B

Minutes of the eSTG Meeting

Doc no:

Telwg30/
BFSG/19

Agenda item :

Business Facilitation Steering Group

Submitted by:

Chair, ESTG

Minutes of the eSTG

Contact: David Hickman
Email: david.hickman@dcita.gov.au

APEC Telecommunications and Information Working Group
30th Meeting | 19-24 September 2004 | Singapore

eSECURITY TASK GROUP MEETING : APEC TEL 30: SINGAPORE

TUESDAY 21 SEPTEMBER 2004

eSTG ACTIVITIES

1. Adoption of Agenda

The Chair opened the meeting. The agenda was adopted.

2. Discussion of Work Program

The Chair emphasised the need at this particular meeting to focus on the eSTG's current and future work program, particularly as the Group would be part of the reporting to TEL MIN 6 next year on progress and activities. The Chair indicated that at various stages during the meeting there would be scope for extensive discussion and examination of the Group's work priorities and possible future directions. The Chair suggested to the Group that it was vital to consider what future streams of work could usefully come out of the two workshops held on Sunday (wireless and CSIRT vulnerability handling) and the cybercrime enforcement capacity building project's second conference of experts held in Vietnam (25-27 August 2004). The Chair also commented that some of the Group's activities are now entering the mature stage of their life cycle and that the Group always needed to focus on the relevance of the work program to emerging e-security priorities. For example, he indicated that there would be a panel discussion following the CERTs/CSIRTs presentation on key e-security issues and trends in the Asia pacific region. Possible questions had been posted to guide the panel. The US, China, Japan, Korea and NZ had agreed to participate. The Chair suggested this session presented an excellent opportunity for the Group to respond to the issues presented, again with a future work program in mind.

ELECTRONIC AUTHENTICATION

3. PKI Guidelines

The Chair gave an historical overview of this long-standing project. He indicated that it had been a mammoth project in terms of scope and complexity and was a credit to the Group's erstwhile Chair, Steve Orlowski. The Chair emphasised that it must now be completed and the Group should aim to wrap it up within the next month. However, it was also emphasised that there would be another opportunity for delegates to clear a final version – it would incorporate some of the possible changes flowing from ETSI and indeed any other points/concerns delegates may have. No specific issues or concerns on the guidelines were raised at the meeting. It was agreed that the guidelines be endorsed subject to the caveat that they would be run past delegates via the Points of Contact out of session for a final clearance, with any amendments being highlighted for consideration. On this basis the Group endorsed the guidelines.

Canada expressed its appreciation of this work undertaken by the former Chair. Canada asked that the final document, which is high level, is closely aligned with the more detailed technical content. Hong Kong China indicated its support for the proposed arrangements.

4. Activities of Asia PKI Forum Legal and Infrastructure Working Group
Asia PKI Forum (Hiroaki Rokugawa)

Details were provided of the Asia PKI Forum. There are four working groups: (1) Inter-Operability, (2) Legal & Infrastructure, (3) Business Application, and (4) World-wide collaboration. Details were provided of conferences. A number of reports have been issued. The point was made that as the use of Public Key Infrastructure (PKI) will increase in cross-border e-commerce transactions and government use in Asia, a number of disputes are expected to arise. A report, entitled "Dispute Resolutions for Cross-Border E-Commerce" first provides an overview of the judicial system and alternative dispute resolutions as applied to e-commerce transactions. Next, it addresses hypothetical cases to which member countries/areas shall provide legal solutions in accordance with present domestic laws and regulations of each country/area. This is because there is no convention or treaty on applicable law and/or international jurisdiction that can be applied to all the member countries/areas of Asia PKI Forum. A report will be issued in July 2005, entitled: "CA's Liabilities"

5. Economy reports (a number of economies provided written reports)

Australia provided a report on its draft Australian Government Authentication Framework. A report was also provided on the Australian IT Security Forum's position on PKI. A document was made available at the eSTG document website.

Canada indicated that it has completed that market focused principles. The set of principles is a high level document for industry as a basis for industry codes and guidelines.

