行政院及所屬各機關出國報告
（出國類別：國際會議）

APEC/SCSC「重大基礎建設及維護系統標準化計畫」訓練研討會報告

服務機關：經濟部標準檢驗局
姓名職稱：饒玉珍/技正
派赴國家：越南河內
出國期間：97年8月26日至97年8月28日
報告日期：97年10月

出席 APEC/SCSC「重大基礎建設及維護系統標準化」訓練研討會簡要報告

會議名稱（含英文縮寫）	「重大基礎建設及維護系統標準化」訓練研討會
會議時間	2008 年 8 月 27 日
所屬工作小組或次級論壇	標準及符合性次級委員會（SCSC）
出席會議者姓名、單位、職銜	饒技正玉珍（標準檢驗局）
聯絡電話、Email	02-33435165 yuchen.rao@bsmi.gov.tw
本次會議討論要點及重要結論（含主要會員體及我方發言要點）	1. 為縮短亞太地區標準間之落差，並發展有助於安全相關標準之框架，俾便在緊急期間得以協助處理亞太地區重大基礎建設和維護系統，請 APEC 各會員經濟體執行內部調查問卷。 2. 調查問卷及相關參考文件 PDF 版置於澳洲 StanCert 網站 http://www.stancert.com/cisss.html。 3. 調查對象包括國內能源、水力、電信、運輸交通、金融、健康安全、食品衛生及政府機關等約 200 位代表，問卷調查期間至本(97)年 12 月 1 日止。
後續須辦理事宜	請國內各相關單位及機關(構)逕上網填寫調查問卷，並將國內調查情形彙整提交主政國澳洲。
建議資深官員就相關議題發言要點（★請務必依會議最新討論情形提建議，並提供簡要中英文說辭，以 1 頁為限）	無
檢討與建議	無

※此表請於會議結束後當日完成，並即以 Email 寄至外交部、貿易局出席會議人員電子郵件信箱。

※14 號字標楷體，行距固定行高 20 pt，請自行調整表格大小。

目 次

壹、緣起及目的

有鑑於APEC各會員經濟體注意到亞太區域易受到安全威脅，如天然災害、傳染性疾病或犯罪活動等而帶來人類生命及經濟之損失，爲期能有及早因應措施，因此於2007年APEC貿易與投資委員會(CTI)第三次會議上，企業諮詢委員會（ABAC）提案，希望能經由較佳的檢驗測試及一致性作法，提出必要的訊息、建議及指導標準，有效保護各國之重大基礎建設，以協助企業界渡過自然災害及非常時期。而本提案也獲得APEC標準與符合性次級委員會(SCSC)及貿易與投資委員會(CTI)的認可。「重大基礎建設及維護系統標準化」計畫係由APEC會員經濟體澳洲提出，且獲得APEC Support Fund 經費補助。

APEC/SCSC項下之「重大基礎建設及維護系統標準化」計畫由澳洲主政，協同辦理之會員經濟體有紐西蘭、越南、祕魯。該計畫主政會員體將先就APEC會員經濟體如何執行內部調查，並提供指導文件，且於計畫期間提供指導及支援各會員經濟體完成內部調查。本計畫將提出相關標準之發展框架，俾便在緊急期間得以協助處理亞太地區重大基礎建設和維護系統，調查對象包括國內能源、水力、電信、運輸交通、金融服務、健康安全、食品衛生及政府機關等。

爲讓各APEC會員經濟體瞭解如何執行內部調查，主辦會員體澳洲邀請各會員經濟體之主要聯絡者(key national contact point)出席越南河內於2008年8月27日召開之訓練研討會。

貳、出席會議重點實錄

一、議程

APEC/SCSC項下之「重大基礎建設及維護系統標準化計畫」訓練研討會假越南河內於2008年8月27日舉行，並由主政國澳洲邀請各APEC會員經濟體之主要聯絡者(key national contact point)代表參加。

本研討會由澳洲StanCert公司之執行長Mark Bezzina先生主持，有來自汶萊、香港、印尼、馬來西亞、紐西蘭、巴布新幾內亞、菲律賓、新加坡、泰國、美國、越南、加拿大、澳洲及我國等經濟體參加。

為期一天的研討會，時間非常緊湊，首先由計畫主持人Mr. Bezzina針對整個計畫之背景、目的、執行方法及時程等進行說明，下午則依據澳洲所草擬的問卷進行3個分組，針對各經濟體國內現況、面臨困難與問卷調查方式充分討論及交換意見後，綜合研討成果進行全體討論，最後歸納並總結提出具體建議，澳洲將對所提出之建議做最後的問卷修正，修正後之問卷將置於澳洲StanCert網站 http://www.stancert.com/cisss.html，由各APEC會員經濟體代表填寫，問卷調查時間自2008年10月1日至12月1日。

二、會議討論之情形

本計畫的主要目的為：(1)確認並詳細說明與保護重大基礎建設有關的議題、障礙及解決方法，並確認使用者對確保重大的基礎建設相關標準重要性的認知；(2)確認並就重大基礎建設之使用者和經營者所要求的標準列出優先次序，並確認現有標準與前揭人員所需標準的差距；(3)就如

何填補標準間的落差提出建議，並發展出有助於確認和分類安全標準的一個制定框架藍圖。

本計畫所述及之重大基礎建設包括電力供應、水、電信、金融服務業、公共事務、運輸、健康安全、政府部門、食品衛生、基本製造業等。這個計畫將與ISO/IEC/ITU安全政策建議小組（SAG-S）及ISO TC223社會安全連結及合作。

針對問卷內容、設計形式、填寫方式、邀請受訪者之身分、語文、名詞定義等問題於會中分成3個小組進行討論及交換意見，而歸納提出具體建議，主政國澳洲將對所提出之建議做最後的問卷修正，並將修正後之問卷及相關資料置於澳洲StanCert網站之「重大基礎建設及維護系統標準化」計畫專屬網頁(http://www.stancert.com/cisss.html)，以便作爲各會員經濟體填寫問卷之參考。

