



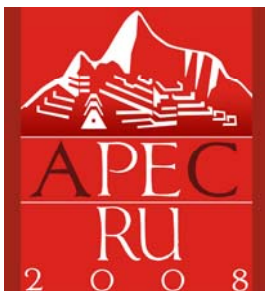
**Asia-Pacific
Economic Cooperation**

2008/TEL38/PLEN/025

Agenda Item: 9.3

SPSG Report

Purpose: Information
Submitted by: SPSG Convenor



**38th APEC Telecommunications and Working
Group Meeting – Plenary Session
Lima, Peru
15-17 October 2008**

SECURITY AND PROSPERITY STEERING GROUP MEETING

APECTEL38, Lima, Peru

October 16, 2008

Convenor : Jinhyun Cho, Korea, Republic of

Deputy Convenor : Jordana Siegel, United States and Steven Stroud, Australia

1. ADOPTION OF AGENDA

The convenor welcomed all economies for coming to Lima for the Security and Prosperity Steering Group (SPSG) meeting in TEL37 and expressed the gratitude to host, Peru.

All the economies were asked to review and comment on agenda. The Agenda was adopted by the SPSG

2. TELMIN7 : Output and Direction Ahead

The 7th APEC Ministerial Meeting on Telecommunications and Information Industry (TELMIN7) was held at Bangkok in April, 2008. The 38th TEL meeting is the first meeting after TELMIN7. The convenor reviewed all SPSG activities including on-going projects and project proposals and developed a stock-take table mapping SPSG works with the Bangkok Declaration. The table was developed to measure effectiveness and also to capture the ongoing work of the SPSG. SPSG can also use the table to help frame future work. The convenor mentioned that SPSG will work together by e-mail to keep the table updated.

3. Report of workshops

Following two SPSG workshops were hosted by SPSG during the TEL38 meeting in Lima

- a. Telecommunications for Disaster Management: Best Practices Workshop
- b. Workshop on Cyber Security Awareness Raising

3.1. Telecommunications for Disaster Management: Best Practices Workshop (Peru, Chile and Mexico)

The workshop purpose is to build the telecommunication capabilities even in case of emergency, including natural disasters, sharing the experience and expertise on resilient and sustainable telecommunication systems to ensure availability.

Peru updated about the results of workshop. Participation included about 75 participants during the full-day workshop. There were 3 components of the workshop: the international perspective (ITU, APEC); Information and experience sharing from member economies and private companies with different types of disasters, such as tsunami, earthquake, hurricane, typhoon, volcano and etc ; and, planning and emergency response. There was also discussion with economies about how to build on the workshop and collaborate going forward. One suggestion is to organize information that is available based on experiences of member economies. Accordingly, Peru proposes that work will continue interessionally with a virtual working group/task force to determine next steps from the workshop and how best to collaborate. Peru would like input from economies about aspects that can be worked on.

The Convener also asked that economies make voluntary contributions. Australia congratulated Peru on the workshop and offered to contribute to work going forward. The US would like to participate in a virtual working group/task force and indicated that the US private sector is also very interested in assisting with development of an agenda.

3.2 Cyber Security Awareness Raising Workshop

Raising the cyber security awareness of all APEC economy stakeholders, including of critical infrastructure owners and operators, small and medium businesses, and end users is one of critical activities to maintain consumer's trust and confidence.

Australia and US held a workshop about cyber security awareness and to discuss how to best proceed with a collaborative activity amongst APEC economies.

In the first half of the workshop Peru, Australia, Japan, Malaysia, Korea and United States provided presentations on awareness raising activities within their economies

targeting government agencies, critical infrastructure, business, industry and consumers. APCERT also provided a presentation on its activities and the activities of its members in this area.

The second half of the workshop provided the opportunities for other economies to share their experiences. Discussed were some of the challenges facing APEC economies in raising awareness about cyber security. These included:

- educating policy makers and other high level officers about the need for awareness raising activities and
- challenges associated with the development of strong public-private sector partnerships to improve the reach and sustainability of awareness activities.

Economies also discussed mechanisms where they could potentially work together to improve cyber-security awareness in the region. These included:

- continuing to share experiences and materials about awareness raising activities
- improving awareness within APEC itself, through drawing attention to the issue of security from officials to leaders and how to encourage other groups to be more secure and take those experiences back to their own economies.
- Great discussion on what we might be able to do together in our economies. This could include developing a contest within APEC economies to develop a slogan or a poster for all economies to use and promote safe online behaviours. The winner of this contest could be then used in all APEC economies for the next year.

