



NASPO

NORTH AMERICAN SECURITY PRODUCTS ORGANIZATION

**NNSC
NASPO NATIONAL
STANDARDS
COMMITTEE**

Report & Recommendations of the NNSC Sub-Committee Formed to Examine the Pros and Cons of Continued Use of Requirement Electives in the NASPO Security Assurance Standard v 1.0P dated March 15, 2005.

Summary

An NNSC subcommittee was formed to examine the allegation that the proposed NASPO Security Assurance Standard contained ambiguous requirements. The subcommittee confirmed the allegation that ambiguity exists in the proposed standard and developed a recommendation that NASPO Certifications be issued on specific explicitly listed mandatory requirements that DO NOT include any electives or options.

However, recognizing that each application of a security technology is likely to face specific and unique threats that the base "class" NASPO Certification does not address, NASPO Certification audits shall also document conformance to any "enhancements" beyond the mandatory requirements for the NASPO class in the final Certification Report. In other words, the final report documents certification to set of specific base or CLASS requirements PLUS a list of any ENHANCEMENTS. "Class + Enhancements"

There will be no ambiguity in the requirement for any specific NASPO class, which is the basis for auditing to issue a certification report. Enhancements allow vendors to specialize and using NASPO audits to document these enhancements, provides a method for vendors to compete for business based on investments made to improve security. Enhancements also allow customers of security technologies to focus vendors on risks specific to the customer's application without wasting resources reducing risks that simply don't apply.

Subcommittee Contributors :-

User Group

David Brown, Intel Corp., Santa Clara, CA (<http://www.intel.com/>)

Rich Carter, AAMVA, Arlington, VA, (<http://www.aamva.org/>)

Producer Group

Jeff Turmel

General Interest Group

Phil Smith/Erik Schetina, Trustwave Inc. Annapolis, MD/New York (<http://www.trustwave.com/>)

Graham Whitehead, NASPO, Vancouver, BC (<http://www.naspo.info/>)

Non NNSC Committee Attendees

Dan Thaxton, Standard Register, Dayton, OH (<http://www.standardregister.com/>)

Mike O'Neil

NASPO Administrator

Ann Whitehead

Problem

In their review of NASPO Security Assurance Standard v 1.0P dated November 16, 2004, Phil Smith & Erik Schetina of Trustwave Inc. highlighted the existence of some ambiguity in the basis of NASPO Certification. Their recommendation 2.1 described the problem as follows :-

2.1 Electives vs. Best-Practices

The concept of issuing both Mandatory and Elective requirements is similar to other standards bodies which issue Mandatory requirements, as well as Best-Practices. Requiring a certain number of Electives to be implemented by a Member however may not be the optimal approach for the NASPO's standard. TrustWave believes that NASPO will find that Members at identical class levels implement different security measures making it difficult for the industry and their clients to interpret the appropriate and relevant security posture of the organization. In general, a security standard should be unambiguous with respect to requirements. Therefore, TrustWave suggests that NASPO consider determining which of the Electives should be Mandatory at the different Class levels, and then substitute the term "Best-Practice" for any "Elective" that is not Mandatory. This will align the terminology of NASPO's standard with those of other standards bodies.

The above recommendation made by Trustwave was discussed at a NNSC Teleconference held on April 8, 2005. It was agreed by attendees at that Telecon that a smaller working group of the NNSC should take a closer look at the pros and cons of the system of Mandatory & Elective requirements used in the NASPO private standard (NASPO Risk Man. Reqmts. v 4.0 dated September 24, 2003) versus a new "transparent" system where there can be no uncertainty in the risk reduction requirements satisfied by the holder of any Class of NASPO Certificate. Attendees at the April 8th Telecon agreed with Trustwave that uncertainty of this kind was undesirable especially in a competitive bidding situation where the demands placed on all bidders must be exactly the same.

Work of the Sub-Committee

The above problem was first addressed by the Sub-Committee in a telephone conference on April 14, 2005 and again on April 20, 2005. A consensus was reached by the Sub-Committee and is presented as a number of recommendations, later in this document, for consideration by the NNSC, the NASPO Standards Committee, and NASPO. Several options that resolve the problem are presented together with summary discussion for each recommendation. It is expected by the Sub-Committee that these recommendations will be brought before the NNSC for discussion and acceptance or rejection by letter ballot.