各會員經濟體之主要聯絡人的責任爲瞭解整個計畫之進行，並協助計畫管理團隊，以完成國內約200位代表之執行調查問卷。

三、計畫提出

計畫最後將由主政國澳洲提出一份報告，內容包括(1)確認並詳細說明與保護重大基礎建設有關的議題、障礙及解決方法，並確認使用者對確保重大的基礎建設相關標準重要性的認知；(2)確認並就重大基礎建設之使用者和經營者所要求的標準列出優先次序，並確認現有標準與前揭人員所需標準的差距；(3)提出APEC各會員經濟體填補標準間的落差之建議，並發展出有助於確認和分類安全標準的一個制定框架藍圖。

參、結語與感想

「重大基礎建設及維護系統標準化」計畫係由APEC會員經濟體澳洲主政，本次研討會目的在於緊急期間能有效協助處理亞太地區重大基礎建設和維護系統，而縮短亞太地區標準間落差及發展相關安全標準框架，所進行之內部調查問卷訓練。

由於這是一份由主政國澳洲針對在緊急情況及災害發生時，期對基礎建設及系統之維護能有一致性的處理及管理方式，以減少對國內經濟的影響，並有助於提高亞太地區重大基礎建設之互操作性和相容性所設計出來的問卷，雖然問卷內容的設計對各個會員經濟體不盡合適，但仍可以感覺到澳洲爲此計畫之用心及爲亞太地區安全所付出之努力。

由於此份問卷內容涉及非常廣，或許對每個業務單位或受訪人員而言，感覺到僅涉及到問卷的某部分，而無法完全填寫，或者是英文問卷，填寫有困難等等問題，但身爲國內「重大基礎建設及維護系統標準化」計畫之主要聯絡人，將儘量配合主政國澳洲，並協助計畫團隊，以完成國內約200位代表之執行調查問卷。

Critical Infrastructure and Support Systems Standardisation Project Training Workshop
Sheraton Hanoi Hotel
Song Thao - Song Lo room (Please check room at hotel desk)
Wednesday, 27 August 2008, 9.00 – 5.00 p.m.
(8.30 a.m. registration for 9.00 a.m. start)

Time	Duration	Agenda item	Session	Output
8:30	30	Registrations		
9:00	10	Session 1: Welcome and introductions	• Welcome • Housekeeping	Presentation
9:10	10	Session 2: Structure of the workshop	• Context & Purpose of Workshop • Workshop structure • Protocols & Outputs	Presentation
9:20	40	Session 3: Overview of CISSS Project	• Overview • Key documents • Questions	Presentation
10:00	15	Session 4: Getting to know each other	• Exercise to facilitate interaction between all participants during the day and ongoing networking	Introductions and opportunity for ongoing networking and peer support
10:15	30	Morning tea		
10:45	30	Session 5: Snapshot of Australian Security Standards and Support Systems survey results	• Overview • Changes to Security Standards Framework incorporated into approach for CISSS project • Questions	Presentation
11:15	15	Session 6: Role and responsibilities of key national contact points (NCPs)	• Introduction and overview • Questions	Presentation
11:30	30	Session 7: CISSS online survey tool Part 1	• Introduction and overview • Questions	Presentation
12:00	30	Session 8: CISSS online survey tool Part 2	• Practical experience with completion of the online survey tool (small groups)	Small group exercise
12:30	30	Session 9: Standards inventory and consideration of gaps	• Overview • Develop inventory of relevant standards related to security • Discussion of any gaps	Presentation and large group discussion
01:00	60	Lunch		
02:00	30	Session 10: Summary of morning sessions Overview of afternoon sessions	• Summary of morning sessions • Feedback on online tool • Other issues • Overview of afternoon sessions	Presentation and large group discussion
02:30	30	Session 11: Reviewing the survey tool	• Sharing ideas on how to improve the survey tool and tailor it to the needs of the audience (small groups) • Feedback ideas to larger group	Small group exercise and summation
03:00	30	Session 12: Marketing and identifying survey respondents	• Sharing ideas on marketing the survey and identifying potential respondents • Feedback ideas to larger group	Small group exercise and summation

Critical Infrastructure and Support Systems Standardisation Project Training Workshop
Sheraton Hanoi Hotel
Song Thao - Song Lo room (Please check room at hotel desk)
Wednesday, 27 August 2008, 9.00 – 5.00 p.m.
(8.30 a.m. registration for 9.00 a.m. start)

Time	Duration	Agenda item	Session	Output
03:30	15	Afternoon Tea		
03:45	15	Session 13: Implementation	• Identify the key implementation activities for the survey	Large group exercise and summation
04:00	30	Session 14: Trouble Shooting	• Sharing ideas on what could go wrong and solutions to these • Feedback ideas and solutions to larger group	Small group exercise and summation
04:30	15	Session 15: Role of Project Team	• The role of the Project Team in supporting the key national Contact Points and their deputies • Other ideas on how the Project Team can assist • How can you support the Project Team?	Presentation, large group discussion and summation
04:45	15	Session 16: Summary and confirmation of future actions	• Summary • Next steps • Thanks	Presentation and discussion
05:00		Close		

Critical Infrastructure and Support Systems Standardisation Project Training Workshop
List of Delegates

First Name	Surname	Country	Organisation
Nor Imtihan Hj Abd	Razak	Brunei Darussalam	Ministry of Development
Wayne	Perrin	Canada	Standards Council of Canada
Ian	Clark	China	Security Bureau, Hong Kong SAR Government
Yu-Chen	Rao	Chinese Taipei	The Bureau of Standards, Metrology and Inspection
Nurasiah Saleh	Samhudi	Indonesia	National Standardization Agency of Indonesia (BSN)
Rafaiq Bakri	Zakaria	Malaysia	Standards Malaysia
Erin	Alderton	New Zealand	Standards New Zealand
Reuben Harokaveh	Harokaveh	Papua New Guinea	National Institute of Standards & Industrial Technology
Carmencita	Magno	Philippines	Bureau of Product Standards, Department of Trade and Industry
Lee Fang	Lim	Singapore	SPRING Singapore
Prasong	Prayongpetch	Thailand	Office of National Accreditation Council, Thai Industrial Standards Institute
Dean	Larson	USA	Larson Performance Consulting, LLC
Vu	Van Hong	Viet Nam	Standards and Quality (STAMEQ), Vietnam
Zhongqiang	Li	China	China National Institute of Standardization
Ingrid	Maciel	Mexico	Dirección General de Normas

