

Minutes of NNSC Teleconference held on April 29, 2005

Meeting Chaired by David Brown

Voting Members, David Brown (DB), George Phillips (GP), Eric Schetina (ES), Rich Carter (RC), Graham Whitehead (GDW)

Non-Voting Members, Bob Noga (BN), Dan Thaxton (DT), Mike O'Neil (MON),

DB - reminded everyone of the NASPO Anti-Trust Policy.

GDW - reviewed actions from last teleconference. Mainly wording of SCOPE, which has been completed and formation of a Sub-Committee to look into the issue of requirements ambiguity caused by the presence of "Elective" requirements in all Classes.

DB - recounted his understanding of the last Sub-Committee teleconference and his understanding of the results. Sub-Committee had looked at the effect of Elective requirements and reached consensus that :-

- to ensure that all Certificate holders satisfy the same risk management requirements, the use of "Electives" should be abandoned.
- in future, Certification should be awarded solely on the basis of meeting a set of Mandatory requirements.
- risk reduction would then be customized with voluntary (or customer suggested compliance) with a set of risk reduction "Enhancements".

Under this new requirements structure, the final Audit report will document all the Mandatory items that have been complied with for Certification and note any additional enhancements that have been met by the company.

GDW – Auditor practice relating to choice of electives (enhancements) would remain as presently used (Auditor is involved in choice). End users would be able to look at Standards knowing class holder has met all mandatory items and can request inclusion of enhancements as required by a specific RFP.

MON - raised the issue of who pays for any additional audit in event of company needing extra certification regarding additional enhancements. DB preferred to bring that to the general NASPO membership for discussion, not the NNSC.

RC - stated that he was happy with firming up the requirements for certification – which was agreed by all present.

DB - thought that both SCOPE and MANDATORY changes to wording were ready for letter vote.

GDW - said the letter ballot was ready to go. Because the NNSC cannot change the NASPO Standards, after the NNSC letter ballot, the recommendations of the NNSC must go to the NASPO Standards Committee for the concurrence of that Committee and their review of whether or not any of the requirements currently shown as "Elective" should become Mandatory.

GDW - reminded everyone that when they receive the letter ballot they are expected to either affirm the proposal, abstain or reject with an explanation – a plain reject is not counted.

DB - then turned the committees attention to the Trustwave input regarding IT, noting that the new structure would make it easier to add tighter IT requirements. He asked if every Class I vendor is handling personal data.

RC - thought not, therefore it could be an enhancement. As a user he would only require it if it was needed. There are two levels of IT :-

- a basic level that all modern computer aided operations should use and
- a higher level for those operations that handle financial transactions or personal data files etc.

DB - Trustwave recommendations had 2 parts – minimum protocols, and a 2nd area where privacy issues would require extra mandatory certification.

ES - Confirmed that the need for extra certification would only be necessary if there was critical information involved. ES stressed that the information must be of a critical nature.

RC – different business processes need different protections

Considerable discussion followed with input from DT, DB, ES and GDW

RC - issue is not necessarily whether the system itself is secure, but whether critical data is secure. This could be in a number of categories i.e. if data is on paper then the company must meet this set of criteria, if data is on a wireless system, then this criteria must be met.

DT – asked whether all critical data should be covered?

RC – mainly looking at Class I but really should be looked at in all Classes.

GDW – Audit covers 3 operating characteristics – looks at an operations vulnerability to attack, how critical the data is that is under It control and therefore what risks must be controlled. The company is still going to have to meet a set of ‘black and white’ requirements, but the audit also looks at specific company needs.

DT – what happens in the case of some accounts needing high security and others not needing such high standards?

GDW – if there is no risk the auditor can asses as such, but if certification is to a lower class, but there is a specific high risk then the auditor will require the company to meet a higher level of control for that specific risk.

DT – is comfortable with that.

GDW – that still only shows the What, not the How.

DB – in reality, are the IT risks any different from any other form of risk. All concerns must be met in the requirements.

GDW – Important to ensure that Standards committee has a checklist which covers all the needs. Must ensure that nothing is left off the list. Mandatory or Enhancement is the secondary issue.

ES – are there any IT requirements presently being missed, any basic needs, especially in regards to personal data? Some personal data is going to be covered by other requirements, such as Sarbanes-Oxley and other already dictated standards.

GDW – considered that however personal data security was being handled it must be a Mandatory requirement and the Auditor could then assess the applicability of the techniques being utilized. If the Standards committee are

agreeable to this there could then be a set of basic protections that should be covered such as firewalls and IT intrusion detection, and the company audit refined accordingly.

ES – put all IT in one section and then disseminate down all the options of coverage.

RC – some concerns about privacy. If a company is handling privacy material then it is Class I, but if it is not applicable the company is still Class I and could respond to a RFP with Class I requirement, even though they actually do not have privacy handling capability.

BN – ISO covers this by having a Certificate that lists both Scope and Exclusions.

GDW – NASPO presently only reveals certification, not even Class, but it would be possible to issue a certificate that lists exclusions (if any).

GDW – if an end user of the Standards requires that specific types of data (such as personal data) are handled in a special way, the end user must either check that the special treatment is included as a Mandatory requirement or call it out as an “Enhancement” (assuming that it exists in the list of possible “Enhancements”).

ES – there is always the possibility of a company adding something just to get certification, but then removing it after having been Certified.

GDW – that is possible, but as there is an annual audit this is unlikely.

DB – discrepancy will usually fall out as you go through the selection process at the beginning of the audit, especially a re-audit.

GDW – prefer Auditors be “damned if they do” rather than damned if they don’t and have items in the mandatory list. An enhancement could be overlooked by both the customer and the auditor.

RC – can be done either way as long as it is clear.

DB – asked how NNSC handles strengthening of the IT requirements

GDW – give the requirement to the NASPO Standards committee and ask them to look into basic IT requirements and whether they need strengthening, whether they should be enhancements or mandatory and ask them to specifically look at IT as it relates to personal data.

RC – agrees

DB asked if all present were agreeable to this – No objections raised.

ACTION – GDW to put the request for the NASPO Standards Committee in writing.

GDW asked if ES would review Trustwave’s original IT concerns and list a basic set of IT requirements that they consider should be in each Class.

ACTION - ES thought he could have that completed within 10 days.

DB – asked about the objectives of the NNSC for the June 16 meeting?

GDW – that is somewhat dependent on the Standards committee. He is aware that the NASPO Standards Committee chaired by Jeff Turmel, would like to complete their actions by June 16.

GDW stated that there is now a need for a new version of the Public Standard

ACTION – GDW undertook to have Version 2.0P sent out by May 6th Version 2.0P will help JT’s committee

Version 2.0P should be ready for approval at the NASPO Board meeting on June 17th.

DB – The objective for the NNSC for the June 16 meeting will be to vote on releasing Version 2.0P for public review.

GDW – the vote will require a quorum. Already know from number of NNSC members who plan to attend the meeting at Sekuworks that a quorum will be present.

ACTIONS from the teleconference:

- GDW to put the request for the NASPO Standards Committee in writing.
- ES to review Trustwave's original IT concerns and recommend a basic set of IT requirements that they consider should be in each Class. To be completed within 10 days.
- GDW to create a draft of v 2.0P by May 6, 2005