

NNSC Teleconference
April 4, 2008

Attendees: David Brown, Chairman,
Graham Whitehead, David Elliott, Bob Addlesberger, Chuck Hardester, Robert Sherwood, Alex Lewis, Mike O'Neil.

Meeting started by referencing the Anti-Trust Policy.

Discussions were based on Master Worksheet, April 4

Main Issue left from the previous meeting to be discussed is Customer List. However, first order of business was to vote on several smaller issues that were discussed at the last teleconference, but were not dispositioned due to lack of a quorum.

The minutes of the teleconference held on March 20th. were not reviewed as they are posted on the website.

Discussion started with ANSI/NASPO 2-22. There was discussion on the difference between specifying product use when a company is handling security technology in raw form and can be used in true security mode, and use once the product is part of something else so that it cannot be changed into anything else. As product goes forward and is integrated into other items the security value is being added, but the vulnerability of the original product is being removed. Most vulnerable items are blank, finished documents, cards, labels etc. once personalized they are not so vulnerable.

DB noted that RS had raised the issue.

RS main concern is the language. The language which is in the Guidelines express the auditors concern about protecting the security value to ensure that the value is not being undermined by the company certifying to an incorrect Class level.

The main concern from the auditors is the need to ensure some level of due diligence is being made by the supplier, that the user is giving correct protection to the product, i.e. trying to ensure that a Class III is not involved in handling passports. If a customer is satisfied with the level of security assurance being used, then the auditor will accept that. However, if an auditor is concerned it can be pointed out in the report, but that will not be cause for denying certification.

RS expressed concern that some Class II will never be audited. 4-19 in the Definition is somewhat open and Interpretations may have too many points, making it too clumsy.

DB noted that bringing into 4-19 the Table helps, but questioned how we reword to move forward?

RS suggested "security technology be put into a state where it cannot be altered. Agreement is not necessary if the security technology is sold in a state where it cannot be extracted for re-use." These words could be added to the Definition.

GDW proposed that RS do a re-wording of the item to gain a clearer definition of the Requirement for both the Definition and the Interpretation.

DB noted that a company must have a written procedure for the protection of the security technology and the company must follow their own procedures. 4-19 is requiring this. There are such a broad spectrum of technologies to cover.

MON asked if it is actually technology or products. Maybe it is the application, not the technology, that needs due diligence.

DE expressed concern that due diligence may not imply documentation.

DB reminded everyone that the Standard must be as black and white as possible, no grey interpretations.

In that case, RS noted, the agreement is for the chain of use so that it cannot be converted to a fraudulent use. He considered that there were still issues with the wording of the interpretations. Change the wording of the requirement to protecting technology as supplied by the supplier. Downstream coverage until it cannot be diluted further.

GDW noted the issue of material supplier selling the product for both secure and non security use. The non secure user is not protecting the technology.

So, where does the responsibility lie?

If selling a product as a secure product or technology, then it needs to be protected at the same security level by all customers. If selling to non secure customers, then there is a need to notify security customers of this sale.

DB now we are back to the initial question – What do we want the auditors to do?

Put the protection responsibility on to the technology owner. The seller should be able to pass the requirement to the customer. This should be a Requirement

4-19 Demonstrates that technology owners are following use restrictions

DE-This goes back to your contract with your customer.

DB-The auditors check whether the company is following the requirement of the supplier of the technology.

GDW – the requirement is the need to show intent of due diligence.

RS and GDW will try to re-word the requirement, definition and interpretation to require an assessment of the risk of potential misuse and lack of protection by customers and implementation of “use rules” in the event the risk must be reduced. The re-wording must take into consideration the fact that the risks are low for product that is unique to a particular customer, fully finished, cannot be reverse engineered and raw security materials cannot be extracted, re-processed and re-used.

DB – Do we ratify the previously discussed items?

2-22 Do we have a consensus of the rewording of transmission to transfer? Oxford dictionary explanation would imply that we should keep both words, which is how the new wording is stated.

No further objections, so 2-22 is ratified.

2-44. remote access to file servers. There was a consensus to split. Encryption is burdensome to Class III. However, if they are using sensitive information than they should be using some encryption technology.

Decision to split 2-44 into A & B for clarification. Authentication for all classes, encryption for Classes I and II. Ratified.

2-45. Not mandatory for any class. Change to M for Classes I and II.

Is there any “grey area” for classifying “sensitive?”

A burdensome process to decide what is sensitive. Maybe some additional information on what should be classed as “security sensitive” should be added to the guidelines. Presently the company makes the decision.

A policy for classifying data could be added to the new Section 9.

2-47

Drop term computer – change to secure data file and add Mandatory when handling PII. Also need to add PII to Glossary, using the Department of Commerce definition. Should it refer to internal and/or external . External only

2-47 is agreed with additional reference to D of C and external.

2-48 Should be optional, therefore E for all classes. Ratified.

2-49 Need to protect PII. Consensus.

Moving to 4-8. Question of whether to keep. Agreed

Records should be stored. Could be stored in employees files which would make it easier for retrieval and updating etc.

GDW-The original idea had been to consolidate all details from security operations in one place. Could change into personnel records.

Consensus to change to personnel filing.

Moved discussion to drug screening



Concern raised by BA. They do drug screening prior to hiring. Then they have no re-test. The standard indicates re-testing annually. This is costly in time, fees, etc. Could this be made random? Regular annual tests give staff the opportunity to purge themselves of drug traces prior to testing. Random testing is logically easier for employer and may be a little more preventative on personnel.

Ref. FAR's and DOD's. FAR's accept random testing.

Noted that some states do not allow random drug tests.

Wording could be changed to have dual option with random only were allowed by state law.

How about % of employees tested? No expertise information on %. Needs to be a meaningful number .

Should be at 25-30%. Agree on 25% with guidelines on 'random'

Random testing unless restricted by law, then use of an alternative system. Use 25% as recommended number.

Change wording in the Requirement, Interpretations and Guidelines.

Next meeting (April 18) will look at 5.30 Intrusion. Suggestion of changing to a blanket coverage and whether M or E for each class. Will start by studying Physical Intrusion and then look back at the Objectives.

Next Teleconference

Friday April 18

10.00am PST

Call in 916 356 2663

Bridge # 2

Passcode: 3771132