Critical Infrastructure and Support Systems Standardisation Project

STANDARDS Australia

StanCert

Session 1

Welcome and introductions

StanCert

Welcome

- Vu Van Hong
- Deputy Director of International Cooperation Department
- Directorate for Standards and Quality (STAMEQ), Vietnam

StanCert

Presenter

Mark Bezzina
Managing Director
StanCert Pty Ltd
Australia

bezzina@stancert.com

StanCert is managing the project on behalf of APEC and Standards Australia

StanCert

Introduction: Mark Bezzina

- Previously Executive Director of Australia's National Standards Body - Standards Australia
  - written and managed the development of over 100 standards
  - set up innovative regulatory regimes and certification systems, and implemented management and compliance systems in a range of organisations
- Master of Business Administration (MBA) degree from Macquarie Graduate School of Management, Sydney and Bachelor of Business (BB) from the University of Technology, Sydney

StanCert

Introduction: Mark Bezzina

- Founding Executive Director of the Society for Knowledge Economics, founder of the National Centre for Security Standards, Chairman and founder of the BizDex Information Management initiative and immediate past Chairman of the Biometrics Institute
- Member of the Australian Services Roundtable, Australian Industry Group, Australian Business Foundation, , the St James Ethics Centre and the Edmond Rice Business Ethics Initiative
- Sits on several high-level government and industry committees

StanCert

Other Project Contacts

Project Supervisor:
Karen Hitchiner,
Manager International Development, Standards Australia
Email: karen.hitchiner@standards.org.au

APEC Project Sponsor:
Brian Phillips
Manager, Standards & International Liaison
Industry & Small Business Policy Division
Department of Innovation, Industry, Science and Research
Email: brian.phillips@innovation.gov.au

Lead Consultant:
Clare Morrison
StanCert Pty Ltd
Email: cmorrison@stancert.com

StanCert

Housekeeping

- Venue information and facilities
- Time keeping
- **Evaluation questionnaires (all) and APEC Per Diem forms (APEC travel eligible economies) to be completed and handed in at the end of the workshop**

StanCert

Session 2

Structure of the workshop

StanCert

Structure

See detailed schedule (any questions?)

Part 1 – Scene setting

Sessions (1, 2, 3, 5, 6, 7) Background

- Session (4) Getting to know each other

Part 2 – Putting it all together (Action)

- Sessions (8, 9, 10, 11, 12, 13, 14, 15) Active learning
- Sessions (10,16) Summary and Next steps

StanCert

Protocols

- All ideas are good ideas
- Support each other
- Help the group to:
  - stick to time
  - stick to schedule
- Yellow tags – ideas or areas to cover

StanCert

What do you want to learn today?

This is your opportunity to learn how to conduct the survey in your own country

- What do you think needs to be covered during this workshop?
  - Sharing ideas
  - Other checkpoints (Session 10, 16) to answer questions, clarify issues

StanCert

Questions and comments

StanCert

Session 3

Overview of CISSS Project

StanCert

Context and purpose

The Project aims to:

- create an integrated standards environment
- identify standards that need to be updated
- identify gaps in existing standards
- seek agreement on priorities

StanCert

Overview

Sponsored by

Asia-Pacific Economic Cooperation (APEC)

the premier forum for facilitating economic growth, cooperation, trade and investment in the Asia-Pacific region

Standards Australia

an independent, non-government organisation that is recognised as the peak non-government standards developing body in Australia

StanCert

Co-sponsoring Economies

- Vietnam
- Peru
- New Zealand

StanCert

Supported by

- APEC Business Advisory Council (ABAC)
- APEC Sub-Committee on Standards and Conformance (SCSC)
- Pacific Area Standards Congress (PASC) (voluntary, independent organization of Pacific area national standards organizations)

StanCert

Overview

- The impetus for this Project came from the need to refocus on security in the Asia Pacific Region following events such as natural disasters and criminal activity in recent times
- It builds on the outcomes of a similar initiative that was undertaken in Australia
- The aim is to identify where gaps exist in the existing standards and recommend priorities for the development of future standards

StanCert

Overview

- The pressure on security professionals and businesses to manage and respond appropriately to security threats has never been greater
- Good security standards provide essential information, advice and benchmarks to guide reasonable and prudent decisions
- Fundamentally, standards articulate best practice

StanCert

Solution oriented approach

- Solution oriented approach in relation to barriers identified relating to protecting critical infrastructure
- A blue-print will be provided for the development of a standards framework for identifying and categorising security standards

ShanCert

All hazards approach

- An all hazards approach is being taken to threats
  - includes security threats such as where someone has the capability, intent and opportunity to exploit a vulnerability to do harm
  - and accidents and natural disasters that may also cause inadvertent harm due to the existence of vulnerability
- Multiple risks can be dealt with by effective and integrated treatments, such as standardised products and services
- Standards can be developed in a modular fashion or in such a way as to not cause additional vulnerabilities by describing key aspects of security that can form the basis for new attacks

ShanCert

Benefits to APEC Member Economies

- A more consistent approach to security along with emergency and disaster management in the APEC region
- The promotion of security standards and systems capacity which support business as well as critical infrastructure in times of emergency, helping to minimise impact on economies.
- Harmonisation of related standards across the APEC region, which will help improve the interoperability and compatibility of systems related to securing critical infrastructure

StenCert

Benefits to APEC Member Economies

- Improved technical capacity through assistance in ascertaining key areas of standardisation focus so that programs may be targeted for the development of security standards
- The capacity to make more informed choices about effective security solutions through better access to information on tested and consistent methods to protect critical infrastructure