United States and Australia will develop a report of the workshop for presentation to the next TEL meeting which will include a proposal for collaborative activity for SPSG consideration. Economies are encouraged to join a virtual working group to assist in the development of this proposal.

APCERT commented that awareness session was a success and felt that the format used was a good approach and allowed more feedback coming from the audience. The workshop identified success stories, methods and approaches in outreach as well as the challenges and agreed that the greatest challenge faced – that the human was most vulnerable. APCERT noted that it would be most useful for APEC TEL to come up with measurable indicators and this area may require more research and study. It is a new

area and would benefit from some kind of study in the future. Measuring impact is something we should work on interessionally.

Canada commented that the format was particularly useful to have informal discussion in the afternoon and a good model for future workshops. Canada would like to work interessionally to further this work and define objectives and specific proposals. Canada suggests that the idea of raising cyber security on an APEC wide basis and suggested that we include language in the leaders statement that confirms the need for awareness raising and confirms the SPSG and the TEL role in this work.

Japan would like to congratulate on success of this work. Japan is very interested in this initiative and would like to work on the result of this workshop.

The Convener reinforced need for additional actions in this area, noting that we need to give attention to developing economies, particularly those that do not have a lot of experience yet in this area.

Singapore would like to thank organizers for the workshop and noted that it is important to keep to timelines particularly if we are looking to include information in the leader's agenda. The declaration will be finalized in October, so all need to keep that in mind.

The Convenor advised that we should exchange contact information through the TEL POC list and make progress on this issue.

4. PROJECT UPDATES AND REPORT

a) Building a Culture of Security – Corporate Policy and Management Issues (New Zealand)

New Zealand indicated that while several economies had responded to the questionnaire distributed, New Zealand would welcome more input from all economies. An interim report is in preparation and would be presented at the next TEL.

b) Judge and Prosecutor Cyber Crime Enforcement Capacity Building Project (USA)

The United States updated the progress made after 37th TEL meeting. The United

States got the project extension approval from BMC (Budget and Management Committee) until May 2009. The training currently scheduled for 10 ~ 12 December (3 days conference), in Kuala Lumpur, Malaysia. The conference will focus on supporting domestic training and awareness raising on cybercrime prosecution and courtroom presentation, with particular emphasis on courtroom presentation of evidence on behalf of government prosecutors.

The training is a "train the trainer" program that would give attendees the tools to develop/enhance domestic training programs. The expectation is that participants will deliver the training (appropriately customized for their respective economies) domestically.

The United States will pay for the training venue and hotel rooms for participants. Participants from eligible economies may also apply to APEC for reimbursement of travel costs, but they must naturally do so before the appropriate deadline. Participants will be responsible for their own per diem.

The training was originally scheduled for April 2008, but was cancelled due to an apparent lack of interest among other economies. At the last TEL in Tokyo, significant interest was expressed to proceed with the project, so the program was rescheduled. The United States are seeing few early registrations, so are concerned about attendance. Anything that can be done to encourage economies to register early is great.

Although SPSG economy representatives may not be the appropriate participants, the United States formally requested assistance from SPSG representatives to identify the appropriate points of contact, at least two points of contact within their ministry of justice or judicial branch to whom we could forward the invitation.

Malaysia is willing to assist US in coordination and would be willing to help with participants as well.

The Convener indicated that economies should expedite their plans to ensure they can participate.

c) Voice over IP (VoIP) Security Guidelines (Australia and Korea)

Australia reported that the project is recently completed. The guidelines are geared to help small and medium enterprises understand some of the risks involved in VoIP technology. Australia has circulated APEC VoIP Security Guidelines and asked other APEC economies to volunteer for translating the guidelines into local languages. To accommodate various translated guidelines, the website (<http://www.apecsecurity.com>) is running and will be maintained for two years. Australia is willing to assist with this if at all possible, so economies are requested to follow-up with Australia accordingly.

The convenor indicated that SPSG reached consensus in adopting the guidelines and would seek the approval from TEL Plenary. The convenor added that the guidelines are a valuable deliverable and SPSG needs to continue updating it. Convenor thanked Australia and Korea for the efforts on the project and valuable project deliverables.

d) APEC-TEL PKI and e-Authentication Training Program (Chinese Taipei)

Chinese Taipei has successfully led PKI and e-Authentication project since 2006. Chinese Taipei updated that 2008 training course will be held from October 29 to November 4, 2008 in Taipei. The training course will include experience sharing, international cooperation, certificate of completion will also be given by the Chair of APEC TEL. Chinese Taipei also updated about the survey summary report available in the form of soft-copy.