Discussion

Attendees at the Sub-Committee telephone conferences on (April 12 and 20) agreed with the April 8th consensus that :-

- a. The NASPO 'public" standard must be compatible with a competitive bid process.
- b. To be compatible with the normal rules of the competitive bid process, all bidders must be faced with meeting exactly the same set of requirements.
- c. The use of Elective requirements in the "Public" version of the NASPO Standard is therefore undesirable and must be removed to prevent the NASPO Standard from falling into disuse by procurement managers because of this ambiguity.

On the other hand, attendees at the Sub-Committee telephone conferences were unanimous in wanting to preserve the ability to “CUSTOMIZE” the NASPO Standard to the specific requirements of an end user or particular type of document, product or organization.

Options for Fixing the Problem

The following options for solving the above ambiguity problem were discussed at the telephone conferences.

1. No Change – Certify in accordance with the March 15, 2005 version of 1.0P and encourage procurement managers to specify that Bidders shall satisfy the published minimum requirements of a specific Class plus any other (non minimum) requirements that are deemed necessary by the procurement authority.

In this version of the NASPO Standard, a certificate is awarded for compliance with a published set of minimum requirements plus a set of un-published additional requirements that are revealed at the time that an application for Certification is accepted by NASPO. To meet the specified (by NASPO) additional requirements candidates for Certification can choose “what” to deliver from a number of published “Elective” requirements to make up the required number of Certification Credit Points. (FYI, The exact number of additional Certification Credit Points is presently defined only in the “Private” NASPO Standard v 4.0)

[this option implies that an existing holder of the specific Class (or higher Class) of Certificate specified by the procurement authority, will know that the organization is compliant with the possible exception of the “other” NASPO requirements that are deemed necessary by the procurement authority. These other requirements specified by the procurement authority may or may not have already been satisfied by the bidding organization in meeting the un-published additional requirements (the Electives) for Certification]

2. As in 1. except that we remove uncertainty about the scope of the “Elective” requirements by publishing (in the public standard) the number of additional Certification Credit Points that must be gained from the “Electives” in each Class and area of risk (exactly as shown in v. 4.0) to become a Certificate holder.

[please note that this option is not reverting to v 4.0 - it transfers from v 4.0 to v 1.0P only the quantification system for Electives specified in v 4.0. This preserves the “performance based” method of specification used in v 1.0P which avoids specifying HOW requirements are to be satisfied.]

3. As in 1. above but use the word Mandatory in place of Minimum.
4. Issue Certificates solely on the basis of compliance with a set of published Mandatory Requirements for each Class. Requirements that are not mandatory would remain specified in this version of the Standards Definition document to be used by Procurement Authorities and Corporations as bid specific additional requirements.

This option has the advantage that all Certificate holders will have gained their NASPO Certificate on the basis of complying with exactly the same set of published requirements.

[Switching to this option implies that the NASPO Standards Committee will need to review all of the requirements in each Class that are shown as “Elective” to determine if any or all of them should be upgraded to become Mandatory]

Conclusions

All of the options cited above remove ambiguity in the specification of Security Assurance requirements from the competitive bidding process. In the case of Options 1,2 & 3 however there can remain a considerable difference between what it will take to satisfy the bid requirement compared to gaining a NASPO Certificate. The difference lies in what it takes to gain the addition Certification Credit Points that NASPO Certification currently requires. In the case of Option 4 what it takes to satisfy the bid requirement is the same as it takes to gain the NASPO Certificate. This option was preferred by this discussion group for several reasons :-

- i.** It removes ambiguity from the bidding process
- ii.** It discourages bidders from seeking ways to prove bid compliance that avoids NASPO Certification. These ways will be sought to avoid the added cost and operational complexity associated with delivering the addition risk reduction present in the “Elective” part of the NASPO Certification Requirement.

One member of the Group was in disagreement with the cause and effect relationship represented by this reason :- the participant expressed the view “that contract requirements will encourage NASPO certification, not this particular change in the standard”.

- iii.** Because of ii. above, the public standard will come closer to satisfying the goal of Organizations seeking to outsource (to NASPO) the Security Assurance auditing of supplier and/or internal organizations.
- iv.** Also because of ii. competing end user Organizations will be more willing to adopt a common Security Assurance standard that will lead to the desired result of supplier companies having to comply with, and be audited by, just one audit entity (NASPO) rather than numerous customer auditors as is the case today.

