

NNSC Teleconference  
March 18, 2005

Callers:

Voting NNSC members: David Brown, Intel (DB), Jeff Turmel, Brady Corp. (JT), Phil Smith, Trustwave (PS), Eric Schatina, Trustwave (ES), Pat Polazzo, Sun Chemical (PP), Rich Carter, AAMVA (RC), Lew Kontnik, Amgen (LK), Don Snyder UL (DS), Graham Whitehead, GDW Consulting (GDW),

NNSC Contributors: Michael O'Neil, Northstar (MON), Rick Ward, Appleton (RW), Dan Thaxton, Standard Register (DT), Ann Whitehead, NASPO (ABW)

David Brown chaired the session.

Opened with welcome to everyone, all attendees identified themselves.

The NASPO Anti-Trust Policy was read.

Agenda reviewed.

GDW reviewed the Actions from Feb. 24 meeting

Action 1 – ANSI roster needs confirmation from Larry Jellen, Government Printing Office, and Lew Kontnik. As Lew was on the call, he tentatively agreed as his point of concern re: scope was being addressed. Don Snyder agreed that UL be included.

Action 2 – to reword section 3. This is done and will be reviewed later in meeting.

Action 3 – inclusion of protocol should be in NASPO Audit procedures, not Risk Management Requirements. Point is still open for debate

Action 4 – to stress the confidential process. Point is already included in Standards and matter closed

Action 5 – to put definitions back in to public document. Some rewording may be needed to reduce giving too much detail. Rewording should avoid indicating HOW requirements are to be satisfied.

Action 6 – Add subsection re: chain of custody. New Section 5.4.12 added - Complete.

Action 7 – Section 5.4.5 re: 'custody' to use wording as per George Philips (ISP) - Complete

Action 8 – Look at work done by Trustwave and look at how to improve security of IT particularly personal data. Trustwave also proposed boosting some electives to mandatory. All members had been asked to review and comment. Neither GDW or DB have received any input to date.

DB proposed adding language to stress importance of protecting audit results. DB was of the opinion that Audit reports would be more valuable to the bad guys than the Standards because they indicate which risks are being managed and which are not. GDW expressed some concern that drawing attention to audit reports may be helpful to the bad guys who might make special efforts to obtain them. GDW advised that the special language proposed by DB could and

perhaps should go into the Auditing Standards document rather than the Risk Management document.

Discussion followed. The following points were made :-

- Section 7.0 states that there would be a report, therefore common knowledge and therefore wording to stress the importance of protecting the audit results could be added (JT and PP).
- audit report is confidential to audited company, so company free to disclose as much as they want as part of a customer/supplier relationship (DB).
- would not want third parties to see actual wording of audits, but NASPO could issue a summary (ES).
- audit report is company property, NASPO will not disclose Audit report, company can come to NASPO to find class, but only with written approval from Audited company (MON).
- NASPO must ensure that what is released is only top level, no details (ES).
- an RFQ could ask for class, but unreasonable to expect details, business details only, the same as asking about ISO certification (LK).
- NDA's prevent companies from revealing who they do business with, using this example, would NDA prevent NASPO from releasing certification confirmation? (RC).
- issue is whether disclosure is to internal company auditors or to other companies (LK).
- only want to share classification, no details (JT).
- without prior approval from a Certificate holder, NASPO will confirm only that an organization is or is not a Certificate holder. The present policy of NASPO is to reveal the Class of Certification only after prior approval has been given by the Certificate holder (GDW).
- MON believes that everyone should be seen as a Class 1.
- DB questioned whether present process is adequate or should it remain an Open Issue. RC considered that the present process raises some concerns.

**OPEN ISSUE** – verification of NASPO position on disclosures.

DB proposed closing out discussion of topics from February 24 and moving to look at Scope. He asked LK to open discussion.

LK explained that user companies already have obligations to standards so that control of security products is already protected. In turn, they (the Pharma manufacturers) are obligated to follow security standards imposed by their customers (the buyers of Pharma products) but these standards may need to be stronger.

DB explained his personal concerns within Intel, that secure products do not 'go out the back door'. Need to protect technology by the time it gets into end product. Referred to the NASPO layer and the need for some requirement on end user.

LK agreed. Sees NASPO being aimed more at the security 'providing' industry – still has some problem with the idea of security technology users being audited. RC – look at different products, some individual products are alright, but anything that is shared between several customers gives concern.

LK recognized challenge of sharing, felt there needs to be good practice within the user arena, thinks onus should be on manufacturers, and that users should not be regulated.

DB used an Intel packaging site as an example of where integration of multiple security products takes place.

DB hopes that NASPO certification will be used to cover all users.

LK agreed that the obligation is on the provider to show they are protecting all customers.

RC – as a customer, he feels that he is entitled to know when others are using the same product, any further details are a business discussion. Expecting more is really more than NASPO can be expected to cover JT agreed.

JT expressed serious concern over the words added in the rewording of Section 3.2. He requested that the last two sentences of the reword be removed as they were too onerous and speculative.

DB asked for an agreement on striking out the last two sentences of the Section. It was agreed.

ACTION – GDW to break out Section 3.2 in the reworded state and circulate to all participants. After circulation and comments there would be a letter ballot.

DB asked for a quick discussion on Agenda Item 6 – what open issue should be tabled for the next telecon? He proposed the Trustwave input be tabled as the next item for debate.

GDW proposed that as the Trustwave input covers the need for strengthening IT security in general and also makes specific recommendations to raise some electives to mandatory requirements that the Trustwave material be the subject of two meetings.

JT, PP and MON agreed that there needs to be some changes to the certification details and therefore two discussions may be necessary.

The next teleconference meeting will be held on

**April 8, 2005 at 8.00am PST.**

**Tel. 916 356 2663**

**Bridge #4**

**Passcode 5792459**