StenCert

Benefits to owners and operators of critical infrastructure

The Project will provide invaluable assistance and efficiencies to the owners and operators of critical infrastructure

- It will help to prevent the need to redevelop or reinvent approaches to solving the same problems many times over
- It will provide simple authoritative guidance and a consolidation of existing good industry practice
- It will assist in decisions about the purchase and specification of quality security products and services

A very important aspect of this project is that it needs to be supported and driven by the owners and operators of critical infrastructure

StarCert

Benefits to owners and operators of critical infrastructure

Standards identified under this project will assist the owners and operators of privately owned critical infrastructure to:

- provide adequate security for their assets
- actively apply risk management techniques to their planning processes
- conduct regular reviews of risk management plans
- report any incidents or suspicious activities to the police
- develop and regularly review business continuity plans, and
- participate in any exercises to test plans conducted by government authorities

StarCert

Standards

Standards are only useful if they are

- needed
- properly prioritised, resourced and developed through an open, transparent and consensus based process
- delivered in a reasonable time frame
- practical and pragmatic
- integrate with other standards
- understandable
- well supported and maintained

SecCert

Examples of Standards

Basic

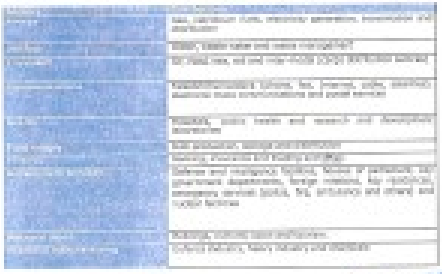
- Fire
- General building, plumbing and electrical
- IT applications and telecommunications
- Blast resistance
- Emergency
- Dangerous goods
- Personal protective equipment
- Emergency power supplies

Security specific

- Doors, windows, screens, grilles, gates and fences
- Locks and seals
- Security risk management
- Guards and patrols
- Safes and strong rooms
- CCTV
- Intruder alarms
- ISMS
- Cryptography

SecCert

Elements of Critical Infrastructure



StarCert

Drivers

- The Critical Infrastructure and Support Systems Standardization Project is necessary because there is a very real need for simple and agreed standards to protect infrastructure
- This guidance is necessary due to the many drivers for security standards that are shown in in the following diagram

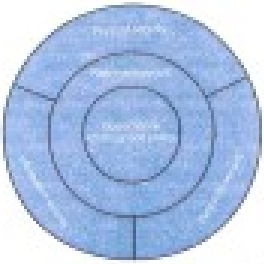
StarCert

Drivers for security standards

- Demand to manage security risks and compliance to protect brands and the community
- Transfer of infrastructure from public to private companies
- The need for documents with authority that have been developed through a formal process of openness, transparency and consensus
- The need for documents developed by an organisation(s) not bound by any jurisdiction
- The need for simple and agreed guidance
- The heightened threat of terrorist attack
- Community concerns about security and privacy
- Regulation (SOX 404?)
- Demand for food and supply chain security
- Demand for international assurance confidence and interoperability
- The need for collaboration in the development of systems

ShariCert

Integrated Security



ShariCert

Project methodology

Project management

- Preparation
- Capacity building
- Consultation
- Analysis and validation
- Reporting and communicating results

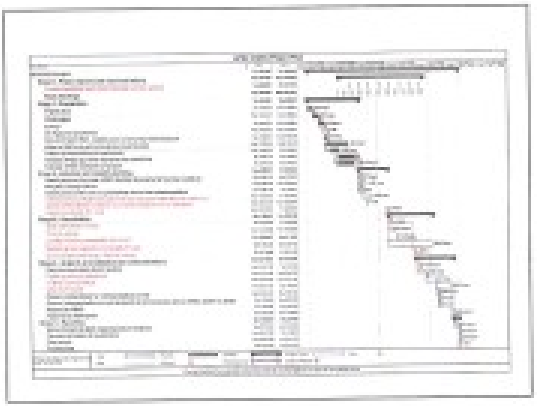
Approach is based on methodology used in a similar project previously undertaken in Australia

StanCert

Project outputs

- An outline of some of the issues, barriers and solutions related to protecting critical infrastructure and identifying user perceptions of the importance of standards related to securing critical infrastructure
- A suggested list of the standards required by the owners and operators of critical infrastructure and the identification of gaps between existing standards and the needs of the owners and operators of critical infrastructure
- Clear recommendations on how the gaps in standards may be addressed and a blue-print for the development of a standards framework that is essential in identifying and categorising security standards

StanCert



Survey

- Security objectives, barriers and solutions
- Common approaches supporting security processes
- Priorities for types of security standards
- Priorities for specific security standards
- Improving the implementation of security standards
- The "ideal" security standard
- Other comments or feedback

SlanCert

Key documents and survey tool

- Background paper
- Project plan
- Online survey tool:
  http://www.starcert.com

A hard copy .PDF version of the survey tool will be made available on request for reference and in case of technical issues

StarCert

Security of data

- SSL encryption will be added to the survey instrument before it goes live
- SSL is short for **Secure Sockets Layer**, and it is a protocol initially developed for transmitting private documents or information via the Internet. It essentially works through a cryptographic system that secures a connection between a client and a server
- Many websites use this protocol to obtain confidential user information

StarCert

Security of data

How does the SSL encryption work?

