

NASPO National Standards Committee
Minutes of Meeting held on February 24, 2005
At LaserCard, Mountain View, CA

Attended by: David Brown (DB) Intel, Ken Branch (KB), George Phillips (GP) ProDocument Solutions, Mike O'Neil (MON) Northstar, Reha Emden (RE) John Henry, Robert Sherwood (RS) Sekuworks, Bob Jochan (BJ) Keller Crescent, Graham Whitehead (GDW) NASPO, Dan Thaxton (DT) Standard Register, Mark Waterbury (MW) Stardust Technologies, Rick Ward (RW) Appleton, Ann Whitehead (ABW) NASPO

Chairman: David Brown

The meeting Agenda is included at the end of the Minutes.

Meeting opened with welcome from DB and the reading of the Anti-Trust policy by MON.

- All attendees introduced themselves, their company and their interest in NASPO.
- DB gave an overview of the purpose of the NASPO National Standards Committee, describing the classifications making up the committee and the official members of the committee.
- GDW gave an overview of where in the process the NNSC is at the present time and explained the difference between the Public Standards (presently version 1.0P) and the private standards of NASPO v.4.0 to which companies are audited. Written comments on v 1.0P have been provided by Phil Smith and Erik Schetina of Trustwave and Lew Kontnik of Amgen. Copies of their input have now been distributed to all NASPO and NNSC members.
- JT provided verbal comment on v 1.0P by stating his concern (referenced later in the Minutes) about the validity of Certificates already issued if some of the Elective requirements are upgraded to Mandatory as Trustwave have suggested. JT concurred with Lew Kontnik that the scope (or applicability) of the Standards to end users must be defined.
- GP presented his written input at the meeting to address his concern over Distributors and Re-Marketers in the downstream part of the supply chain. Copies of GP's input were distributed to all attendees and will be forwarded to NNSC members who were not present.
- GDW requested permission to release the formal NNSC Roster to ANSI.

ACTION:GDW to request permission from those not in attendance before forwarding the names to ANSI.

- DB described the "forming, norming, storming and performing" approach to the project and considered that the NNSC was almost out of forming and into storming. He stressed the importance of understanding the consensus process and the meaning of all the requirements in v 1.0P.
- DB reported the first issue – received by Lew Kontnik of Amgen (item 4 in the minutes of the teleconference of February 11, 2005) which related to the standards applicability to end users.
- JT commented that this is not clear in Section 3.
- in the ensuing discussion it was noted that
 - Standards are voluntary, not dictated
 - Enforcement to producers, not users can be foreseen
 - Users see value in certifying producers
 - The chain of supply needs to be followed in both directions for security
 - NASPO standards could be used to cover Sarbanes-Oxley requirements
- It was acknowledged that Lew Kontnik's observation had raised the question of scope and attendees agreed there is a gap. Further discussion on Lew's point was deferred until he is able to more actively participate in the matter.

ACTION: to consider wording and clarification of Section 3.0

- Question of how close to a submittable document was the process at this time?
- DB expressed his concern that the public document not give too much detail to the “crooks”
- RS stated that the wording needs to be vague enough not to raise alarms to those considering the standards, but strong enough to deter “the bad guys” A fine line!
- MON advised that some definitions should be taken out.
- DT addressed the use of electives, pointing out that the “public” will not know exactly what gained an organization their certification. All that will be known is that they met the minimum requirements of the class. The same point was made by Trustwave in their review.
- MON stated that companies still need to supply security above the mandated levels.
- A lengthy discussion ensued. The following points emerged.
 - use of electives conceals the use of some infrastructure, systems, procedures, etc.
 - there is more certainty in Class I and II because there are fewer elective requirements in those classes, especially in Class I
 - knowledge of the “Elective” requirements that were used to gain Certification is confidential to the NASPO Auditor(s) and the Certified organization.
 - The Audit results (and therefore the exact basis of certification) are treated as high security information in accordance with NASPO Auditing Standards.
 - NASPO will never release Audit results to a third party unless “forced” to do so by Judicial subpoena.
 - Disclosure of audits is totally under the control of the Certificate holder. For example, it is within the power of decision and action of the Certificate holder to disclose the results (hopefully under a NDA) of the Audit to any third party who has a need to know.
 - It is a NASPO policy to disclose only that an organization has been awarded a Certificate. NASPO does not disclose the Class of the Certificate.
 - There was strong consensus within the meeting that it is the results of the Audit (and the identity of the Auditor) that require the most protection because they help the “bad guys” to identify potential “weakness in the armor”
- Also noted was that for ANSI, if a requirement is not explicit or is ambiguous then it is not part of the standard. ANSI acknowledges that this is a security standard and therefore the document cannot reveal all requirements, but it must show the “What” if not the “How”
- Suggestion that a protocol for controlling confidential material could be included in the public document

ACTION: get input from all members on suggestion of including a protocol for controlling confidential material

- KB indicated that standards should continue to be improved to continue to deter the “bad guys.” Adjust the standards as the circumstances change.
- Reference was made to EMV standards for Mastercard and Visa etc.
- JT did a brief data mine for these standards, and discovered, to most attendees surprise, that they are available over the internet.
- DB noted that what the “bad guys” really want are the audit results. Audit results should be securely held as the process is not the target, the audit result is.
- Suggestion that words should be added to the public document re: confidentiality of audit results.
- If the private standard becomes the public standards the definitions could be put back, but not the evaluations. What would it look like?