China indicated it has an Electronic Signatures Act (August 2004), which will take effect April 2005. Its purpose is to regulate electronic signatures – it also covers legal liabilities.

Hong Kong China indicated that in June 2004 a consultation paper was issued on unsolicited messages (spam). That consultation ends on 25 October.

Indonesia advised that in August 2004 they have an infrastructure internet team. They are also collecting information on spam.

Japan also reported on developments.

Korea indicated that they are keeping pace with PKI interoperability- via the Asia PKI forum.

Malaysia advised it hopes to have an anti spam workshop in the first quarter of next year in KL. They hope to establish a PKI forum by the end of the year.

New Zealand reported on the secure electronic mail service (providing a means of exchanging information securely) and the national authentication project (tenders being issued – pilot results by TEL 31). In December last year, e-government unit stipulated that Microsoft's Information Rights Management is not to be used in government.

Chinese Taipei reported on its Electronic Signatures Act – an amendment will be ready by December.

Vietnam reported on electronic authentication – government decree on electronic authentication is being drafted, which will be submitted for approval.

SECURITY OF INFORMATION INFRASTRUCTURE AND NETWORKS

6. Spyware: implications for security; current approaches

7. Securing information networks and systems against Spam

Noting that no economy had sought to make a formal presentation in either of these two areas, the Chair suggested that it was important for the eSTG to carefully consider what it could usefully do to address these two important issues, without duplicating existing work in other forums. There was a discussion on whether spam and spyware could be coupled as issues in a possible workshop. New Zealand strongly encouraged work be considered in these areas. Korea felt that a joint approach could be useful. It was acknowledged that these terms can mean different things to different people and precision is needed. It was also acknowledged that they also involve a wide range of issues, not just e-security.

The US suggested a possible joint session for two days with the ECSG – around the time of the next TEL meeting. It would be an APEC wide event, to address spam, cybercrime, and Internet integrity. Apparently this joint meeting proposal had been raised in an informal way recently with the ECSG chair, although no specific details had been formally agreed.

On the issue of whether to consider spyware and spam together, Canada suggested that spam is sufficiently complex such that just a spam joint workshop would be better. Moreover, perhaps because of timing considerations, next September (2005) would present a better opportunity for this joint session proposed by the US rather than a February date. Canada also sought clarification of the US proposal.

No document had been submitted before the meeting by the US setting out the details of the proposal (a document was uploaded later that morning).

It was agreed that a discussion group would meet at 1.30pm to clarify possible work on spyware.

It was also agreed that there would be further discussion on both spam and spyware under the final agenda item (workshops). That would allow more time for discussion and consultation until that item.

8. APEC.isu. website

Professor Corey Schou (US) presented a paper on expanding APEC TEL outreach to academia and vendors. He highlighted some of the language choices that are available (eg Vietnamese, Spanish, Korean, Japanese and Chinese). The website is at http//: apec.isu.edu/index.htm.

9. Wireless security

Feedback on this workshop and next steps is attached to this report.

10. Computer Emergency Response Teams/CSIRTs

The US provided an overview of US CERT International Activities. *Secure Cyberspace* – the 5 key priorities were outlined.

Australia provided an update on CERT Capacity Building Project. There was a tender for training involving Chile Peru Mexico and Russia. CERT CC is undertaking that work.

Feedback on the CSIRT information sharing workshop is attached to this report.

There was a discussion on strategies for building further CERT/CSIRT cooperation and capacity. It was suggested that hitherto the TEL had relied on series of CERT/CSIRT workshops. This time we had a vulnerability handling workshop. A more permanent agenda item involving CERTs/CSIRTs was proposed – to mainstream their role into the eSTG. The Group endorsed that approach.

11. Regional Developments

Chris Connolly from Galexia (an ICT consulting firm) provided information on the "harmonisation of e-commerce legal infrastructure in ASEAN" project. It aims to establish a harmonised legal and regulatory and institutional infrastructure for e-commerce. The project focuses on authentication and digital certificates.