The convenor thanked Chinese Taipei for continuing the work on PKI/e-authentication.

e) Guide on Policy and Technical Approaches against Botnet (China)

China provided an update on the background of the project – it was completed in October 2008. This project included a variety of activities - set up an experts group, held informal meeting, designed and conducted a survey, held a seminar in Beijing, built a forum for combating botnets, and held a seminar in TEL 36.

The guide includes an overview of botnets and related malicious activities; current status of botnets; countermeasures for government; countermeasures for industry; best practices; and acknowledgements.

The convenor noted that SPSG reached the consensus to adopt the guide as the deliverable and seek the approval from TEL Plenary.

China also updated about the plan to publicize the guide; continue sharing and experience exchange among TEL members and organizations; building cyber-security platform and coordination system to improve capacities of countermeasures and address regional and international cooperation.

The Convener recommended that China coordinates with the APEC Secretariat regarding process for next steps and asked all economies to give the comment to China before the publication. China reply that, after the consultation with APEC secretariat, the final guide will be sent to APEC secretariat for the publication on APEC website and that China seeks further comment from member economies for the guide before the final submission to APEC secretariat.

The convenor made appreciation remarks on China's leading efforts at countering botnet and congratulated on finalizing the self-funded project.

f) Cyber Security Exercises Workshop(USA/Korea)

The United States and Korea updated that the summary report of the workshop held at TEL36 in Santiago was circulated among virtual expert group and online in TEL38 website.

SPSG agreed to adopt the summary report as the deliverable of the workshop. The deliverable will seek approval from the TEL Plenary.

In addition, The United States and Korea mentioned that, as a response to the call from Bangkok declaration and the follow-up for this workshop, the virtual working group will continue to work intercessionally to identify areas for future work

g) ICT Products and Services Security Workshop (Japan)

Japan noted that they were supposed to submit the support for APEC TEL 38, but are not yet ready to submit the report. There is a draft report, but do not have time to

circulate and ask for comments, so need more time to do that. Japan requested an extension to the next TEL in Singapore to finalize the Project report. The questionnaire will be circulated again for response from various economies. The SPSG agreed to the extension.

h) Handheld Mobile Device Security Workshop (Malaysia)

Malaysia updated that the summary report of the workshop held at TEL37 in Tokyo is now available on the TEL38 website.

A second deliverable from this workshop is a set of guidelines. Malaysia will continue to work on these interessionally and present them at TEL39 in Singapore.

On the request to extend the project period, SPSG reached the consensus and would seek the approval from TEL.

5. OTHER UPDATES ON SPSG ACTIVITIES

a) APCERT Updates and Challenges (APCERT)

APCERT is currently 21 CSIRT teams from 15 economies. There is a need for regional collaboration and building trusted contacts. Objectives are to encourage regional support, information sharing, assist other CSIRTs. APCERT chair provided an overview of recent APCERT activities such as working with the DotAsia Advisory Council to tighten procedures with registrars. The brief also provided information on the current state of Phishing. Current Phishing activities include DNS Fast Flux. One recommendation is to remove the domain. Botnets are also a significant issue and there is a need for more activity to address this.

The convenor noted that individual APCERT teams have actively participated in TEL activities and expressed the word that APCERT, as a group, will contribute to the unique value of TEL.

Canada asked who is typically the sponsoring entity for National CSIRTs. There is no one model, but it is most often one of the Ministry of Economy, Ministry of IT, or Ministry of Science.

b) The StopSpamAlliance (www.stopspamalliance.org)

The StopSpamAlliance is a joint initiative to combat spam amongst APEC, OECD, London Action Plan, and the ITU. Messaging Anti-Abuse Working Group (MAAWG) was also involved is doing some work on botnets, which may be of interest, and the information is available on the stop spam alliance website.

b) ITU's High Level Expert Group (HLEG)

The Convener provided a report about the work of the ITU HLEG. The Secretary General will present recommendations from the HLEG to the ITU Council in November. This will include a focus on global cyber security and next steps based on the HLEG work. On behalf of the TEL, the Convener has contributed some input from an SPSG perspective. Recommendations by the HLEG in the form of Chairman's Report have been published in ITU website¹

Australia inquired about next steps for the ITU and how to ensure that we do not duplicate efforts.

The Convener indicated that following the submission of recommendations to the Secretary General, the HLEG will no longer be convened. The ITU Secretary General will determine next steps and how to proceed. However, the ITU will sign an MOU with the Malaysian initiative, IMPACT (International Multilateral Partnership Against Cyber-Terrorism), to facilitate ongoing collaboration.

