

NNSC Teleconference Minutes

Thursday, February 7, 2008

Chair: David Brown, Intel (DB)

Attendees: Graham Whitehead, NASPO (GDW), Kevin Kaporch, GPO (KK), Eric Geiger, Brady (EG), Chuck Hardester, NAPHIS (CH), David Elliott, Ashton Potter (DE), Mike O'Neil, NASPO (MON), Ann Whitehead, NASPO (ABW).

[Reference Document](#) : NNSC Master Worksheet dated 7 February, 2008

DB opened meeting with NASPO Anti-Trust policy. Referring to the Agenda for this meeting and minutes of the last meeting, DB asked if there were any corrections to the minutes, or questions concerning the agenda for this meeting which had been circulated at the same time.

GDW stated that he had some changes – some were typos, but in two places he had reworded the notes to clarify their meaning. i.e. p.2, 2nd paragraph should note 4 or 5 new requirements and that items A-E were addressed in the meeting.

DB asked for a motion to accept the amendments and for GDW to circulate the corrections to participants and add to the website. A motion to accept the minutes and revisions was made by DE, seconded by CH and accepted by all.

DB then referred to the Master Worksheet, specifically page 34 of 39, Sections 1-5

GDW stated that p.2 had an explanation of each section which should make block voting possible.

Section 1 contains changes to requirements that the Committee had decided should be rejected

Section 2 contains changes that the committee had agreed to accept

Section 3 were items needing further discussion (p.25)

Sections 4 & 5 were new changes (p.31 & p.34)

A formal letter ballot requires 2/3 of members to make a quorum, verbal voting only requires 1/3 (total voting membership is 15). As the group were only making verbal votes the requirement was for a minimum of 5 persons, so the group were within guidelines to be able to vote.

DB after clarifying that there were no questions or objections to the structure of the work, went to Section 1 noting that all comments submitted had been reviewed, discussed and rejected. He asked that if any item still needed further discussion it be moved out of this section and back into Section 3 for further review. No such request.

Motion to accept Section 1. No disagreements or abstentions.

Voted approval. **As a result of this vote a total of 6 proposed changes were rejected by the committee,**

Moving to p.6, Section 2. These were suggestions made that had been discussed, sometimes refined, and then agreed to. Some are only changes in wording, not meaning. Some changes are only to be added to the Interpretations.

CH asked for clarification of red and black crosses in the worksheet – these were markings used in the initial review by the User, Producer and General Interest groups to indicate items needing discussion. Crosses in the column shown with a question mark were taken to indicate that discussion either of the requirements itself, definition of mandatory/elective classification were required.

DB explained that the final version will not have the Question mark column, although GDW noted that this version would be kept on file for the ANSI audit of the NASPO Review Process.

DB asked if there were any proposed changes in Section 2 that should be moved out into Section 3 for further review.

MON asked that 1-4 be discussed. He expressed concern regarding use of the word "warrant" as this may have some legal implications and he considered that this wording should be 'softened' if possible.

KK also noted that the wording also means delegation of authority.

ABW suggested changing the wording to 'assurance'

DB asked if there was any objection to changing "warrant" to "assurance" No objections

DE asked for some clarification of 2-13, but had no objection to it.

EG noted that 2-15 was a concern raised by BA (Bob Addlesberger) as to whether false data was unethical. There was discussion about the need to sometimes be "misleading" in order to trap fraudulent activities. It was not considered unethical in terms of illegal activity.

DE thought it should be left as an Enhancement

DB suggested that it be an Enhancement with wording that encouraged the use of law enforcement knowledge. EG concurred that it was only unlawful if it was done without law enforcement knowledge.

GDW noted that there was a caution in the document.

DB proposed moving to 4-8. He noted that this item has had lots of wording changes and discussion and should be re-read

DB then moved to 5-3. He had made a note that this item was 'confusing'.

GDW said that this item had been raised by both the Producer and the User group. There was some differing views as to the requirement being made Mandatory for Class III. It is presently an Enhancement.

GDW considered that it was unlikely that a Class III would have a control room.

KK noted that if a company has one then it should be Mandatory, but agreed that not many Class III would have one.

DB said that if a company has a Control room then access must be controlled.

DE noted that there is nothing requiring any Class have a Security Control Room

DB asked that the wording be changed.

DB proposed that 5-3 be moved out of Section 2 and into Section 3.

DB then asked if there were any further concerns before accepting changes in items in Section 2.