- The survey link and survey pages will be encrypted during transmission
- The survey responses will be encrypted as they are delivered
- Exports of data to the project team will be delivered in an encrypted format

The level of encryption is **Verisign certificate Version 3, 1024 bit encryption**

SlanCert

Data analysis and reporting

- The data will be collated, analysed and reported across the APEC region (all responses)
- The data will also be reported by APEC Member Economy providing there are sufficient responses
- Care will be taken to ensure the confidentiality of individual respondents
  (As the categories are broad, we do not anticipate that this will be an issue)

SlanCert

Session 4

Getting to know each other

- Group exercise

Getting to know each other

Objective:

- To meet and engage with each other
- Energiser

This exercise aims to introduce participants because the project relies on delegates networking with and supporting each other

Exercise Instructions

1) Rearrange chairs into 2 rows facing across table
2) Participants are seated
3) Introduce yourself to the person opposite who responds by introducing him / herself.
4) Exchange business cards
5) The people in one of the rows move to the next chair on the signal (Decide which row will move)

SlanCert

Getting to know each other

Introduction example script:

- Hello, I am .....
- I work for 'X organisation' in the position of .....
- And you are ?
- I am pleased to meet you. May we exchange business cards? Thank you

SlanCert

Morning tea

Opportunities to get to know each other better during the breaks

ShanCert

Session 5

Snapshot of Australian Security Standards and Support Systems survey results

ShanCert

Security standards and support systems standardisation project (4S) - Australia

The 4S project aimed to address the stated role for Standards Australia in the Critical Infrastructure Protection National Strategy (Version 2, 13 March 2004):

> *"Standards Australia should promulgate standards on risk management, corporate governance, business continuity and security"*

This recommendation flows out of the Business-Government Task Force on Critical Infrastructure report (May 2002) that recommended:

> *"the Commonwealth should develop models of good critical infrastructure assurance, taking into account relevant standards, in consultation with the private sector and the States and Territories"*

SiamCert

Project Objectives

- Describe some of the issues, barriers and solutions related to protecting critical infrastructure
- Identify the importance of standards to securing critical infrastructure
- Identify and prioritise the standards required by the owners and operators of critical infrastructure
- Identify the gaps between existing standards and the needs of the owners and operators of critical infrastructure
- Make recommendations on how the gaps in standards may be addressed
- Develop a blueprint for the development of a security standards framework that would assist in identifying and addressing security standards

SiamCert

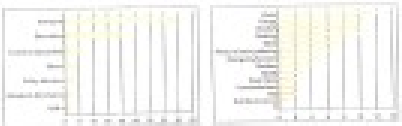
Groups consulted

- National Centre for Security Standards - NCSS
- Critical Infrastructure Advisory Council - CIAC
- Banking & Finance IAAG
- Communications IAAG
- Emergency Services IAAG
- Energy IAAG
- Food Chain IAAG
- Health IAAG
- Icons & Public Gatherings IAAG
- Transport IAAG (Aviation, Rail and Maritime)
- Water Services IAAG
- Built Environment DAG
- CIP Futures DAG
- IT Security DAG
- Other groups as necessary

StanCert

Survey respondents

There was a total response rate of 78. This represents a response rate of approximately 37%

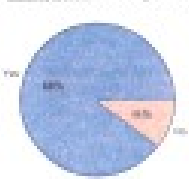


Analysis was conducted across all sectors and within sectors where there was a reasonable response rate

StanCert

Overcoming Security Barriers

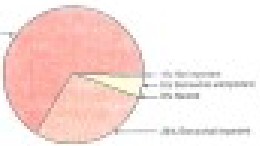
Question:
Would the solutions to overcoming these barriers involve adopting a common approach or standard?



StanCert

Importance of Standards

Question:
How important do you believe common and agreed approaches, standards, methods, protocols and procedures are to improved security?

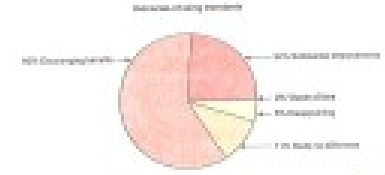


StanCert

Experiences in using Standards

Question:

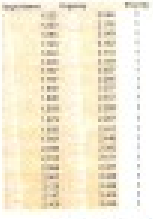
In your experience what has been the outcome of using these standardised business processes and systems?



SterCert

Priority 1 Standards

31 standards were identified as priority 1; these are listed below along with their urgency and importance score. A low score denotes high importance or urgency.



SterCert

Key issues and barriers

- The lack of industry specific security standards or security development frameworks
- A lack of funding and resources to properly manage security
- The poor standards of security guards, training and their morale
- A limited understanding of the specific nature of the security threat to industry and consequently how best to prepare for it
- The difficulty in protecting infrastructure spread across the country
- The threat of identity theft and the complexity of identity management

ShanCert

Solutions

- The development and implementation of a formal security standards framework
- A clear government strategy to address the issue of communication and sharing of information – significant progress has been made on this aspect as a result of the creation of the TISN
- Greater involvement of police and other law enforcement agencies in helping with the protection of remote infrastructure
- Strengthening of security clearance standards
- The development of stronger security training, licensing and accreditation standards for security guards
- Increased government funding to develop, implement, educate and enforce security plans and the recognition by government of the resource implications for the security industry

ShanCert

Desirable attributes of a framework

- Identify broad areas of security standards
- Be simple and communicable
- Provide the basis for categorising, managing the scope and taking stock of existing standards
- Help identify gaps and priority areas
- Be supported by key stakeholders and provide alignment with other existing frameworks such as the PSM
- Be widely used, openly available and unencumbered by intellectual property protection

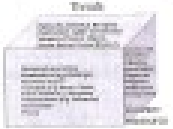
StanCert

Suggested framework coverage

[illegible]	[illegible]	[illegible]
Employees and organisational culture	Plant and property	Informational assets includes such things as records, intellectual property, know-how, alliances, partnerships and networks. Transactions may be stored or transmitted in physical form such as hardcopy documents or in bits and bytes (logical form) such as in IT applications, databases and the like
[illegible]	Capital and financial	
Customers and suppliers	Operational such as process capability. This includes access to energy, raw materials and other required resources.	
The community	Reputation, goodwill and public confidence.	