ACTION: NASPO secretariat to add the definitions to the document and circulate to NNSC members for comment.

Break

Review of Actions:

1. Reword the scope in Section 3.0 to address applicability to end users etc.
2. Include the definitions, but not the numerical system.

3. Determine if any Electives (as Trustwave have suggested) should be raised to Mandatory requirements

- MON explained how mandatory came about and how electives were added.
- GDW suggested that there is a need to retain the requirements identified as Electives (either as Mandatory or Elective requirements) in order to avoid lowering the NASPO Standard and making it easy to gain Certification by spending money on a few items of infrastructure and some security systems.
- Can the NASPO Certificate and Audit Report documents be made secure documents? Yes, use security paper etc. NASPO could issue a standard for the security of it's own documentation.

Phil Smith (Trustwave and IAFCI) was brought into the meeting by telephone.

His concern is with security of data transfer. His comments included

- Clarification of definitions. PS will also check with 2 other persons for their input.
- Electives – important as 2 different companies could qualify with different electives, depending on best practices. This is similar to government ranking process.
- Need to look at security breaches via internet/ computers.

Conversation with Phil Smith was kept short as PS was unwell. Consideration of Trustwave's detailed recommendations, particularly those related to IT security were deferred pending Phil's recovery from the Flu.

- GP expressed concern that the supply chain both up and down be examined, including selling through agents.
- GDW thought that public standard could be used both up and downstream and that a new area of risk (No.9) could be considered if the type of risk uncovered by GP warranted separate coverage. Attendees appeared to agree that the specific risk identified by GP should be controlled with the addition of a new requirement in the Supply Chain Risk Area – there being no need for a 9th risk area.
- Customer risk covers supply chain, but the customer related risk management may need more detailing.
- As well, add a subsection in Section 5.4.5 that specifically addresses distributors, brokers and remarketers. Require a custodial agreement.
- Additional comments were that changing electives to mandatory was of concern to existing Certificate holders because the change would invalidate certificates already issued.
- Nature of the company indicates the information requirements, so the credits would vary, which is the purpose of the electives.
- The auditor can make judgments of class and suggest appropriate electives.
- The company is given a time period to implement new requirements – this is a directive for NASPO to address, not NNSC.

ACTION – All members of the committee to submit negative comments, in writing to DB and GDW by March 11, 2005

All members to look at input from Trustwave (IAFCI)

Next Meeting will be by teleconference on **Friday March 18, 2005 at 8.00am PST**. Courtesy of Intel

Telephone number (916) 365 2663
Bridge # 3
Passcode 6808697

ACTIONS

- GDW to request permission from those not in attendance before forwarding the names and affiliations of NNSC members to ANSI.
- to consider wording and clarification of Section 3.0
- get input from all members on suggestion of including a protocol for controlling confidential material
- words should be added to the public document re: confidentiality of audit results.
- add the definitions to the document and circulate to NNSC members for comment
- Add a subsection on chain of custody including remarketers.
- Add a requirement (to the “downstream” part of the Supply Chain Risk Area) for Providers to enter into a “Custody Agreement” with Distributors and Remarketers. The Custody Agreement must include a requirement on the part of the Distributors and remarketers to seek prior approval from the Provider to supply the product to the end user, who must be identified.
- Put in a narrative at the beginning (section 5.4.5) re: custodial agreement
- All members to look at input from Trustwave (IAFCI)
- **ALL MEMBERS OF THE COMMITTEE TO SUBMIT THEIR COMMENTS TO DB AND GDW BY MARCH 11, 2005 FOR DISCUSSION AT THE MARCH 18 TELECON. NEGATIVE COMMENTS MUST BE IN WRITING GIVING REASONS FOR REJECTION AND SUGGESTIONS FOR CORRECTION.**

END OF MINUTES

AGENDA

8:00 **NASPO National Standards Committee Workshop Meeting.**

David A. Brown - Chairman

Welcome and Anti Trust Statement

Introduction of Members & Status of Committee Membership

Review of the Committee based consensus process

Review of the Draft Standards Definition Document v.1.0P

Disposition of comments and recommendations for change

Review and update of the Committee timetable

Date of next meeting & teleconference

Any other business

12:00 Adjourn