?
  - Should CIM items be in the PP simply as AppNotes for the ST writers?
- Action: Create the PP-A and PP-B mappings for the existing CIM now (PP-A: Sukert, PP-B: Nevo)

## Clause 1-9 comments [Wright]

- Mostly editorial comments (from Alan Sukert)
- Results posted here: <http://grouper.ieee.org/groups/2600/comment-tracking/oct2006-results.pdf>

## Threat/Objective/SFR/SAR analysis [Smithson]

### *Threats/objectives:*

Refer to

<http://grouper.ieee.org/groups/2600/presentations/lexington2006/SFRworksheets23c.xls>

- (walked through the process)
- Group decided to add O.NETWORK to T.DOS.NET.CONNECT|CRAFT|FLOOD (rationale: flow control helps mitigate the threat)
- Agreed with proposal to remove O.PROTECT from all threats except T.UD.SALVAGE and T.TSF.SALVAGE.
- Agreed with proposal to remove O.ACCESS, O.NETWORK, and O.MONITOR from T.TSF.CRED.GUESS, and to add OE.TRAIN to T.TSF.CRED.GUESS
- Decided to add O.DELETE to T.TSF.SALVAGE (rationale: consistent with T.UD.SALVAGE)
- Unresolved: should T.TSF.SALVAGE be used in PP-C?
- Agreed in principle with proposal to remove T.TSF.SW.UPDATE from PP-D, but need to check with Carmen Aubry.

- Unresolved: there was some lack of clarity about whether T.EA.FAXBRIDGE should be used in PP-C.

### **SFRs:**

Refer to

<http://grouper.ieee.org/groups/2600/presentations/lexington2006/SFRworksheets23c.xls> and to

<http://grouper.ieee.org/groups/2600/presentations/lexington2006/pp-sfrs23c.doc> as discussed. Some results were posted in

<http://grouper.ieee.org/groups/2600/presentations/lexington2006/SFRworksheets23d.xls>

- Group agreed with the overall proposal.
- we need to go through the applicable SFRs and look at the audit and management recommendations in CC part 2 and consider adding audit/mgmt SFRs accordingly.
- Decided to add FCS\_COP.1 (and related dependencies) to O.NETWORK for environments A (user and mgmt data) and B|C (mgmt data only).
- Decided to add FDP\_UCT.1 and FDP\_UIT.1 to O.NETWORK for environment A.
- Considering adding FMT\_MOF.1 to ORACLES to environment A and maybe B|C (for CIM)
- Considering FMT\_MSA.3 for ORACLES for A|B and maybe C
- Considering FMT\_REV.1 for O.ACCESS (would this be used for such things as deleting a user?)
- Considering FRU\_FLT.1 and its dependency FPT\_FLS.1 for O.RESILIENT (instead of ATE\_FUN.1)
- Considering expanding the definition of O.GENUINE to include validation of software updates and applet loads
- Considering FTP\_ITC.1 for O.GENUINE (if we decide on #8)
- Still looking for an SFR or extended requirement for O.FAXONLY

### **SARs:**

Refer to

<http://grouper.ieee.org/groups/2600/presentations/lexington2006/SARworksheets23a.xls> and to

<http://grouper.ieee.org/groups/2600/presentations/lexington2006/pp-sars23a.doc>

- Group agreed on the overall proposal.
- Everyone seems to want ALC\_FLR for environments A|B|C

### ***Users/Subjects/Interfaces/Objects/Operations:***

Refer to

<http://grouper.ieee.org/groups/2600/presentations/lexington2006/usioo23a.xls>

- Presented an incomplete example of an entity model
- Proposed that an example entity model be completed and used in examples in PP application notes.
- The SFRs would not specify particular entities, but the application note examples would help guide the ST writer by demonstrating the intention of the PP SFRs.

### ***Family PP versus four individual PPs:***

Refer to

<http://grouper.ieee.org/groups/2600/presentations/lexington2006/pp-abcd-demo-23a.doc>

- Proposed that we consider making a single "family of PPs" document instead of making four individual documents.
- There was some skepticism about how this could be done
- A throw-away example was drafted (pp-abcd-demo-23a.doc). It shows some ways to put four PPs into one, from front matter through security objectives. The SFRs and SARs were not modified in this document, because they are already rolled the SFRs and SARs into single documents pp-sfrs23a.doc and pp-sars23a.doc.
- A straw poll was taken to see who thought that a family PP might be a good approach and who thought that it wouldn't be a good approach. There were six in favor the family PP approach, five opposed, and the rest (four or five) undecided.
- It was suggested that a PP editor's meeting could be held before the next (December) P2600 meeting. Sharp's facility in Malwah was suggested because of its proximity to Nevo, Chen, and Sukert, and central location to Smithson and Aubry

### **PP-C review [Chen]**

Refer to

<http://grouper.ieee.org/groups/2600/drafts/ProtectionProfiles/pp-c-23a.pdf>

- Addressed some action items
- Fixed some formatting on SARs

### **Sameer Yami's comments [Yami]**

- assurance maintenance

- it's not something you add; it's a process, not an SAR [Sukert]
- it was in ccv2.x
  - not anymore [Smithson]
- what about storing encryption keys while data protection is required? you cannot store them on the encrypted disk
  - O.PROTECT is for nonvolatile devices when removed or disconnected from the device, like a hard disk or flash card, but it would not apply to flash that is SMT mounted, so you would store your keys on something like that [Smithson]
- does out-of-box security mean that it is secure right away or can be secured?
  - CC requires you to test as shipped [Thrasher]
    - not anymore, now you need to provide documentation that allows you to get from as-shipped to as-evaluated, and the evaluators perform that too [Sukert]

### **Next meeting [Wright]**

- December 11-12 in El Segundo, CA (near LAX) at Peerless.
- Expect two full days to meet in El Segundo.

### **Closing [Wright]**

See you in El Segundo

***\* Adjourned at 4:35 PM, 10/24/2006 \****