6. SPSG REPORT ON OUTREACH ACTIVITIES

a) Report on 3rd WSIS Action Line C5 Facilitation Meeting, Geneva, Switzerland, 22-23 May, 2008

The Convenor was invited to represent APEC TEL at this meeting and provided some updates on SPSG. The summary report of meeting is available in ITU's website²

¹

http://www.itu.int/osg/csd/cybersecurity/gca/docs/Report_of_the_Chairman_of_HLEG_to_ITU_SG_03sept_08.pdf

²

b) Report on THE APEC SEMINAR ON PROTECTION OF CYBERSPACE FROM TERRORIST USE AND ATTACKS, Seoul, Korea, 26 - 27 June, 2008

The seminar is the joint project between APEC CTTF-TEL. Korea government, Ministry of Foreign Affairs and Trade, invited the convenor to represent TEL in the seminar and speak about TEL activities related to cybersecurity and cybercrime.

c) Report on ITU Regional Cybersecurity Forum for Asia-Pacific & Seminar on the Economics of Cybersecurity, Brisbane, Australia, 15-18 July, 2008

The Convenor was invited to represent APEC TEL at this meeting and provided some updates on SPSG. The summary report of meeting is available in ITU's website.³

7. DISCUSSION ON COLLABORATION WITH THE WPISP-OECD

a) Update on the outcomes of the OECD Ministerial meeting

OECD/WPISP provided an update on the OECD Ministerial Meeting, which was held in Seoul, Korea June 17-18.

Challenges noted in the Ministerial Declaration include:

Secure CII and respond to new threats; ensure a trusted Internet-based environment which offers protections to individuals, especially minors and other vulnerable groups; and, promote the secure and responsible use of the Internet.

Objectives include developing policies that protect CII at national and international levels from security risks, strengthen resilience, reduce malicious activity online, encourage collaboration between government, private sector, civil society, and technical community to understand impact, and encourage cross border collaboration.

The planned work for work with APEC includes: follow-up on work on Malware; indicators for security and trust; and protection of children online.

http://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/WSIS_Action_Line_C5_Meeting_Report_June_2008.pdf

³ <http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/brisbane-cybersecurity-forum-report-july-08.pdf>

b) APEC TEL – OECD on Malware

The Deputy Convener introduced preliminary thoughts about future work of APEC TEL/OECD regarding Malware. Is there any area that we can collaborate that would add value to the global effort, but will not duplicate efforts that are already underway? We have mapped out the various organizations that are doing work in this area on a variety of topics. We would like to invite input at this stage.

The Convener suggested that we consider, review and provide input intercessionally. We will not make a decision today, but need to think about possible next steps, including budget, etc.

Suggestions were made on forming a virtual working group to discuss this further. Convener will follow up with an initial inquiry.

Canada noted that the coordination of these efforts will need to be carefully managed and there may need to be some leadership amongst organizations.

It is recommended that we evaluate next steps as equal partners and focus on an area where APEC and OECD each have expertise. There is a need to ensure that the work is joined up going forward.

The Convener indicated that the Malware report will be published.

b) APEC TEL – OECD on Indicators for Security and Trust

With regard to indicators for Government ICT Security and Trust, OECD is currently in the process of drafting this program of work with colleagues in the Statistics Department. The first objective is to better inform policy makers, facilitate prevention of risks and foster trust, and to allow for comparisons across economies.

The work is currently not part of the work plan and would not be self-funded. The WPISP will discuss in November and explore potential financial support from delegations to conduct this work. OECD suggests that the SPSG consider at TEL 39 to revisit this issue.

Australia inquired as to whether we can use APEC funds to support this project on Security Indicators and Trust. The Convener indicated that we need to evaluate this further and will follow-up with DSG to determine whether we can collaborate. Convener also indicated that we need to scope this further.

8. NEW PROJECT PROPOSALS FOR TEL 39

The convenor briefly presented material on the project proposal issues and guidelines to follow.

a) Workshop on initiatives among Member economies promoting safer Internet environment for children (Japan)

Japan presented their proposal regarding a safer internet for children. The proposal is co-sponsored by Australia, Canada and the United States and seeks for one full-day time slot during TEL39. There will be a working group formed. There are a few phases of this work envisioned. Japan proposes holding an APEC-OECD Joint Symposium at the next TEL 39 in Singapore. Outcomes from this project will include a Joint Symposium Report from the Symposium at Tel 39.

Convener noted that Japan will also need approval from the OECD/WPISP, so we may need to adjust the timeline accordingly.

