



**NASPO**

NORTH AMERICAN SECURITY PRODUCTS ORGANIZATION

**NNSC**  
**NASPO NATIONAL**  
**STANDARDS**  
**COMMITTEE**

---

## **Minutes of Teleconference**

**On January 24, 2008**

Chaired by David Brown, Intel (DB)

Attendees:

Chuck Hardester (CH), Bob Addlesberger, Gemalto (BA), Mike O'Neil, NASPO Exec. Dir. (MON), Graham Whitehead, Greenleaf Consulting (GDW), Jim Shaffer, (JS), Erc Geiger, Brady Corporation (EG), Win Baylies SEMI (WB)

Reference Document : NNSC\_Master\_Worksheet\_18Jan08.pdf

DB Noted that discussion would be based on the January 18 version of the Reference Document which was 34 pages long. The document is a summary of every change or new proposal received up to a week ago plus additional input from Sekuworks and an attachment from NIST. Ongoing comments had been summarized. There were still some sections for disposition. He estimated that from work to date about 60% of proposed changes will receive consensus and 40% still need more in-depth consideration. He stated that he and GDW had had discussions since the last telecon and had reached agreement on many of the items that they considered did not need debate (i.e. wordsmithing, reorganizing, removing duplication), but if anyone did not agree with their disposition they should come forward and the item will be disposed off by the group.

DB then asked MON to cover the Anti-trust policy. MON did this, referencing the need to leave a meeting if after bringing the matter to the attention of the Chairman their ant-trust concerns were not dealt with. DB requested that as this was a teleconference, if anyone did leave for such concerns they announce their name so that others were aware of who was concerned.

It was noted that item 2 on the agenda, the deadline date had passed, but this was a target date. GDW proposed a new target date of mid to late April, taking into account the ANSI requirement for a public review period. This seemed a reasonable target . There would be a verbal consensus, then a formal letter ballot. Next the document would have a final update and BSR9 would be issued to take the document for public review and all responses and queries must then be evaluated and a response given. The final document could then be presented to ANSI.

Agenda Item 3. Decision to look at end of document first and discuss the proposal for a new section relating to Security Risk Assessment. This would be a totally new addition.

GDW had circulated material from Jim Shaffer on risk management. It included references to 2 NIST standards. He commented that ANSI encourages use of references to existing standards. Both standards are publicly available. They are general guidelines on what risk assessment means and how to do it. NIST and ISO 17999 and 27001 are good references. GDW checked whether anyone had not received the material, which was sent out on January 22.

4 or 5 new requirements i.e. requirements A to E at the end of the Worksheet were addressed. The purpose of A is to reduce the risk of poor security management. Item A is what might be considered as a for requirement of security management?

DB questioned whether there was any dispute that Security Managers have some level of competence. As it was not disputed then there was the need for a definition that is measurable. At times the qualification was gained through experience etc. rather than academic qualifications. If you were a company looking to fill this role, would this be enough? DB referenced having sent out links to SEMI directives. WB noted that the SEMI documents are coded – yellow is how to use and blue documents are those presently out for comment. WB explained that SEMI recognized the need for security risk management standards, not necessarily a qualification.

BA stated that he felt less comfortable with the requirement defined in the document. He thought that many companies started with a QA manager and added security as a responsibility. The person may have lots of experience in security, but no academic qualification.

There followed a significant amount of discussion which concluded that the requirement should be for a security management program. This would be easier to measure than a specific human requirement. GDW noted that the objectives on Page 34 actually use the terminology of management rather than manager. The requirement should get more rigorous as the classes of certification rises. GDW commented that B,C,D, are all requirements placed on security management – identify & analyze threats, vulnerabilities and risks, assess risks and show actions to mitigate.

BA considered there were two requirements – one is the designated security responsibility and the other is for the audit to be of the work product rather than the security manager per se.

Looking at Risk Management Performance, GDW will reword this section. As this was a concern raised by Kevin Kaporch (GPO) he would also check whether this direction was agreeable with KK.

Moving on, GDW commented that B,C, and D were included in the pre-Audit deliverables at the present time. Companies that have been audited to date have

already met this requirement although it has not been set in the requirements in the standard.

DB noted that all this Security Risk Management would constitute a new Section – Section 9. The definition would be measurable.

