

SBP/07-0026

INCITS

InterNational Committee for Information Technology Standards
INCITS Secretariat, Information Technology Industry Council (ITI)
1250 Eye St. NW, Suite 200, Washington, DC 20005
Telephone 202-737-8888; Fax 202-638-4922

Date: October 26, 2007

Reply to: Ed Stull

Phone: (301) 260-1781

Email: estull@datavantage.com

Draft Minutes - Formation Meeting
INCITS Study Group on Security Best Practices
Meeting 4

Teleconference Meeting

Wednesday, October 23, 2007 11:00 PM to 2:15 PM

1. Administrative

1.1 Call to Order

Mr. Stull, Chairman of the INCITS Study Group on Security Best Practices, called Meeting 4 by teleconference to order at 1:14 PM. He welcomed the participants and thanked once again Mark Clancy and Citigroup for arranging the teleconference.

1.2 Appointment of Recording Secretary

Mr. Stull noted that he will prepare the minutes with the help of Christine Knibloe.

1.3 Introduction of Participants

Each meeting attendee was introduced by roll call, then the Chair asked if anyone else was present. Only existing members were present:

Member	Representative(s)
Booz Allen Hamilton	Nadya Bartol (2 nd meeting)
Citigroup	Mark Clancy
Communication Intelligence Corp (CIC)	Russ Davis (Advisory)
Coventry Health Care	Tom Wehrle (Alternate)
Credit Industriel et Commercial	Kenneth Belva (Alternate)
Direct Computer Resources (DCR)	Joe Buonomo (Alternate) Ed Stull
Financial Insights	Aaron McPherson
IBM	Christine Knibloe
Pacific Life Insurance Co.	Micki Krause (2 nd meeting)

Mr. Wood, the Zions Bancorporation member, announced by email just before this meeting that he would not be present at the meeting due to an urgent business obligation.

Voting Status

At this meeting the following membership changes have occurred since the last meeting:

1.4.1 Organizations that have requested voting membership

None.

1.4.2 Organizations that have requested advisory membership since the last meeting

None.

1.4.3 Organizations that have updated/changed their membership since the last meeting

None.

1.4.4 Organizations that have resigned their membership since the last meeting

In the absence of response to requests, Vineyard Bank and Wells Fargo have lost their recent membership status.

1.4.5 Organizations that missed the last two meetings and will be issued jeopardy letters

None.

1.5. Antitrust Guidelines

REF: <http://www.incits.org/inatrust.htm>

Ms. Stull reminded the participants of the need to maintain the utmost fairness in the conduct of the Study Group and referred the participants the reference document below.

2. Chairman's Remarks

Mr. Stull expressed that the goal of this meeting and the balance of this month (October) was to mostly complete the discovery portion of the work leading to the development of the Study Group report to the INCITS Executive Board. He further offered that he estimated that the current membership was short by about 3 to 4 members for easily distributing the workload of preparing and writing this report.

Again, Mr. Stull emphasized the importance of developing a strong consensus base over the financial service and insurance sectors. In responding to this comment, the participants strongly agreed that the broadest consensus would be developed through relationships with the major industry consortia such as X9, BITS, FSTC, LOMA, etc..

3. Approval of the Agenda

REF: SBP/07-0017

Mr. Stull invited the participants to review the agenda to determine if any changes were needed. Mr. Benigni offered to present a brief report on the recent SC 27 meeting which Mr. Stull assigned to Agenda Item 5a. The following motion was addressed:

Motion: Clancy - Move to approve the revised agenda.

Second: Buonomo

Motion Discussion: There was no formal discussion of the motion.

Vote: 6-0-2=8

Motion passed.

4. Document Distribution

REF: SBP SD-01 (SBP Standing Document 1 – Document Register)

Mr. Stull call attention to the online Document Registered (http://www.incits.org/tc_home/sbp/sbpdocreg.htm) then called for any late documents to be presented. No late documents were presented.

Mr. Stull also call attention to the password-protected Members Only section of the Study Group's web site (http://www.incits.org/tc_home/sbp.htm) and noted the value of these document collections.

5. Approval of Pervious Meetings (2, 3) Minutes

REF: SBP/07-0018 Draft Minutes - INCITS Study Group on Security Best Practices, Meeting #3, October 12, 2007

REF: SBP/07-0016 Draft Minutes - INCITS Study Group on Security Best Practices, Meeting #2, October 4, 2007

No changes were expressed. The following motion was addressed:

Motion: Clancy - Move to approve the minutes.

Second: Buonomo

Motion Discussion: There was no formal discussion of the motion.

Vote: 6-0-2=8

Motion passed.

5a. Report on Recent SC 27 Meeting by Mr. Benigni

Update on the status of 27005, *Information Security Risk Management*:

US National Body approved this document and did not comment on it prior to the meeting. The US NB participated in the meetings and helped move the document forward to the FDIS stage.

After much discussion the document was approved for registration as an FDIS with 4 "no" votes from Austria, Australia, New Zealand, and Spain. Austria objected to use of an unknown term (incident scenario), the rest of the "no" votes cited the fact the document does not address recent developments in the field of risk management, including ongoing work on ISO 31000 and ISO Guide 73, as well as some risk analysis research. Spain will be providing a contribution to address the latter issue.

The US NB approved the document with our position being that it is needed now and waiting for the ISO 31000 is not appropriate. We believe that once ISO 31000 is published an early revision of ISO/IEC 27005 will be required to make it consistent with ISO 31000.

The revised text of 2nd CD is due to SC27 Secretariat on November 16, 2007.

6. Review of Previous Meeting's Action Items

Action Item 1: Members were invited to submit contributions for consideration at the October 23, 2007 teleconference meeting proposing

further refinement of the work plan topics (Risk Management and Compliance).