Australia noted their support of this proposal and would like to be involved. Thailand also noted their support of this proposal and would like to be involved in the Symposium. United States noted just how complex the internet economy is. Mexico noted that if Japan is also focusing on cell phones with regards to child safety, they would like to also help with that issue.

OECD will plan to discuss this at the WPISP meeting in November, but given that this was raised during the Ministerial, OECD expects countries to support this work.

This proposal is adopted as an SPSG proposal and will be referred to the TEL for approval. Convener also asked that Japan will also need to notify all APEC economies once this proposal is approved by the OECD WPISP.

b) Bi-lateral Cybercrime Legislative Drafting Workshop

Convener noted that cyber crime is noted in the TELMIN declaration. Member economies should give some special consideration of this proposal.

United States presented their proposal focused on two bilateral legislative drafting workshops that will be held with economies that need assistance, and this project is the follow-up of “Judge and Prosecutor Cyber Crime Enforcement Capacity Building Project”. Malaysia and the Philippines will be co-sponsors for the project.

Canada asked whether the US can share lessons learned from these sessions based on the work that the US has done in this area. Canada would also like to see a course outline and a syllabus.

US indicated that criteria for the workshop will be circulated following the TEL and that the sessions will be tailored for the specific economies that will receive the training.

This proposal is adopted as an SPSG proposal and will be referred to the TEL for approval.

c) Submarine Cable Protection Information Sharing Workshop

Australia noted the presentation given at the last TEL and that the proposal will include a 1-day workshop at the next TEL in Singapore. Hong Kong and Chile will be co-sponsoring the project.

This proposal is adopted as an SPSG proposal and will be referred to the TEL for approval.

9. MALICIOUS ACTIVITIES AND MISUSE OF THE NETWORK INFRASTRUCTURE

Nothing to report.

10. EXAMINATION OF THE SECURITY IMPLICATIONS OF EMERGING

TECHNOLOGIES

Nothing to report

11. EXAMINATION OF ISSUES CONCERNING DISASTER MANAGEMENT, INCLUDING SUBMARINE CABLES

The Australian communications sector has been doing work on this topic and will circulate the materials for everyone for information.

12. ECONOMY REPORTS

Referring to Regulatory Update,

- Canada reported on “Trust and Confidence in the E-Economy”
- Indonesia reported on “cyber regulation”
- Korea reported “Strengthen the Internet confidence and security”
- Peru reported on “Communications System for Emergency Situations”
- Philippines reported on “Cybersecurity and development”
- Chinese Taipei reported “Information Security Improvement in Chinese Taipei”
- Thailand reported on “ICT Security”
- USA reported on “NTIA Seeks Public Comments for the Deployment of Security Technology Within the Internet Domain Name System” and “DHS Announces National Cyber Security Awareness Month”

13. MATTERS ARISING

The convenor mentioned the request from APEC secretariat on the candidate submission of Top Ten list of APEC Achievements and exchange views via e-mail.

Malaysia noted the development of a new standard that is relevant to TEL economies – ISO IEC 27011(Information security management guidelines for telecommunications). It is important for handling emergencies and should be reviewed within the SPSG.

APCERT also attended the ISO meeting in Cypress last week and there are other process issues that SPSG should be aware of. Responsible vulnerability disclosure that economies should

review and discuss domestically.

14. MEETING WRAP-UP - Other Business

The Convener closed the meeting and noted our need to continue to collaboration on an ongoing basis.

Summary of Decisions made at the SPSG Meeting at TEL38

Self-funded Project

The SPSG agreed to seek the approval from TEL Plenary on one self-funded project

Bi-lateral Cybercrime Legislative Drafting Workshop

Proposed by United States

Co-sponsored by Malaysia and Philippines

Workshop Proposal for TEL 39

The SPSG agreed to seek the approval from TEL Plenary on two workshop proposals.

Workshop on initiatives among Member economies promoting safer Internet environment for children(One full-day)

Proposed by Japan

Co-sponsored by Australia, Canada and United States

Submarine Cable Protection Information Sharing Workshop(One full-day)

Proposed by Australia

Co-sponsored by Hong Kong, China and Chile

Approval sought on Project Deliverables(Item 4)

c) Voice over IP (VoIP) Security Guidelines (Australia and Korea)

e) Guide on Policy and Technical Approaches against Botnet(China)

f) Summary Report of Cyber Security Exercises Workshop(USA/Korea)

Approval sought on Extension of Project Period(Item 4)

g) ICT Products and Services Security Workshop(Japan)

h) Handheld Mobile Device Security Workshop(Malaysia)