Sun–Kyung Choi from Korea gave a presentation on the Asia Pacific Information Security Center. She noted that hacking incidents have increased dramatically (26K reported in 2003). An interesting statistic is that 80% of top ten attack originating countries are located in the Asia pacific region. Emphasis is placed on regional cooperation (APCERT/FIRST).

Takashi Ishitobi (METI) outlined the vulnerability handling framework in Japan. METI has a computer security early warning partnership with industry. Vulnerability was defined. He argued the necessity for the framework, emphasising the role of government. He then outlined how to facilitate the framework.

Kazuyoshi Matsumoto (National Institute of information Communications Technology, Japan) outlined research activities at Information Security Center (NICT). Information was provided on the organisation of the centre and the Incident Handling System.

12. Cybercrime Legislation and Enforcement Capacity Building Project

The United States (Richard Downing) provided feedback on the second conference of experts in Hanoi August 25-27, which was funded by the US. Mr Downing had submitted a detailed report as an eSTG document. He thanked Vietnam for hosting the event and for providing enormous assistance in its planning and organisation. There were over 120 delegates from 17 economies. This event focused on legislative development, improving international cooperation in law

enforcement agencies investigations, and models for cooperation between law enforcement and industry.

The Conference flagged possible further work on:

- Training for judges and prosecutors
- Better outreach to business and the public about cybersecurity
- Develop relationships between industry and law enforcement

Australia indicated it is doing some work in that first area (training) and will share its approach and findings at the next TEL.

Mr Downing indicated that direct assistance projects are planned for Chinese Taipei (October 2004), Peru (November 2004) and Thailand (Nov 2004), which makes for a total of six projects.

A one year extension has been requested from TEL for this project (until December 2005). However, it is emphasised that the budget will not be extended. Only six out of the seven direct assistance projects have been accomplished. There are requests from other economies for assistance. There is also a call for a third conference of experts. The US (resources permitting) will undertake two additional direct assistance projects (economies not yet selected) and will seek to have another conference of experts next year. This approach was endorsed by eSTG.

13 Internationalisation of e-security certification

Professor Corey Schou presented on behalf of (ISC)2, the global not-for-profit consortium. In his presentation he outlined their two key globally recognised credentials – CISSP and SSCP.

14. Economy reports

No oral reports were provided.

BUILDING A CULTURE OF SECURITY

15 Rethinking Information Security Strategy and Practices
Microsoft (Meng Chow Kang)

This presentation focused on a security strategy for defensive security., building a fortress around critical information assets and defence in depth. A key theme was: There is no perfect security – it is as strong as the weakest link.

16. Key trends and issues in e-security in the Asia Pacific region
(Joint presentation on behalf of CERTs/CSIRTs)

It was greed at TEL 29 that it is very useful to have a strategic analysis by all the CERTs/CSIRTs of key e-security issues and trends in information security.

Graham Ingram (AusCERT and Chair of APCERT) and Jeff Carpenter (CERT CC) gave a joint presentation. Their presentation is available as a formal document at the website. It focused on online financial fraud - Trojans - spam as an attack vector. They emphasised the need to act in

concert against these attacks. These trends represent long term threats to consumer trust. A host of strategies need to be adopted – not least multi factor authentication.

A panel discussion was held aimed at generating an eSTG view on the presentation and possible areas for action. China, US, Japan, NZ and Korea participated on the panel. They flagged issues such as incident handling differences and language barriers, the importance of cooperation between CERTs, & harmonisation of laws. INTUG suggested there are a number of key stakeholders and made the point that equipment is sold to users which makes users vulnerable.

17. Small business perspective

Online Security Tutorial and guidance for small business

Michael Baker from AOEMA demonstrated many of the features of this online security tutorial package which targets APEC small businesses. It was jointly funded by APEC and Australia. It provides easy to follow practical guidance and training tips for small business.

18. New project proposals/workshops

Ms Monica Ochoa from the TEL Secretariat provided a very useful overview of new project approval processes.

GBDe proposal

GBDe outlined its workshop (half day forum) proposal which had been submitted as a TEL document. It would be self funded. It contains a workshop proposal with two sets of issues/panels: Cyber security business cases; and a second element on the future of the Information Society.