All agreed by verbal vote. **As a result of this vote 32 proposed changes were accepted by the committee.**

DB asked that everyone move to Section 5, p.34

GDW provided some explanation. He explained that Section 5 is a "mockup" of exactly what the new Section 6.9 of the ANSI/NASPO standard would look like starting with the statement of risk management objectives on page 37, follow by the risk reduction certification criteria table and definitions to be included in Appendix A.

Two of the items in the risk reduction table, 9-5 and 9-6 had been moved from their original location where they were certification criteria 2-17 and 6-15 respectively. Continuing discussion noted that although 2-17 had moved to 9-5 there was still a need for further debate. The requirement now looked at having a single point contact. This would change to someone being designated rather than detailing competency and requiring academic credentials.

DE also proposed that 9-5 and 9-6 be flipped from an editorial view.

DB asked everyone to confirm that they were comfortable with the approved moves. It was resolved so it was noted that there was no longer a 2-17

GDW considered that 9-6/6-15 probably needs further discussion. The designation had been changed to have a single point contact for this role. It referred to the NIST standards and ISO standards which are publicly available. The emphasis was the change from Manager to Management

KK stated that he was satisfied with this change as it was the outcome that was important not the personnel. The competency would manifest itself through the documentation and the audit.

DB noted that GDW had asked for a review of the objectives. DB noted that the objectives get longer, but more tolerant, going down the Classes as the requirement for Class I level is more definite.

This would be Section 6-9.

DB asked if anyone had any further objections or concerns about what was in Section 5 of the Master Worksheet. No further comment, therefore section passed by verbal vote. **As a result of this vote a new Section 6.9 was added to the ANSI/NASPO standard with a total of 6 risk reduction requirements (4 new risk reduction requirements plus two moved from earlier sections).**

DB reminded everyone that this was only a verbal approval of what goes into the final Letter Ballot followed by full public review.

Discussion then moved back to Section 3 of the Master Worksheet, Item 2-18.

MON considered that the definition of sensitive information may be an issue.

GDW stated that there was much more detail in the Interpretations. GDW suggested that consideration be given to extending the 2-18 policy to cover the case of sensitive information being created by working remotely (outside of the fortress so to speak) of the secure facility.

MON stated that company should specify what they consider security sensitive material.

DB preferred the policy to be named as remote work policy rather than home. Based on DB concern that the title was insufficient MON proposed changing the item to Remote Work Policy. GDW will change policy name.

DE noted that the company should develop the policy.

DB agreed that what a company policy should address should not be dictated.

MON considered that the Interpretation can define security sensitive information and also what is considered remote.

GDW will reword both the requirement, definition and the Interpretation.

Moving to 2-22

DB asked if it was necessary to be more prescriptive (as suggested in the wording of the Disposition) or is it just a policy issue?

MON – the present policy determines what needs to be encrypted and acceptable encryptions.

GDW noted that presently the requirement is only for security sensitive files to be encrypted for transmission. This is detailed in the Interpretations, but in the Requirement it is a blanket statement.

DE commented that this presupposes that the person receiving the file has the capability to decrypt the data. This needs to be addressed as it is not always the case.

EG noted that some companies password protect their transmissions by sending two files – the data and the password, separately. He noted that customers do respect security and accept secure file transmission as a “necessary evil”. It was noted that there may be a need for a different style of communication within a company from that of outside communication. Some encryptions could be undermined by the customers own technology (or lack thereof). DE commented that often, government customers have a hard time de-crypting. It was generally considered bad policy for suppliers to dictate encryption requirements to their customers.

Questions arose regarding whether this requirement should be E or M for which classes (not resolved)

GDW noted that the wording could be expanded in the Interpretations.

GDW agreed to change the wording to address the need for a mutually agreed procedure between the transmitting parties.

Discussion then moved to section 2-44 and 2-45, but meeting ran out of time for further discussion. Will be tabled at next meeting.

EG proposed that the next meeting be a Webinar so that everyone could see the items under review. GDW would need to be Editor.

DB reviewed the actions from the last meeting which had been tabled at the end of the minutes.

All actions had been completed other than

1. DB contact with TAPA was still ongoing
2. minutes had been circulated, but GDW to resend the corrections.

Actions from this meeting:

GDW to send corrected minutes of January 24 teleconference

GDW to reword Requirement and Interpretation of 2-18

GDW to reword Requirement and Interpretation of 2-22

GDW to clean up document to reflect number changes, new section addition etc.

GDW to circulate latest document, and comments from Sekuworks, prior to Webinar

Next teleconference meeting:

Thursday, February 21

10.00am PST

tel: 916 356 2663

bridge # 1

passcode 6850277