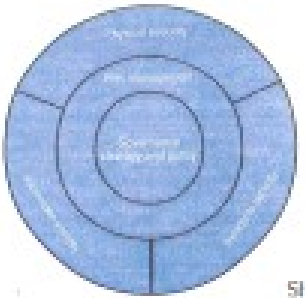
StanCert

Frameworks investigated



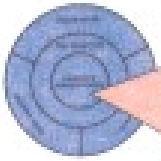
SlanCert

Integrated security framework



SlanCert

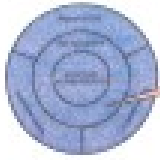
Framework



- Governance
- Board and senior management buy-in
- Security policy
- Security management objectives and targets
- Systems for the categorization of tangible and intangible organizational assets
- Legal compliance management processes
- Communications and media management processes
- Systems audit and assessment processes
- Management review mechanisms
- Continuous improvement mechanisms
- Outsourcing and purchasing security
- Purchasing policy - security requirements in contracts
- Review, audit and assessment
- Reporting incidents and issues management
- Legal issues and steps to report to external authorities

SlanCert

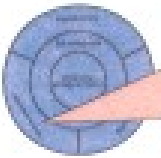
Framework



- Security intelligence gathering
- Risk management systems
- Business continuity management
  - Emergency response
  - Continuity response
  - Recovery response

SlanCert

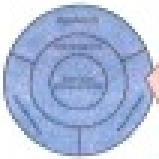
Framework



- Integrated system for the management of information security (17799)
- This element deals with the confidentiality, integrity and availability of information and encompasses such things as:
  - Document, data and records control
  - Security of networks
    - Hardware
    - Software
    - Communications
    - Supporting processes

SlanCert

Framework

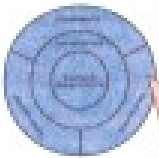


This element encompasses:

- Occupational health and safety
- Pre-employment screening
- Privacy
- Administrative records
- Security roles and responsibilities
- Induction and training
- Disciplinary procedures
- Identity management
- Access control (employees and other)
- Protecting individuals in the workplace, working from home or working overseas

SlanCert

Framework



- Integrated systems for the management of physical security
- Physical security standards include:
  - Access to security advice from professionals
  - Security equipment requirements
  - Site selection and design security
  - Building, facility and event security
  - Perimeter security
  - Lighting
  - Alarms
  - Safes and strong rooms
  - Guards, patrols and control rooms
  - CCTV
  - Locks, doors, windows etc

StanCert

Session 6

Role and responsibilities of key national Contact Points (KNCPs)

StanCert

Role and responsibilities of KNCPs

- Attend the one-day project training workshop
- Keep informed about the project, including its scope and objectives
  - Review correspondence from the project team
  - Respond in a timely manner to communications (check emails)
  - Follow instructions given
- Be familiar with the content of the online survey tool and supporting materials
- Provide ongoing information and training to the deputy on all aspects of the project
- A commitment of time and effort until approximately late December 2008, after which collation and analysis of the survey results will commence

StarCert

Role and responsibilities of KNCPs

- Identify approximately 200 representatives in security related areas to participate in the survey and provide contact details for these individuals to the project management team
  - Based on the Australian experience we can expect a response rate of about 30%, i.e. 60 per APEC Member Economy if the target of 200 is reached
- Follow up respondents
- provide ongoing support and advice to survey participants with the assistance of the project management team

StarCert

Role and responsibilities of KNCPs

- Request respondents to complete the survey using the online survey tool via the StanCert website: www.stancert.com (button linking to survey and background information will be on home page)
- If a respondent has difficulty accessing the survey refer this to project team

StanCert

Role and responsibilities of KNCPs

- Network and help each other
  - share ideas
  - offer support and encouragement

StanCert

Reporting

Provide fortnightly reports on progress to project team

No. persons approached to participate	Gender breakdown M F	No. persons agreed to participate	No. followed up	Comments

Any other suggestions?

StanCert

Session 7

CISSS online survey tool Part 1

StanCert

CISSS online survey tool Part 1

- Introduction
- Online demonstration
  - Overview
- Questions

ShenCert

Session 8

CISSS online survey tool Part 2

ShenCert

CISSS online survey tool Part 2

- Practical session:
  Completing the online survey tool

- Divide into 3 small groups
- Elect recorder and presenter for each group
- Participants to record any issues/comments in a PowerPoint slide for discussion
- Suggestions should be specific (page number, question) and offer solutions
- Everyone should try to complete the form online
- Each group presents issues/comments to larger group

SteriCerf

Session 9

Standards inventory and consideration of gaps

SteriCerf

Standards Inventory

- There has been exceptional standards development work undertaken in the various APEC Member Economies and the project can build on this
- There is also legislation in place that may be relevant to the project's objectives

StunCert

Organising standards & Legislation

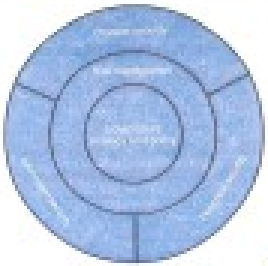
Aim:

To organise relevant standards and legislation under the categories in the Integrated Security Framework

This information to be collected by facilitator for inclusion in the project

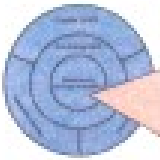
StunCert

Integrated Security Framework



StanCert

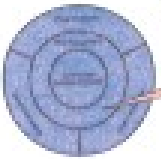
Framework



- Governance
- Board and senior management buy-in
- Security policy
- Security management objectives and targets
- Systems for the categorisation of tangible and intangible organisational assets
- Legal compliance management processes
- Communications and media management processes
- Systems audit and assessment processes
- Management review mechanisms
- Continuous improvement mechanisms
- Outsourcing and purchasing security
- Purchasing policy - security requirements in contracts
- Review, audit and assessment
- Reporting incidents and issues management
- Legal issues and when to report to external authorities

StanCert

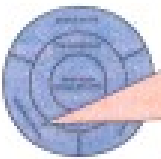
Framework



- Security intelligence gathering
- Risk management systems
- Business continuity management
  - Emergency response
  - Continuity response
  - Recovery response