Panel 1: Cyber Security Business Cases
Prospective Speakers: One from government; One from company / private organization ; One from a GBDe member company

Topics:
Company security practices. (security policy, privacy policy and security management)
The responsibility of board members, managers, and employees.
Case examples of security incidents or attacks.

Panel 2: Future of the Information Society
Towards an Ambient, Ubiquitous, Knowledge-based Economy

Prospective Speakers: One from company / private organization; Two from GBDe member companies

Topics:
What a "ubiquitous information society" will mean for APEC economies
The potential impact of RFID as a key technology for the ubiquitous society
Other ubiquitous technologies and their implications (application of IC card, mobile, and broadcast)

GBDe explained that the purpose of this forum is to promote further dialogue between governments and businesses in order to develop global multi-stakeholder perspectives on e-commerce policy.

Japan indicated its support for the proposal. A number of economies indicated that the second element of the proposal was unclear and did not seem to fit with the eSTG's role. GBDe asked that the eSTG deal with the first part. They indicated that they planned to take up the other part of this proposal with the BFSG. On that basis the eSTG supported Panel 1 of the proposal noting that BFSG would be considering panel 2. It was made clear to the GBDe that the eSTG could offer no support for panel 2 as it did not fit with eSTG's role.

AOEMA project proposal – cybersecurity tool

This project proposal had been submitted as a document. It aims to provide a self-paced on line security assessment tool for SMEs and include a training modules. NZ, US and Australia indicated their support for the project, but no specific funding was committed. This will be worked up as a formal project proposal seeking funding.

Spam and Spyware

Spyware: Flowing from a large discussion group that convened at lunch time (1.30pm), it was agreed that a questionnaire would be submitted to interested economies on spyware. It will touch on economies understanding of the issue (in an e-security context) and any regulatory steps that may be being considered.

Spam: Canada expressed concern at the lack of detail surrounding the 2 day spam joint conference proposal. A fairly basic draft proposal had been uploaded late that morning by the US so as to facilitate some discussion. There was a view in the eSTG that there could usefully be a two day program on malicious spam (as the CERTs/CSIRTs described it, spam as a malicious attack vector). It was agreed that the US Canada Australia and NZ would meet the next day to try and flesh out precise details on this workshop with a view to taking it forward to the BFSG. Following that discussion, it was agreed that there was not sufficient time to clarify all the details needed for a tightly prepared proposal to go to BFSG the next day. This was mainly because of the sheer scale and scope of the draft US proposal which involved another APEC group. The small group acting on behalf of the eSTG (including the Chair) agreed that there was undoubted merit in the proposal and encouraged the US to continue to pursue it once a clear final proposal had been drafted and there was support from the ECSG to the details of the joint conference on Spam. There would need to be extensive consultation with economies and, because of the scale/scope of the proposed event, discussions with the TEL and ECSG chairs. The US was also encouraged to think about it being a purely TEL event as a fallback position.

APEC Wireless Workshop Report

A. Background and Discussion

A half day Wireless Security workshop was held at TEL 30. The focus of the workshop was education and awareness raising and offered speakers from business, government, and public safety organizations from approximately half a dozen APEC member economies.

It was co-chaired by Sallie McDonald (U.S. Department of Homeland Security) and Joel Michael Schwarz (U.S. Department of Justice).

The workshop looked at 802.11-based technology (Wireless LANS), and began by explaining the vulnerabilities that exist and why these vulnerabilities are important to be aware of. There were also discussions on securing wireless, the impact of wireless on law enforcement and public safety, wireless in the workplace, as well as a discussion of potential next steps for the TEL in the area of wireless.