By error there are two B items, so they were referred to in this discussion as B1 and B2. Both these should have ongoing risk management assessment, which would allow for ‘whistle blowing’. It was suggested that the language should be made more aggressive. DB proposed that the language should reference Class I requirement as being ongoing whereas Class III may not be so frequent. GDW asked the question of JS as to whether this is spelled out in NIST standards such that NASPO could reference them and therefore follow the practices and procedures.

JS responded that the language does not dictate the frequency, but does say ‘ongoing’. Need to gauge the value of the ‘crown jewels’. The timing could be left open, or NASPO standard could specify a frequency timing.

BA considered this may end up as a matrix to cover class, risk levels and management responsibilities

GDW noted that these would be added as new requirements. DB proposed that they should be designated as 9-1, 9-2, 9-3 etc.

GDW also proposed that any references to items of Security Risk Management from Sections 1 through 8 be moved to Section 9.

DB asked if the group were comfortable with a Section 9 and Risk Management rather than Manager? All agreed to the change.

GDW commented that point D had been dismissed after consideration. Arose from question of companies receiving same class when they had been measured against differing criteria – mainly when a security company had a product that was not tangible i.e. a software product. Decide that no change was necessary as the requirement was met by being Not Applicable.

Looking at E it was noted that this was a topic brought forward by observation of Lew Kontnik. Unusual for a standard to reference auditing. There was already an action on this point - to reread narrative and check for audit impact requirement. This has been done and no cause for modification of requirement was found. Had anyone else done this review? Could change wording of definition, but it is acceptable to have ‘teachy stuff’ in the document.

DB noted that the point had been considered and there would be no changes unless other comments were received – No comments, therefore leave as is.

DB noted that items A-F were now closed.

GDW commented that the last page of the review document was important. Explains how statements of risk management are different, how they provide a means by which an organization and auditor can judge how risk management is being performed. A list of criteria rather than a statement of objective. He

requested that this be critiqued. DB proposed that this be added to the list for discussion at the teleconference in two weeks time (Feb.7)

GDW offered to list changes that have already been agreed to prior to the next meeting so that they could be approved.

DB explained that section 4-A and 5-I are new.

GDW gave a brief background that it was considered that transportation should be added to the requirements. Issue was how. Best know is TAPA Freight Security Standards, but TAPA is private and therefore standard cannot formally be referenced or noted. Can it be noted that the standard is available for purchase? Anyone know of any other standard that could be used/referenced? DB explained that referencing a private standard breaks ANSI rules, however, GDW questioned whether it would be acceptable to reference them as guidelines.

DB questioned whether if any company purchased the TAPA standard to use in their NASPO audit, TAPA could get confirmation from NASPO that it was a legitimate request. GDW considered that maybe NASPO should have a copy of the TAPA standard to make available to those seeking NASPO certification.

EG questioned whether TAPA would be willing to work with NASPO on this? DB thought there was business interest in such cooperation. He also asked MON whether the discussion was moving into 'questionable' territory and was advised that there was a need to be careful.

GDW considered that the reference would only be in the Interpretations, not in the Standard. There would not be a requirement for companies to be TAPA certified, just adopting some of their practices and procedures.

CH questioned why this item would not be an M for class III? DB stated that in class III it was thought that the scope of damage would be within a specific contained item. He explained his view of Class I-III re: transport.

Mon commented that ISO 28000 Supply Chain Security Standard states the need to have secure supply chain practices in place. He also referenced the Supply Chain information and Analysis group. Which looks at supply chain security using information on Risks and attacks. The group is tied to Homeland Security. He proposed that we look at this group and what they are doing and who the members are. GDW asked that MON give the URL so that it could be circulated to the review group.

Section 4A and 4B are really the same – do not need both. Understanding from last meeting that 4C is needed.

EG commented that he had just had a situation where 4C was very important

4C will be included.

5A Anti-piggyback. This arose in the Dallas meeting. It needs discussion so was passed to the Agenda for the next meeting.

Agenda for next meeting to include:

Objective statement

Non controversial changes

5A

Group vote on items with no further discussion

Work through remaining list.

DB asked if everyone was comfortable if DB & GDW talk to KK prior to the next meeting re: update. No objection.

Actions:

GDW - issue minutes

- issue list of non contentious issues

- Write Security management requirements

MON - send URL reference to GDW (done)

DB - contact TAPA re: use of FSR standard by NASPO

DB/GDW to communicate with KK.

Next teleconference

Thursday February 7

10.00am PST

Call 916 356 2663

Bridge #1

Passcode 6195145