Recommendations

1. Abandon the use of “Electives” for all Classes of NASPO Certification.
2. Base Certification solely on compliance with a set of published mandatory requirements.
3. Replace the term “Elective” requirements with “Enhancement”
4. The NASPO Standards Committee (not the NNSC) to review all of the existing risk management requirements to confirm those to be included in the mandatory category and those to be included in the enhancement category.
5. Change the wording of several sections of v 1.0P to be consistent with recommendation 2.
6. Add additional wording to encourage Certification candidates to enhance their compliance with the mandatory requirements by implementing a relevant selection of risk reduction enhancements. The wording should make it clear that compliance with all risk reduction enhancements will be noted in the NASPO Audit Report and that the latter may be used by the Certificate holder to verify the enhancements in the event that one or more of those enhancements are specified as a procurement requirement.
7. Add wording in v 1.0P to address treatment of mandatory requirements in situations that involve no risk. For example, if a wireless network is used to transfer files, that network must be secure. If no such network exists then clearly the NASPO Auditor will register “no

risk” and indicate that the requirement is not applicable in the context of that specific organization.

Reasons for Recommendations

Under the present system, NASPO Certificates are awarded when applicants have :-

1. satisfied all risk management objectives.
2. complied with all “Minimum” risk reduction requirements.
3. complied with “Elective” requirements that gain the applicant a required number of “Certification Points” in each area of risk.

For example, to be awarded a Class II Certificate, applicants must reduce **Supply Chain Risks** (see p. 21 of v 1.0P dated March 15, 2005) by complying with all 11 of the Mandatory requirements shown in Table 6.4.1; gain a total of 7 Certification Points by self selecting the implementation of sufficient Electives from a total of 12 supply chain electives (see p.49 of v 4.0 dated September 24, 2003) and finally they must satisfy the Supply Chain Risk Management Objective (see p. 21 of v 1.0P dated March 15, 2005).

As a result of the above 3 components of this Certification system it is true that :-

- a. all Certificate holders have satisfied **exactly the same** set of Minimum requirements.
- b. All Certificate holders have satisfied **exactly the same** set of Risk Management Objectives.
- c. All Certificate holders have gained the required number of additional Certification Points.
- d. Some holders will have gained more additional Certification Points than others (by implementing more risk reduction electives).
- e. Each holder will have, in all likelihood (especially in Classes II & III that have more choice of Electives), selected and complied with a different set of Electives.

It is this latter item **e.** that is the root cause of concern expressed by those involved in the competitive bid process. Clearly, if it is a requirement of a competitive bid, that a bidder comply with a specified NASPO Class of Security Assurance, the procurement authority cannot be certain (because of item **e.**) of the specific risks that have been reduced by a NASPO Certificate Holder. By eliminating the ‘Elective’ self selection component of the present system a procurement authority will know that all holders of a NASPO Certificate have reduced exactly the same set of risks. More importantly, the procurement authority will know that specifying a specific Class eliminates the possibility of bidders protesting because of an “un level playing field” caused by a competitor gaining a NASPO Certificate by implementing (what might be perceived as) easy to achieve “Electives” that are not necessarily relevant to the risk situation of the bidder.

To avoid changing the 3 component structure of the present NASPO Standard, consideration was given to other ways that procurement authorities might be able to specify the NASPO Standard in a manner that avoids the uncertainty and potential protest problems that arise from the “Electives” component. Ways considered included :-

- i. specifying compliance only with the Minimum requirements of a specified NASPO Class.

NNSC Sub Committee Report & Recommendation on Electives

- ii. as in i. above plus compliance with specific “Elective” requirements associated with that Class or any Class.
- iii. specifying compliance with specific Minimum and/or “Elective” requirements regardless of Class.

All of these ways succeed in eliminating the “Electives” uncertainty but create other problems. Only in the case of method i. can the holder of the specified Class of Certificate use that Certificate alone as evidence of meeting the procurement requirement. In cases ii and iii the holder may need to deliver additional security. As well, none of the methods are procurement friendly. All require a fairly intimate knowledge of the 3 component feature of the present system and awareness that the “Electives” component implies that holders of the same Class of Certificate are very likely reducing a significant number of different risks. Used in these ways (as in i, ii and iii above) also creates potential problems for NASPO. Method i. in particular (and ii to a lesser extent) represents compliance with a subset of the full set of requirements that must be satisfied for NASPO Certification. The size of the subset varies with each Class. An indication of the subset sizes can be seen in the Accreditation Points Summary table given on p. 46 of v 4.0 of the Standard. The “Points” associated with satisfying the Mandatory and Elective requirements are as follows :-

Requirements	Class I	Class II	Class III
Mandatory Points	194	108	40
Elective Points	30	43	49
% Electives	15%	40%	123%

These quantities provide an indication of the “amount” of risk reduction contributed in each Class by satisfying the Mandatory requirements compared to the Electives. In Class I the “Electives” contribute 15%. In Class II the “Electives” contribute a significant amount of risk reduction. Clearly, in Class III, ‘Electives” contribute most of the risk reduction.