SterCert

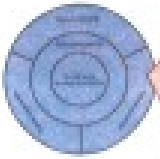
Framework



- Integrated system for the management of information security (ITIMS)
- This element deals with the confidentiality, integrity and availability of information and encompasses such things as:
  - Document, data and records control
  - Security of networks
    - Hardware
    - Software
    - Communications
    - Supporting processes

SterCert

Framework

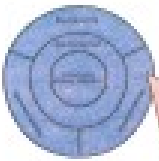


This standard encompasses:

- Occupational health and safety
- Pre-employment screening
- Privacy
- Administrative records
- Security roles and responsibilities
- Induction and training
- Disciplinary procedures
- Identity management
- Access control (employees and other)
- Protecting individuals in the workplace, working from home or working overseas

StanCert

Framework



- Integrated systems for the management of physical security
- Physical security standards include:
  - Access to security advice from professionals
  - Security equipment requirements
  - Site selection and design security
  - Building, facility and events security
  - Perimeter security
  - Lighting
  - Alarms
  - Safes and strong rooms
  - Guards, patrols and control rooms
  - CCTV
  - Locks, doors, windows etc

StanCert

Session 10

Summary of morning sessions

Overview of afternoon sessions

StanCert

Summary and overview

- Summary: morning sessions
- Feedback on practice with online survey tool in last session
- Other issues
- Overview: afternoon sessions

Reminder:

Per Diem and evaluation questionnaires need to be completed, signed and collected before delegates leave the workshop

StanCert

Session 11

Reviewing the survey tool

StanCert

Reviewing the survey tool

- Small groups
- How can the tool be improved?
  - Sharing ideas
- Feedback session

StanCert

Reviewing the survey tool

- Divide into 3 small groups
- Elect recorder and presenter for each group
- Participants to record suggestions in a PowerPoint slide for discussion
- Each group presents suggestions to larger group

StanCert

Guidance for exercise

- Do you understand the content/questions?
- Does the format for the answers work ?
- Should there be additional questions or areas to be covered?
- Suggestions should be specific (page number, question) and offer solutions

StanCert

Session 12

Marketing and identifying survey respondents

StanCert

Marketing and identifying respondents

- Small groups
- Aim:
  Identify 200 respondents per APEC Member Economy = estimated response 30% (60)
  Gender balance
  - Sharing ideas on how to achieve this
- Feedback session

StanCert

Guidance for exercise

- Identify potential respondents through your own networks
- Ask their contacts to identify other potential respondents
- If sending information to targets by email - no spamming
- Direct contacts to StanCert website to access the link to the survey instrument and background information
- Telephone/personal contact and encouragement to participate

StanCert

Guidance for exercise

- Respondents should have relevant background in security related area(s).
- Respondents should have reasonable level of English comprehension as the survey will be in English
- No pressure on participants
- Be polite, supportive and prompt in responding to enquiries (representing APEC)

StanCert

Guidance for exercise

- Refer respondents to project team if unsure of the answer to any questions (important to be consistent when providing information)
- Keep project team informed about progress and any issues

StarCert

Marketing and identifying respondents

- Divide into 3 small groups
- Elect recorder and presenter for each group
- Participants to record suggestions in a PowerPoint slide for discussion
- Each group presents suggestions to larger group

StarCert

Session 13

Implementation

StanCert

Implementation

- Large group discussion
- What are the key steps the NCP should take to implement the project successfully?
  - Sharing ideas
- Feedback session

StanCert

Implementation

Suggestions

- Be proactive
- Be positive
- Communicate efficiently (check emails and respond quickly to enquiries)
- Follow up on contacts
- Market the project

Other ideas?

SternCerf

Session 14

Trouble shooting

SternCerf

Trouble shooting

- Small groups
- What can go wrong ?
- Solutions
  - Sharing ideas
- Feedback session

StanCert

Trouble shooting

- Divide into 3 small groups
- Elect recorder and presenter for each group
- Participants to record any issues/comments in a PowerPoint slide for discussion
- Everyone should try to complete the form online
- Each group presents issues/comments to larger group

StanCert

Session 15

Role of project team

Role of the project team

- Large group discussion
  - Sharing ideas

Role of the project team

The role of the project team is to assist you to conduct the survey successfully in your country.

We will do this by:

- Providing information and regular updates on progress (fortnightly reports)
- Answering your questions and assisting you to answer questions from respondents
- Providing tools as required
- Collating and analysing data

What else can we do to assist you?
How can you assist us?

ShenCert

Session 16

Summary and confirmation
of future actions

ShenCert


Thank you
CLOSE
StarCert

Asia-Pacific
Economic Cooperation

Background Paper

Critical Infrastructure and Support Systems Standardisation Project

A Standards Australia and APEC initiative to promote a better standards infrastructure for security

2008

Authored by: Mark Bezzina

Asia-Pacific Economic Cooperation

Table of Contents

Asia-Pacific Economic Cooperation

Purpose

This background paper has been prepared to communicate to key stakeholders the purpose, methodology and expected outcomes of the Critical Infrastructure and Support Systems Standardisation Project (The Project).

Background and introduction

Standards play a number of important roles in supporting efforts to achieve security. For example standards can be used to:

- promulgate best practices and methodologies for security management.
- specify test methods and parameters to aid in detection of threats.
- specify performance requirements to ensure equipment and systems provide the necessary performance and protection in extreme conditions.

The Project will assist in the development of a proposed framework of standards to address the need to protect critical infrastructure in times of emergencies, whether these be caused by natural disasters or criminal activity.

It will also promote security standards and systems capacity which support business as well as critical infrastructure in government control.

Building technical capacity for developing Asia Pacific Economic Cooperation (APEC) member economies will be a key focus. This capacity building will involve assisting developing economies survey the needs of standards users to ascertain key areas of standardisation focus as well as help target programs for the development of security standards.

The project will also promote the harmonisation of related standards across the APEC region - this will help improve the interoperability, and compatibility of systems related to securing critical infrastructure.

The main beneficiary of this project is the business community of APEC Member economies, as it will contribute to a higher degree of security of critical infrastructure as a result of standardised and tested security management systems needed to meet emergency situations.