During the workshop, the following information was developed:

- According to a survey conducted by Hong Kong, China, it was illustrated that while the number of wireless users is increasing at a great rate, the percentage of those users failing to secure their wireless systems is increasing at a greater rate (71% unsecured wireless users in 2002, versus 79% in 2004).
- Wireless poses a number of law enforcement related problems, such as unlawful sharing or stealing of connections and unauthorized access, as well as concerns with regard to criminals exploiting wireless to act in anonymity and stymie law enforcement investigative efforts.
- Wireless is being deployed in the critical infrastructure arena and, according to a survey conducted by Australia, 64% of private critical infrastructure providers surveyed use wireless in their systems (with 16.6% of those respondents reporting that they believe their operations could be compromised through those wireless connections).
- In the workplace, there is much appeal to using wireless to facilitate business and increase productivity, but much work needs to be done to ensure that systems are being securely deployed, and that employees are not installing unauthorized wireless access points.
- There are small business and individual user issues. As a speaker from Intel explained, there is an apparent disconnect between the wireless security options being offered by businesses and the user needs/understanding of those wireless security options.

B. Possible Next Steps

1. <u>Consumer Education/Business Education</u> – While efforts continue to secure wireless, it is clear from a number of speakers that wireless security currently remains a concern, especially with regard to the small "knowledgeable amateur" user (referred to by Korea as a Group 1 user; a self constructor who installs, operates and monitors the wireless LAN on his own, without an administrator).

<u>Impact on consumers:</u> According to a speaker from Intel, this concern appears to be due, at least in part, to a disconnect between the security features manufacturers chose to include in the wireless products, and the needs/understanding and ease of use of these features by wireless users (especially Group 1 users). This problem was clearly demonstrated by a survey conducted by Hong Kong, which showed that the percentage of users failing to secure their wireless

systems is actually increasing over time (71% unsecured in 2002, as compared to 79% unsecured in 2004).

In addition to difficulties with using the security features included with wireless products, a related problem discussed was that many wireless products are shipped with security features disabled, by default, and therefore users are not even aware of these potential security features (or the threats that these features are designed to protect against).

Impact on business: According to a speaker from the GBDe, wireless is increasingly being integrated into business, and there are security implications that need to be considered, such as proper usage of wireless by employees, unauthorized installation of wireless access points, new vulnerabilities being introduced into a system, etc. During the discussion of next steps, a speaker from Cisco also volunteered that the potential failure of wireless LANs needs to be considered and incorporated into business contingency planning (which could be amended to incorporate plans for fail-over to a wired network when there is a failure in the wireless LAN).

Based upon these issues, it was recommended that further work be considered in the area of both consumer and business education. *Two potential options for future work in the area of education on wireless include:*

a. AOEMA will be proposing the preparation of a booklet on wireless safety, similar to earlier publications such as Safety Net and Safety Mail. This publication will likely include topics such as: a discussion of the various wireless standards; responsibilities of providers and users for securing wireless; security concerns; configuration recommendations for home and office wireless networks.
b. Opening a dialogue between wireless users and wireless manufacturers/distributors, to work toward bridging the apparent gap between the security features that are being built into these products and users' inability to configure and use these features. Within this dialogue, discussion could also be had about the idea of shipping wireless products with security features turned on, by default, and how to make this security more useful, simple to configure, and easy to understand for novice, Group 1 users. As Japan noted during the next steps discussion, we need to develop flexible models to accommodate different user levels, while never losing sight of the fact that it is important to have, at a minimum, easy security set-ups for beginners and the general public. A draft list of potential participants in such a dialogue is appended to the end of this report, as "Attachment A."

2. Economy Self-Examination – One area that became clear from the workshop was that wireless potentially provides significant advantages to criminals who perpetrate their crimes using the Internet, and that it creates new burdens for law enforcement and public safety officials attempting to investigate and prosecute those criminals. For example, a speaker from the United States explained that a criminal could log into a wireless user's network, often without the user's knowledge, and then commit crimes over that connection without leaving any trace, since there would be no authentication by the criminal and wireless access points do not necessarily log information about wireless users (especially when another's wireless connection is used without authorization).

Similarly, it is unclear how wireless might impact an economy's current legal infrastructure, in terms of the substantive laws that criminalize attacks on computer networks and the procedural laws that enable investigations of crimes involving technology (such as laws that permit real-time interception of content). For example, an economy law that makes it illegal to

circumvent security in order to gain unauthorized access to a computer network, could present prosecution difficulties when the network compromised is a home wireless network, and the wireless user does not have security features enabled (due to a lack of knowledge of the features, disabling of those features for ease of use, etc. – all discussed above in Nest Steps number 1).

