

NASPO National Standards Committee  
Minutes of the NNSC Teleconference of May 13, 2005

Callers

David Brown (Chairman) (DB)  
Eric Schetina (ES)  
Dan Thaxton (DT)  
Mike O'Neil (MON)  
Phil Smith (PS)  
Rich Carter (RC)  
Graham Whitehead (GDW)  
Ann Whitehead

DB opened with a review of the NASPO Anti-Trust policy

DB Purpose of the meeting is to review the Trustwave comments on IT. Asked ES to walk through the suggestions

ES – referred to page 3 recommendations. Suggested using the basic NASPO standards and then add in others as required or relevant to the company being audited. Noted that there are already hefty security best practices in place with CIPS, Mastercard, VISA standards etc. The requirements should be looked at according to the Class. He stated that the recommendations are being looked at internally at Trustwave to check they are on the right track.

GDW – noted that the Trustwave input was a good piece of work. It is not actually the work for NNSC to write the standards – it should go as a recommendation to the NASPO Standards committee for formal review.

DB – in effect, NNSC is the firewall, it could be looked at by anyone. What is not included in the Standards can still go into the Audit, again the what not the how.

ES – considered that the details will come out as it is looked at by the group.

GDW – some wording at the “high level” should be added into the narrative He noted that so far, all the NASPO companies audited have had an IT person, but that will probably not be the case as smaller companies get audited.

Suggested inclusion of one, or two, separate sections relating to IT security systems. The European standards refer to it as ‘Computer Security’

DB – Actual requirement will be added to the Standards. Audit process/practice will be looking at adding detail to the requirement.

DB – Should look at items to be recommended to the Standards committee.

There are several distinguishable items that can be added to the matrix. i.e. Create a secure network (p.5) Require a firewall – different levels for different classes

ES – First need to be comfortable with the higher level and then work the details downwards.

DB – As a user the risk is the supply to the company. A significant risk to accompany is someone attacking their vendor and therefore interrupting their supply. Data needs to be secure from any malicious attack.

GDW – there is a difference between having an IT person and actually putting security requirements into practice.

DB – Look at headings first. Create a secure network – make this the objective

ES – have a heading with the requirement underneath

DB – Information Security Policy – a heading

GDW – that is presently in, but not broken down

DB – Firewall and Rule Set. Is this a requirement? Presently not in as an explicit requirement

RC – one of his concerns is that it depends upon the network – could be just internal

ES – firewall only relates to internet access

DT – not so, could be an internal network but still need internal firewalls

ES – if data is not critical then it is not applicable

RC – there should be a statement of need for firewalls

DT – then we are dictating language – this is ‘how’ not ‘what’

DB – then make a Requirement for a Strategy/Method that protects against unauthorized access

ES – firewalls and anti-virus are usually in standards requirements. Require appropriate controls would blanket all needs.

DB – that means the firewall is not a Standards requirement but it is an auditing requirement.

RC – has some concern that the general mindset of people assumes the world is attached to the internet.

ES – all things can be stated as “not applicable”

GDW – necessary to make clear in the narrative what the auditor expects regarding firewalls, anti-virus etc. As a minimum the statement could be conditional if you have this then you need this, if you have that then you need that.

GDW – proposed that information Risk Management be treated the same as Materials with no need to secure openly accessible information. Considered the Trustwave work was “bang on” and it now needs to be translated into NASPO narrative and requirements. Companies need to do whatever it takes to protect critical data only. The ‘How’ will still be between the company and the auditor.

DB – move to look at Secure All Wireless networks. If there are non, then they are all secure. Is there any issue when they do not have them? No.

ES – Anti-Virus covers scans, patches and security

DB – Access Control. Is that physical or virtual? i.e. even in Intel he cannot get into the data center physically, but can get in virtually with passwords.

DB – Monitoring – really breach detection strategy

Need to translate wording into NASPO formats. There are three forms – Goals, Narrative and Tables

ACTION – GDW to translate ES work into NASPO format. Important that the suggestions made do not get diluted in the creation of the Narrative or details of the tables

DB – can this be done within 3 weeks?

GDW thought Yes. He will work with Jeff Turmel and Eric Schetina and bring recommendations to NNSC which will then take recommendations to the NASPO Standards Committee

DB - continue with Agenda – next item is the update on the Letter Ballot

GDW – Reminded all that no major changes can be made without 50% of committee members returning ballots – already have 50% returned. 75% of returns need to be affirmative. Already have that too. Technically can go forward, although 30 days can be allowed. As there is already enough concurrence to move forward, NNSC will request final input by mid week and then go forward with the recommendations to the NASPO Standards Committee

DB – Looks like formally submitting Version 2.0 will be able to go forward on schedule.

GDW – item 4 Version 2. He omitted a reference to George Phillips Chain of Custody concerns.

DT – 5.4.12 relates to that. Any others?

GDW – Yes, possibly 3 references. There is another in 4.15 and Definitions 4.15. He will send an e-mail to everyone on this. GDW noted that there had been some concern expressed about this matter and whether it is a restriction of trade in some jurisdictions. May need to be modified or include a warning re: not being applicable in some jurisdictions.

MON – could say strongly encourage, but may not be stated as a requirement.

GDW – agreed that wording could be softened. Presently only NNSC members have a copy of Version 2. Version 2 and the changes need to be considered by the NASPO Standards committee. Will JT have any conflict of interest between his role on the two committees? Probably not.

ACTIONS from the teleconference:

- GDW to write Trustwave work into NASPO Goals, Narrative and Tables.
- GDW to work with ES and JT on wording
- GDW to send e-mail relating to omissions of Chain of Custody in Version 2.0 and soften the wording concerning the requirement for Chain of Custody Agreements.
- GDW to request final ballot input by mid-week
- ABW to circulate minutes.

Next teleconference to be held on Friday June3, 2005 at 10.00am PST

Tel 916 356 2663

Bridge # 3

Passcode 5248304