

NNSC Telecon  
April 8, 2005

Chaired by Jeff Turmel

Voting Attendees: Jeff Turmel, Brady (JT), Eric Schetina, Trustwave (ES), Phil Smith, Trustwave/IAFCI, (PS), Rich Carter, AAMVA (RC), Graham Whitehead, GDW Consulting (GDW))

Non Voting Attendees: Rick Ward, Appleton (RW), Dan Thaxton, Standard Register (DT), Bob Noga, Flex (BN), Mike O'Neil, Northstar (MON), Ann Whitehead, GDW Consulting (ABW)

Jeff Turmel read Antitrust Policy

Everyone acknowledged their attendance on the call and it was agreed that a meeting quorum was present.

ABW gave brief review of actions outstanding from the last meeting and their present status and noted continuing open items.

GDW explained recent conversations with personnel from the GPO and their intention to participate in the NNSC.

GDW referenced Action item 3 from last meeting which related to wording of Scope. The new wording had been circulated and responses gathered from Jeff Turmel, Louann Siebert, Dan Thaxton, Stephen Price-Francis.

JT asked about deadline for closing this item. GDW stated it to be 10 days from ballot vote – need votes from 50% for it to be valid and 75% must be in favour for change to be confirmed.

GDW to circulate final wording along with a ballot sheet to eligible voting members.

Meeting turned to Trustwave input after reviewing Version 1.0P. PS and ES asked to give an overview of their input, their comments and concerns. They had looked at NASPO Public Standards and considered the computer/information area to be a little weak. Thought that there needed to be more emphasis on best practices where it applied to critical information processes and systems.

GDW noted that the Audit process requires company to look at what information they consider to be critical. JT believed a review of “critical” to be important – he had discussed this with DB (David Brown, Intel, NNSC Chairperson, absent from this call) re: elective/mandatory status

Following Trustwave's expression of concern, one question is whether information security should be a separate audit?

DT – if measured on aspects of information security standards then it should be in the main audit. Company needs to know the rules and therefore what to prepare for.

DB/JT talked about distinctive elements. Different degrees of security are needed for products than for transactional elements.

DT – maybe it could be an addendum or a subsection

GDW – question whether it contains personal data? If it does then it should need a separate audit.

ES – there are already many security standards for personal data which are set by each industry section. Could they be used?

GDW stated that ANSI rules allow for an organization to reference other Standards within their Standards, so long as the Standard being reference is an American Standard.

JT – wants one set of standards to go to.

BN – ISO works by covering everything and referencing exceptions.

JT – that would be inclusive to the audit, but could note Not Applicable to irrelevant topics.

RC- could have optionals that include fields according to specific industries.

DT – companies have rules already set by the need to comply to customers criteria. All companies should be expected to meet a minimum standard regardless of customer requirements.

GDW – if company is handling personal data they are automatically required to meet Class 1 standards. In the case of a company like Standard register, they cover all classes as some of their facilities are Class I, some II and some III. Each needs to understand their risks and control them.

GDW – example of audits that have already taken place – look at privacy requirements that company already works to and anything not applicable is waived and noted in the final report.

JT – maybe a more integrated statement is all that is needed.

GDW noted that some of the Trustwave comments coming from Version 1.0p have already been addresses by adding definitions back in. Asked for PS concurrence that this had happened and PS agreed.

JT noted that DB had wanted Trustwave input to be topic of two meetings.

Looking at the 6 page document, some problems have already been removed.

P.3 had a recommendation of changing electives to best practices. Electives suggest the standard is too ambiguous.

ES – best practices are good to do, but not required Maybe anything needed should be required, anything else noted as best practice.

GDW – stated that in Mountain View meeting DB had expressed importance of keeping results of audit confidential. Organization needs to know what gained certification, but it should be confidential to Auditor and company and revealed only on a business customer/client relationship.

DT – concurred with GDW review of his comments.

RC – government procurement RFP's. They could specify Class I or II, but it would not show compliance with specific points as long as included only as an elective.

DT – government specs, do not allow for discretion, noted an example of companies being one class and almost eligible for higher class, but as items of electives are not reported the government would not know what specific points were the strengths of the company.

MON – During the Standard development they had looked at different risk mitigation and realized there are different issues for different companies and there need to be some flexibility to cover these differences.

ES – Auditor should have some flexibility of judgement, however, these could cause very different standards. The Auditor should make the judgement, not the company.

GDW – have changed mandatory to minimum. Government could require that minimum be met. Could also change electives to minimum. Totally unambiguous. Moving to minimum covers government RFP requirements.

RC – could have optional requirements i.e. if your company does this---you must comply with this.... Maybe some of these could be grouped together.

ES – need to reference what they are trying to get at, not the solution

GDW - Standards are supposed to be performance based. Someone needs to write out arguments and then do letter ballot for each point. The decision has to be unambiguous, compatible with procurement, like a specification requirement JT admitted that he had realized that he had made some misinterpretations of Trustwave input. Need to look at pros and cons of reasoning for structural changes to standards.

ES concurred that that was Trustwaves main purpose.

JT asked if this should be discussed line by line and by telecon, or by face-to-face meeting.

GDW commented on RC's present dilemma of his RFP having no differences in interpretation.

DT again stated the need to have the What, not the How without getting specific, so maybe things should be left as minimums for each Class.

GDW noted changing mandatory to minimum

ES considered that anything in the Standards was both mandatory and minimum

JT proposed that a small group from the NNSC work together on minimum/mandatory, minimum/electives and possible need for more rigid standard requirements and enumerate this point.

Small group of volunteers to include – JT/GDW/DT/ES/RC/MON and DB

GDW asked permission to send copy of Standards to ES in order for him to discuss the Public Standard with better understanding of NASPO Standard.

Agreed. It was agreed that all non-NASPO members of the NNSC should have the full standards with a written agreement to restricted use.

JT to draft restrictive letter and send to GDW and MON for approval.

GDW/JT to hold a de-brief with DB on April 11, 8.00amPST

Next full teleconference to be scheduled for April 29, 2005 8.00amPST to allow sub-committee to complete their work. Details of Bridge number and Passcode to be distributed later.