Finally, Australia's presentation on the results of a survey it conducted on the use of wireless in its critical infrastructure ("CI") sectors illustrated that wireless is indeed being integrated into critical infrastructure systems (64% of CI survey respondents reported using wireless technologies in their systems). Sounding a cautionary note, however, Australia also advised that of those CIs currently using wireless, almost 17% reported that their operations could be compromised through those systems.

Based upon the issues raised, it was recommended that *economies consider performing self assessments on the following three areas and then report back to the e-STG at the next TEL meeting, with an eye toward identifying potential future work in this area*:

a. Self Examination - Impact of wireless on an economy's laws and regulations – could include an examination of: how the use of wireless by criminals could affect enforcement of existing criminal laws, including network crime laws; how, and whether, wireless technologies can legally be used by law enforcement and public safety agencies in conducting investigations; how wireless impacts current procedural laws, including laws pertaining to monitoring of electronic communications; whether economies have regulations (or proposed regulations) that apply to the manufacture, sale or use of wireless technologies.
b. Self Examination - Impact of wireless on criminal investigations and prosecutions – could include an examination of: whether the use of wireless by criminals has posed problems for investigators in tracking and identifying those criminals, and what those problems entailed; whether the use of wireless by criminals has posed problems for prosecutors in terms of bringing cases, including decisions not to prosecute because of evidentiary difficulties or concerns, concerns about lack of knowledge or expertise amongst prosecutors, or the courts; cases involving wireless that have been lost (or dismissed before conclusion of the case) due to a lack of understanding of wireless by judges, courts or other triers of fact, or other complications relating to wireless; case reports and examples of wireless cases that have been successfully prosecuted to conclusion; solutions and unique approaches taken by economies to overcome the challenges posed by wireless.
c. Self Examination - Use of wireless in an economy's critical infrastructure sector – economies might chose to use Australia's survey of its critical infrastructure sectors and modify that survey for distribution to their own critical infrastructures.

3. Development of Principles on the Availability of Wireless Access Point Log Data Essential to Protecting Public Safety

During the presentation by the United States, the workshop discussed some of the challenges that wireless has posed for law enforcement investigations, including the unauthorized/malicious use of wireless LANs to commit crimes, and the lack of logging done by wireless access points, both of which make it difficult to ascertain the identity or location of a person engaged in criminal activity. These problems are likely to compound as economies look to develop and implement wireless area networks (such as wireless coverage for an entire metropolitan area), which could make it more difficult to uncover the identity or location of a criminal using wireless within that metropolitan area.

One idea proposed by Cisco was the idea of developing principles on the types of data that might be useful to log for law enforcement and public safety purposes (and which users might wish to consider enabling when implementing wireless). These principles could also consider the types of data that might be useful to consider (for logging purposes) as economies move forward in implementing wireless metropolitan area networks.

Moving Forward – Temporary Wireless Working Group Between TEL 30 and 31

Because these issues are quite new, and economies are still in the process of digesting all of the information brought out during the wireless workshop, it may be premature to recommend specific actions such as undertaking new surveys, scheduling additional workshops, etc. At the same time, there is a great deal of discussion that can be had about the Next Steps outlined above.

As such, the United States would propose that a temporary Wireless Working Group ("WWG") be formed to hold further discussion on these next steps and to propose future work, if any, needed to move these ideas along. Cognizant of the other APEC-related work in which economies are already engaged, the U.S. proposes that the WWG hold periodic conference calls between this TEL meeting and the next, further flushing out the wireless next steps developed during the workshop, with a goal of reporting back to the next TEL meeting on the results of those conference calls, and proposing future work, if any, that the TEL might consider undertaking in this area. This would also enable the WWG to consult with other multilateral organizations and ascertain what work, if any, they have done on wireless.

This approach was supported by the eSTG. All interested economies and delegates are to be given an opportunity to participate.

