

**NNSC Teleconference**  
**Thursday, September 27, 2007**  
**10.00am PST**

Chair: David Brown, Intel (DB)

Callers: Graham Whitehead, NASPO (GDW); Chuck Hardester, NAPHSIS (CH); Shawn Cashin, AAMVA (SC) on behalf of Tom Wolfsohn, Bob Tillman, ARMA (BT), Tim Miller, TUV Rheinland (TM), Andreas Gehrmann, TUV Rheinland (AG), Kevin Kaporch, GPO (KK); Eric Geiger, Brady Corporation (EG); Win Baylies, SEMI (WB); Alex Lewis, Kurz USA (AL). Ann Whitehead, NASPO (AW) – minutes.

DB opened meeting. Checked who was on line. Stated that he had been unable to attend the NASPO Standards Committee meeting in Chicago in early September and was working from the minutes of that meeting. He noted that a lot of time had been spent on work done by Andreas Gehrmann of TUV analyzing ISO standards. He raised the question of whether the revision of the NASPO standard should reflect the language and terminology used in ISO standards, and if it should reflect the ISO language, to what degree?

GDW noted that Andreas had done a superb job of comparison of all the Security Assurance, particularly in the IT and Supply Chain sections. He added that ISO tend to be area or technology specific.

DB asked if TUV would be willing to continue the work and explicitly detail the changes in language and terminology to better align the NASPO standard with ISO. He had an affirmative answer. AG confirmed that TUV is fully behind this work.

TUV have been asked to clarify and list ISO overlaps with NASPO standard and to distil it down as much as possible. The list will be brought to the next meeting and the group will edit the NASPO definitions to be more in line with ISO language, assuming that there is agreement about the meaning, and if necessary add to the NASPO definitions.

DB sees two areas of work – IT and Supply Chain. He sought the committees input as to whether there was a conflict. ISO has Type A, Type B and Type C. Asked AG and TM for clarification of these Types.

AG stated the NASPO standard is not Type A which is Management application. Could be Type B or C. used in connection with 27001 or 9000 AG considered that NASPO does not fit exactly but 27001 is the best related. He also clarified that IT in ISO is Information protection, which is information in any format – electronic, paper etc.

DB appreciated that clarification.

GDW asked if NASPO could circulate the work that TUV had done and AG gave agreement.

DB asked that the work be circulated to all formal members of the NNSC and any other interested parties. He asked about the possibility of becoming an annex to ISO 27001, but Ag considered that that would be a very long process.

DB asked for comment on meeting the ANSI requirement and the ISO concurrently.

KK stated that this would bog down the process. GDW concurred and proposed that the NNSC meet the ANSI requirement and reference and relevant ISO material. He did consider that a comparison should be made between the NASPO and ISO glossaries.

DB: Need to focus on the purpose (or scope) of the update. The NNSC needs to identify risks that have changed and any new risks that should be covered. Document the connection with ISO and make a long term effort on the international work.

GDW agreed that the priority is to address changes/missed risks and he would work with TUV to put words around these omissions.

DB had four areas of work for NNSC – 1) identify risks missed, 2) identify any risk changes, 3) “tweak” the language and 4) capture and document standards where there is potential overlap

DB requested that the three groups (producer, user, general interest) and interested individuals identify any risks they consider the Standard has missed.

GDW noted that as an example the NASPO standard touches on disaster recovery or business continuity for which there is an ISO standard. ANSI likes to see reference to other existing standards.

AG commented that that particular standard is actually a British standard, possibly only a draft.

GDW noted that the NASPO standard is not always specific or detailed enough. He considered that the best guidelines are by TAPA for Freight Security Requirements Standards. However, DB

acknowledged that the TAPA standard is a private standard not controlled by an ANSI-like or ISO-like organization. TAPA would have to agree to being referenced.

DB made an Action item that NASPO formally ask TAPA whether NASPO can reference or include the relevant TAPA material in the NASPO standard.

GDW stated that the freight Security requirements are on the member page of the TAPA website and he would ask Tracey Christensen (TAPA rep. on the NNSC) for access to the member site in order to look at the freight requirements.

DB wondered whether the present standard could be updated with TAPA material with their permission, or whether TAPA could upgrade their standard. Would it go into the standard or the Interpretations for the auditors?

GDW considered that the first step was to reach consensus that this area needs strengthening.