The problem for NASPO is that specifying compliance only with the Mandatory (=Minimum) requirements will motivate bidders to avoid the added cost & complexity of the Electives by finding a way to avoid NASPO Certification that requires them. A way to do this is to convince the procurement authority that non NASPO Certified auditors are able to do this with validity. This undermines the integrity of the NASPO Standards and thus is undesirable for all stakeholders.

Others in this Sub Committee group believe strongly in the principle that all holders of the same Class of Certificate must reduce the same risks but accept the fact that risk exposure will vary between holders. To cater for the latter, the suggestion was made to create a two component system consisting of a set of Mandatory requirements and a set of self selected or customer specified risk reduction “Enhancements”. Under this system, NASPO Certification would be based solely upon compliance with all of the Mandatory requirements. At the same time as verifying compliance with the Mandatory requirements, NASPO Auditors would also verify compliance with any risk reduction “Enhancements” that were either deemed necessary by the applicant or required by the applicants customer to reduce one or more specific risks. It is believed that this system would be more customer and procurement friendly, signal a higher degree of equality between holders of the same Certificate and ease the selection & specification (by security technology users) of specific risk reduction requirements to cater for specific risk exposure. It may also avoid implementation of some unnecessary risk reduction that was introduced in the 3 component system just to gain the requisite additional Certification Points.

NNSC Sub Committee Report & Recommendation on Electives

At the end of the day it was the consensus of the Sub Committee that the move be made to a 2 component system, as outlined above, for these primary reasons :-

- holders of the same Class of NASPO Certificate know that they are all reducing the same set of risks.
- organizations wishing to use that Class of Certificate, as hard evidence of risk reduction, know that all holders of that Class of Certificate are reducing the same set of risks.
- risk exposures that are not covered by the Mandatory set (required for Certification) can be reduced either by self selection or by customer/procurement specification of one or more of the risk reduction "Enhancements".
- removal of an incentive to avoid NASPO Certification caused by procurement authorities specifying compliance with the set of Minimum requirements in the 3 component system.
- to motivate procurement authorities to specify compliance with a specific Class of NASPO Certification.
- to make the NASPO Standards more user friendly and more easily customized to the specific risk exposure and/or corporate risk reduction policies and requirements.
- to simplify NASPO Auditor training and Audit operations.

POSTSCRIPT

One issue that was brought to the attention of the report writer (after the two Telecon) concerns the permissible scope of the "Enhancements", the cost of auditing them and who pays. The issue was raised is as follows:-

When an end-user decides that they want to have 10 specific "enhancements"; who audits the supplier for the enhancements? Do we send an auditor to verify those 10 enhancements, how about 3 enhancements? This could get very costly for the supplier if we have to send an auditor in at \$1000.00 a day, plus expenses to verify a few enhancements.

Points made by Participants

Part of the reason for using the 3 component system in the original NASPO Standards was to use the "Elective" component to conceal the use of protective barriers from the bad guys. "Security through Obscurity", as it was termed, has not been found to be effective according to Trustwave.

Counterpoint to Trustwave comment:-

One of the most effective deterrents with a home alarm system is the sign you put in your front yard and stickers you put on your windows. This is the first line of deterrence and is equivalent to being NASPO Certified. The burglar doesn't know what you have inside, but does know you have an alarm system and goes some where else. Under the system we are proposing we are essentially putting a list on the front door with no ambiguity, telling the bad guys what we have inside the house; alarms on the windows, no alarms on the doors. He knows there is something valuable inside, so, instead of wondering if you have an alarm on the door, or a big dog, or armed guard; he will go through the unalarmed door.

NNSC Sub Committee Report & Recommendation on Electives

Concealing some of the requirements from the bad guys also conceals them from the good ones. This was considered by several participants to be a major disadvantage.

Basing Certification, on a set of Mandatory requirements only, reduces Auditor discretion. This in turn is expected to reduce the degree of variation between individual Auditors and improve Audit results repeatability. It may also simplify and ease the Audit process.

Counterpoint :-

The Auditor will use the same level of discretion in evaluating the Mandatories or the enhancements (electives), and this change will have no effect on the auditor's discretion or degree of variation.