ATTACHMENT A

As discussed in Next Steps #1, it was agreed that education and awareness-raising in the area of wireless could be facilitated through a dialogue between wireless users and wireless manufacturers/distributors.

Groups that might be useful to consider in this dialogue could include:

1. Wireless user groups
2. Manufacturers of wireless products
3. Security consulting firms that specialize in providing consulting services to businesses on wireless implementation (highlighting common problems that are raised, and advice given to avoid those problems)
4. Representatives from various industry wireless organizations including, for example, the Wireless Coalition, the Broadband Wireless Internet Forum, the Private Wireless Coalition, etc.
5. Representatives from technical support advocacy groups (or Technical Support divisions from organizations that manufacture wireless products) (to discuss common problems/mistakes/concerns they receive from wireless users)
6. Consumer advocacy groups
7. AOEMA (on the information gathered about wireless use amongst SMEs)
8. Economies that have done work/research on this topic (such as Hong Kong's survey of wireless usage), economies that are considering implementing regulations for wireless, or economies that are considering implementing wireless metropolitan area networks.
9. Academicians that have looked into the issues surrounding wireless use (including the security problems, behavioural issues regarding use or disabling of security features, etc.)

CSIRT Workshop on Vulnerability Handling
APEC TEL 30 – September, 19 2004 - Singapore

Workshop chaired by Ms Liesyl Franz, United States

Theme:

Raising awareness on the importance of vulnerability handling for computer security incident response teams with national responsibility and government cyber security policy makers.

This theme reflected the growing need for computer security incident response teams (CSIRT) and government cyber security policy makers to recognize the issues around cyber vulnerability disclosure and address them appropriately. This workshop built on the previous CSIRT workshops held in conjunction with the APEC TEL meetings in Hong Kong (29), Chinese Taipei (28) and Malaysia (27) on the need for and key components of computer security incident response teams. Our intention was to provide APEC economies' policy makers and computer response teams with some ideas about how to make progress in this important area in today's global, digital, and interconnected community.

The agenda for the workshop included:

- Introduction of vulnerability handling from CERT/CC including definition and description, discussion of impact on economies and critical infrastructures, and vulnerability handling experiences;

- Panel on CSIRT vulnerability handling experiences/case studies, including presentations from JPCERT/CC, KRCERT/CC, and AUSCERT;

- Panel on vendor vulnerability handling experiences/case studies, including presentations from Cisco, the Japan Electronic Industry Technology Association (JEITA), and Microsoft; and

- Discussion panel among APEC economy CSIRTS, including JPCERT/CC (Japan), KRCERT/CC (Korea), AUSCERT (Australia), MYCERT (Malaysia), SingCERT (Singapore), CNCERT (China), HKCERT (Hong Kong, China), and CERT/CC, as well as vendors, including Cisco, JEITA, and Microsoft.

Results:

- Information and discussion about vulnerabilities and their impact on our economies and critical infrastructures, as well as challenges and problems faced in vulnerability handling.

- Identification of some steps that APEC economies can take to move forward on vulnerability handling:

    1. Need for CSIRTs designated by their economies to build and enhance vulnerability handling capabilities;
    2. Need for CSIRTs to cooperate with each other to share information and fill gaps where capability and environments vary; and

    3. Need for CSIRTs to work with their respective vendors and CIP organizations appropriately to address vulnerability handling; and

    4. Need to continue to find additional ways to build trust. The workshop participants recognize that vulnerability handling is a sensitive issue, but it is crucial to proactively

protect networks and critical infrastructures and to defend against potential attacks. To work with all the stakeholders, it will require continued efforts to establish trust in this environment building on trust occurring through daily and periodic CSIRT interactions and through workshops such as these.

Recommendation for Next Steps for ESTG:

- The series of APEC TEL CSIRT workshops (4) brings awareness and education effort for ESTG to a logical close. Therefore, the United States proposed bringing the CSIRT component into the ESTG agenda on a permanent basis, with a work program to be agreed by the ESTG. The United States also suggested that the themes of international cooperation and building trust could drive a work program for the CSIRT component of the ESTG.

This recommendation was discussed in the eSTG and endorsed.