Mr. Stull reported progress by members on this action items and offered that this action item was now completed.

Action Item 2: The Chair with contact INCITS Secretariat regarding the new members at this meeting.

Mr. Stull reported progress on this action item, but more work remained to reach the needed participation level. Ergo, this action item will remain open.

Action Item 3: Mr. Stull will create and contribute a high-level draft of the SG-SBP Technical Report.

This action item was completed. Mr. Stull distributed the high level draft of the Study Group report using the Study Group Reflector.

Action Item 4: Members were invited to submit contributions on the Work Plan and Timeline for consideration at the next meeting.

No work plan contributions were received. However, due to the membership consensus over the general work plan introduced at Meeting 3, it was agreed that this membership action item was now completed.

7. Unfinished Business

There was no unfinished business.

8. Review of Strategic Collaborations

REF: SBP SD-03 SBP Standing Document 3 – Strategic Collaboration

Mr. Erkonen, the Vice Chairman for Strategic Collaborations, was not present at the meeting and unannounced. No participant was aware that he had designated anyone to act in his behalf. As a result, the status to be reported to the Study Group membership of his interactions with X9, BITS, FSTC and possibly others remains unknown and a pressing matter.

Action Item: Mr. Stull is to call and send an email to Mr. Erkonen asking him to prepare a brief status statement and distribute it through the Study Group Reflector.

9. Review of Consensus Base for Financial Services Sector

The meeting participants strongly agreed that the broadest consensus would be developed through relationships with the major industry consortia such as X9, BITS, FSTC, SC 27, etc.. Further, it was believed that although the Study Group will be soon acquiring several new members, it is not likely that the Study Group will ever acquire, nor is it appropriate, that the Study Group will have the high participation numbers to achieve broad international consensus. Thus, collaboration with industry consortia remains the best approach to achieve the consensus goals. Additional participation by government representatives would also help build consensus. The members also recognized and discussed the commonality shared by the financial services and the insurance sectors would help build consensus.

Mr. Stull again offered that it was important to also consider technology vendors, including service providers, in that their technology and the availability thereof is what drives the market place.

10. Review of Consensus Base for Insurance Sector

Mr. Wehrle, also representing Mr. Talbot, expressed their continued efforts to acquire more Study Group participants from the insurance sector. Ms. Krause, addressed again that the insurance sector was just now beginning to recognize the need for insurance-sector wide cooperation and collaboration to achieve its goals for improved security. Ms. Krause is actively pursuing participants from and possible collaboration with LOMA.

11. Technical Interchange: Risk Management and Compliance

Discussion continued from Meeting 3 about the nature and requirements of risk management and compliance, again noting how it is that compliance can become misaligned with risk management. The work at Financial Insights was noted due their endeavor to create a "Fraud Index" and how such metrics may aide in defining the problem space of the financial services and insurance industries. Similarly, it was noted about the metrics work in the life insurance sector for evaluating risk. The consideration was on how such metrics endeavors could be encouraged and unified leading to industry wide methods for risk assessment.

Mr. Stull called on members to describe their own preferences for risk management approaches and models as well as how they are currently dealing with such issues in their organizations. Mr. Clancy described the general approach used at Citigroup. Note that this appears to be found reasonable among the meeting participants.

All of the contributions in the Document Register were noted to require further study by the membership based on the meeting discussions and thus will be carried to Meeting 5 for final consideration. Following the meeting, various members will be contributing further documents that they believe relevant to the meeting discussions.

12. Technical Interchange: Other Proposed Study Topics

No contributions were made to this agenda item. Therefore, Mr. Stull, after calling again for contributions and without objection, moved to the next agenda item.

13. Development of Security Best Practices Report

Mr. Stull discussed again the nature of Study Group Technical Reports and expressed that the current high level plan for creating the SG-SBP Technical Report would be to use the month of October to discover resources and concepts that were good candidates for further study; then, use the month of November decide about the discoveries of October; then, use December to create and assemble the body of the report; and lastly, use the early part of January (2008) to complete the final editing touches on the report. Delivery of the report would be at the January 2008 INCITS Executive Board meeting in Washington DC. Mr. Stull had created and distributed through the Study Group Reflector, a high-level draft of the report that would subsequently be updated with member contributions.

Mr. Stull called for a member to volunteer to be the Editor of the report. Mr. McPherson volunteered wherein he and Mr. Stull will meet subsequently to begin assembling a thematic outline of the report.

14. Work Plan and Timeline

REF: SBP SD-04 (SBP Standing Document 4 - Work Plan)

Mr. Stull referenced the previous agenda item and offered, if no objection and in the absence of other contributions, to continue to use the Meeting 3 discussion (as described above in 13) for specifying the general Work Plan and Timeline.

15. Review of Action Items from This Meeting

The following action items were assigned during this meeting:

Continued Action Item 1: The Chair with contact INCITS Secretariat regarding the new members at this meeting.

New Action Item 2: Mr. Stull will call and send an email to Mr. Erkonen asking him to prepare a brief status statement and distribute it through the Study Group Reflector.

16. Future Meetings

REF: SBP SD-05 (SBP Standing Document 5 - Calendar)

Mr. Stull noted that the next meeting would be held November 20, 2007 by teleconference, and that this would be the last meeting for finalizing the basic discovery of documents, role-players and concepts and, most importantly, the primary meeting to resolve Study Group positions on these discoveries.

17. Adjournment

The October 23, 2007, Meeting 4 of the INCITS Study Group on Accessibility adjourned at 2:10 PM by unanimous consent.

Motion: Clancy - Move to adjourn the meeting.

Second: Buonomo

Motion Discussion: There was no formal discussion of the motion.

Vote: 6-0-2=8

Motion passed.