DB asked who will give TAPA response. GDW suggested that TAPA representative should attend the next NNSC meeting

Db then asked if there were any other weaknesses (in the NASPO standard)

GDW stated that using feedback from NASPO audits one item was that the NASPO standard assumes that an organization has a Security Manager who knows risks & vulnerabilities & how to deal with them. However, the standard is being used not only by seasoned security companies, but also by newcomers who may be using it as a checklist and may not actually have a Security Manager at this point. The updated Standard could detail the need for security management. Alternatively, there are several other standards NASPO could reference in ISO 28000 & 27000 series

DB questioned what to do.

GDW proposed leaving as is, assume security management. Not specify qualifications of security manager, experience, training etc. Could reference appropriate ISO standard

AG – Generic risk management is in ISO 31000 and detailed to specific areas such as in 27000 and 28000

DB mentioned how the NASPO standard is not a “how to do it” instruction book so references would be good.

KK proposed that reference be made to core competences, not titles or degrees.

AG said that specific role of SM is more detailed in 27000 – it states what risk management should be able to deliver.

DB is this giving enough direction to those who will be doing the detailing?

DB Important to remember that NASPO gives the What, not the How. He proposed that this gap be closed before the next meeting.

GDW agreed, it needs the committee to review

DB asked about any major “tweaks” coming from the auditing experience.

GDW noted that he has taken the worksheet and looked at the flaws & listed possible upgrades.

DB asked that this be circulated to those who have not yet received it and that it be an Agenda item at the next meeting. Then there can be a vote on the edits and at least the easy ones be eliminated at the meeting.

AG commented that looking at the information Security section for scrapping digital media, the requirements to eliminate data on archive media being scrapped is listed as an Enhancement implies nice to have, but not necessary. The requirement should be changed to Mandatory.

GDW admitted that there has been some criticism of this and it should be Mandatory, especially for Class I & II.

DB this will require a formal ballot and voting.

DB asked if it was possible to vote now, but GDW stated that everyone should put comments on the Worksheet.

DB asked if everyone had the Worksheet? GDW to circulate to those in need.

GDW also proposed circulating the Worksheet on a rolling basis as items get resolved. He will create a Master Worksheet of Issues and Recommendations so that they can be voted on as they are dealt with. He reminded everyone that this review need good records and traceability as ANSI itself will audit NASPO for compliance with procedures.

GDW commented that the process of review was only just getting going, and some groups were more advanced than others. There is a lot of interest in participation. i.e. at the IDSP meeting ANSI announced that NASPO was going through the review and there was a lot of interest in it. Hopefully it will not get too difficult to handle.

DB ANSI needs to know that the review is underway.

There needs to be a working plan.

Discussion ended with a decision to have telecons every three weeks, usually on a Thursday (other than Thanksgiving)

EG asked about the possibility of working with Microsoft Calendar. DB thought there may be some problems with firewalls so he proposed to try the system. He agreed it would be efficient if possible to do.

GDW proposed a "sign off" meeting to take a final formal vote before moving to the public review. He would like to aim for December/January.

Discussion came to an agreement that there should be a face-to-face meeting of the NNSC after the Board meeting of the next series of NASPO meetings which will be held in Dallas in December. This means the NNSC will physically meet in the afternoon of Thursday December 13 in Dallas (exact location to be confirmed as soon as hotel contracts are finalized)

Teleconference adjourned.

## **ACTIONS**

AG to send copy of ISO 31000 to DB

GDW to send Worksheet to any person without a copy.

DB to formally approach TAPA re: use or reference to their standard

ABW to confirm location details for Dallas meeting

GDW to produce Master Worksheet

**Teleconference details** – reminders will be sent out prior to each call:

Topic: NASPO Standard Update  
Date: **Thursday, October 18, 2007**  
Time: 10:00 AM US Pacific Time  
Duration: 2 Hours  
Chairperson: David A BROWN  
Dial in # 916-356-2663  
Bridge: 5  
Passcode: 4624993

Topic: NASPO Standard Update  
Date: **Thursday, November 08, 2007**  
Time: 10:00 AM US Pacific Time  
Duration: 2 Hours  
Chairperson: David A BROWN  
Dial in # 916-356-2663  
Bridge: 2  
Passcode: 4180676

Topic: NASPO Standard Update  
Date: **Thursday, November 29, 2007**  
Time: 10:00 AM US Pacific Time  
Duration: 2 Hours  
Chairperson: David A BROWN  
Dial in # 916-356-2663  
Bridge: 1  
Passcode: 9662494

Topic: NASPO Standard Update  
Date: **Thursday, December 20, 2007**  
Time: 10:00 AM US Pacific Time  
Duration: 2 Hours  
Chairperson: David A BROWN  
Dial in # 916-356-2663  
Bridge: 5  
Passcode: 1887727