



NASPO

NORTH AMERICAN SECURITY PRODUCTS ORGANIZATION

Minutes of NNSC Teleconference

Thursday March 20, 2008

Callers: David Brown (Intel), Mike O'Neil (NASPO), Graham Whitehead (NASPO), Kevin Kaporch (GPO), Bob Addlesberger (Gemalto), Chuck Hardester (NAPHSIS), David Elliott (Ashton Potter), Robert Sherwood (Sekuworks, NASPO Chairman)

Apologies received from Jason Orloff and Jim Shaffer

Chair: David Brown

Anti Trust policy was noted.

The updated workshop file had not been distributed prior to the call, other than to David Brown. A few minutes were spent sending the document to everyone on the call and confirming delivery to all participants.

It was noted that several changes had been resolved at the meeting in Dallas on March 13. The discussion moved to Section 2-22. An action from the Dallas meeting was to add wording to the Definition. It was asked whether the changed wording reflected the decisions made at the Dallas meeting. It was confirmed that the encrypted transmission implied security sensitive material only. What is secure information is addressed in the Guideline and is considered to be company specific. Discussion followed regarding what should be put in the document that goes for public review re: encryption. Should it note private as well as publicly reviewed encryption. There are only two public encryption technologies. It was decided that a definition of strong should be added to the Interpretations. Leave the wording as is for the public reviewed document. This is a topic of concern to Dan Thaxton, so he can contest it further during the public review period if he is not satisfied that they have addressed the item sufficiently.

Considerable discussion on this topic included notes that some customers send unencrypted sensitive material, the customers accepting the risk. The company is ultimately in control and therefore if a customer is unwilling to receive encrypted material the company must decide on their willingness to send open files. Asked whether the item was also relevant to Canada, being as NASPO is north America, it was commented that although North America, this standard is an American National standard and therefore needed to comply with Fed. Guidelines. (all encryption methods are NSA approved)

GDW to add words to the Definition saying that strong includes algorithms tested by NIST plus any government systems, all with NSA approval. The wording will include a reference to both NIST and NSA.

For efficiency it was decided that GDW will email all wording changes to the group for review and voting at next call.

Moved to 2-44. Major issue is whether to change E to M for both Class I and II. Generally considered that it was essential and should be M for Class I and II. As Class III tend to have little infrastructure and are less secure, Class III could have the option, but not make

encryption a requirement. Class III could be forgiven encryption, but still need authentication.

It was decided to split authentication and encryption. Authentication to be required of all three classes with encryption a requirement of Class I and II but an E for Class III.

2-45 was debated, it is presently an E for all classes. It is related to 2-22, with 2-22 being the first form and 2-45 the secondary data, therefore they should be at the same level – M for Class I and II and E for Class III. This was accepted by all.

2-47 Dual Access. This topic received considerable evaluation. Dual access is common in most military and systems containing personal or private data and other sensitive material. The matter could be clarified by using the word data instead of computer and split general and sensitive data. It is possible to comply with the requirement for dual access without needing two physical presences so that persons can access with input from two different locations. Protect specific areas with dual access. It will remain as the same requirement, (E & M)

GDW to reword to reflect dual access to secure data files and remove reference to computers. Protect specific areas with dual access.

2-48 done, remain an E.

2-49 to stay as is.

Move to 4-8

Need to agree on retaining the requirement. Agreed that at minimum it should be added into the interpretation. It should address whether it is Mandatory depending on physical or virtual content.

It was considered that the requirement needed to stay. It keeps people within the supply chain aware and signing confirms that awareness. Similar to the need for NDA's. The Interpretations can reflect the waiver for virtual technology.

It was further considered that this awareness could be an addition to security training and that in future editions of the standard there should be a separate section for security training as presently the subject is referenced in several areas throughout the standard requirements, but the references would be better consolidated together in one area. This could be a sub-section of Section 6 or possibly a new Section 10.

4-8 requires that there exists an awareness of supply chain risks. This requires some record of the awareness, be it signatures, fingerprints or some other record. Debate as to whether this is done now or over time. 4-7 is a document that recognizes the need to pay special attention to supply chain vulnerabilities while 4-8 is the recognition of having read the document. These could possibly be combined. Most duplication of requirements have been removed in this review of the standard, but these two could logically be combined and possibly moved to personnel in future editions.

Decision to leave as is for the present review and look at consolidating issues into better groupings in the next 2 year review. Will re-write some clarifications and add reference in Interpretations to organizations without physical product.

KK had to leave call – this meant there was no longer a quorum for voting, but it was decided to have discussion on another issue with a vote at the next call.

Discussion moved to 4-19. The Interpretations question how the customer is going to use product. Most times, companies have a need to know how product will be used. It is necessary to have some knowledge of the end purpose to ensure the correct class of

certification be appropriate for the value of the technology. How do you assess the dilution of the technology? The Auditors just want to ensure that good strong technology is being well protected. The entity to evaluate this is the technology owner.

It was decided to refine the requirement to ensure that the technology owner understands the use of the technology. 4-19 is too generalized, there is a need to document that due diligence is being done. Maybe this needs a usage agreement, with some ingredients controlled. It needs to be embedded in a way that it makes it difficult to exploit. The owner of the technology must understand the risks and protect the technology. It is difficult to cover the full spectrum. Need to recognize that the level of vulnerability reduces as you go down the chain. Vulnerability of the product needs to be documented until it reaches a non-vulnerable state.

This topic will be the start of the next working teleconference in two weeks time.

Next teleconference:

FRIDAY April 4

Call: 916 356 2663

Bridge: 3

Passcode: 9175535

Following calls

Friday April 18

Call:916 356 2663

Bridge: 2

Passcode: 3771132

Thursday May 1

Call: 916 356 2663

Bridge: 2

Passcode: 8533637