The standards identified as a result of this project will also assist member economies and the owners of critical infrastructure to make more informed

choices about effective security solutions through better access to information on tested and consistent methods to protect critical infrastructure.

This project is the result of a proposal by APEC Business Advisory Council (ABAC) presented at CTI III 2007 that the SCSC undertake work to assist with business continuity through periods of natural disaster and other major disruptions.

This proposal was endorsed by the APEC Sub-Committee on Standards and Conformance (SCSC) and the APEC Committee on Trade and Investment (CTI). The agreed proposal stems from similar work recently undertaken by Standards Australia. ABAC presented the proposal at the April 2007 Pacific Area Standards Congress (PASC), where it was also unanimously supported. Australia believes that APEC is the most appropriate organisation to assist in funding the project given the project's regional focus - all APEC members stand to benefit from its outcomes should they choose to participate, particularly developing members for whom the project will be an important capacity building exercise. Australia through its National Standards Body, Standards Australia has committed to contribute significant funding to the project in addition to valuable intellectual property and expertise.

This project will build on other surveys conducted by the ISO/IEC/ITU Strategic Advisory Group on Security (SAG-S) as well as ISO TC 223 that focuses on societal security. Additionally, the project will liaise closely with these two bodies throughout the conduct of the project.

This APEC project proposal is based on a similar initiative funded by the Critical Infrastructure Protection Branch of the Australian Commonwealth Attorney-Generals Department. This earlier project was initiated to complement Australia's critical infrastructure protection arrangements. The Australian Government takes an indirect approach to helping businesses manage their security risks by influencing and encouraging the development of best practice policies and procedures as an alternate to regulation. Standards Australia worked with the Australian Government to examine gaps in the existing library of security standards, and to develop an integrated security standards framework. This has produced several new and revised standards and guidelines applicable to safeguarding critical infrastructure and managing business continuity, and mapped the direction and priority for future standards development.

The Project

Key objectives

The key project objectives are:

1. Identify and detail some of the issues, barriers and solutions related to protecting critical infrastructure and identify user perceptions of the importance of standards related to securing critical infrastructure;

2. Identify and prioritise the standards required by the owners and operators of critical infrastructure and identify the gaps between existing standards and the needs of the owners and operators of critical infrastructure;

3. Make recommendations on how the gaps in standards may be addressed and develop a blue-print for the development of a security standards framework that is essential in identifying and categorising security standards.

An all hazards approach is being taken to threats. This approach includes security threats such as where someone has the capability, intent and opportunity to exploit a vulnerability to do harm and accidents and natural disasters that may also cause inadvertent harm due to the existence of vulnerability.

The reason for this all hazards approach is to ensure that where possible multiple risks are dealt with by effective and integrated treatments, such as standardised products and services. The resultant standards can be developed in a modular fashion or in such a way as to not cause additional vulnerabilities by describing key aspects of security that can form the basis for new attacks.

Critical infrastructure can be damaged or destroyed by a number of factors including the following:

- Natural disasters
- Negligence
- Accidents
- Terrorism
- Hacking and vandalism
- Criminal activity
- Malicious damage

The standards identified under this project should assist the owners and operators of privately owned critical infrastructure to:

- provide adequate security for their assets
- actively apply risk management techniques to their planning processes
- conduct regular reviews of risk management plans
- report any incidents or suspicious activities to the police
- develop and regularly review business continuity plans, and
- participate in any exercises to test plans conducted by government authorities.

A very important aspect of this project is that it needs to be supported and driven by the owners and operators of critical infrastructure.

It is anticipated that the project will focus on elements of critical infrastructure as shown in Table 1.

TABLE 1. ELEMENTS OF CRITICAL INFRASTRUCTURE

Sectors	Sub Sectors
Energy	Gas, petroleum fuels, electricity generation, transmission and distribution.
Utilities	Water, waste water and waste management.
Transport	Air, road, sea, rail and inter-modal (cargo distribution centres)
Communications	Telecommunications (phone, fax, Internet, cable, satellites), electronic mass communications and postal services.
Health	Hospitals, public health and research and development laboratories.
Food supply	Bulk production, storage and distribution.
Finance	Banking, insurance and trading exchanges.
Government services	Defence and intelligence facilities, houses of parliament, key government departments, foreign missions, key residences, emergency services (police, fire, ambulance and others) and nuclear facilities.
National icons	Buildings, cultural, sport and tourism.
Essential manufacturing	Defence industry, heavy industry and chemicals.

Asia-Pacific Economic Cooperation

Project Output

The major project output will be a final report that contains the following elements:

1. An outline of some of the issues, barriers and solutions related to protecting critical infrastructure and identify user perceptions of the importance of standards related to securing critical infrastructure.

2. A suggested list of the standards required by the owners and operators of critical infrastructure and the identification of gaps between existing standards and the needs of the owners and operators of critical infrastructure.

3. Clear recommendations on how the gaps in standards may be addressed and a blue-print for the development of a standards framework that is essential in identifying and categorising security standards.

Drivers for the Project

The Critical Infrastructure and Support Systems Standardisation Project is necessary because there is a very real need for simple and agreed standards to protect infrastructure. This guidance is necessary due to the many drivers that are shown in Figure 1.

FIGURE 1 DRIVERS FOR SECURITY STANDARDS

- Demand to manage security risks and compliance to protect assets and the community
- Transfer of infrastructure from public to private companies
- The need for documents with authority that have been developed through a formal process of openness, transparency and consensus
- The need for documents developed by an impartial body not bound by any jurisdiction
- The need for simple and agreed guidance
- The heightened threat of terrorist attack
- Community concerns about security and privacy
- Regulation (light touch)
- Demand for food and supply chain security
- Demand for indicative assurance confidence and consensus
- The need for collaboration in the development of systems

Integrated security standards framework

Traditionally standards develop in a bottom up fashion. This occurs because industry experts working in a particular field identify a need for a new standard. For example an Information Technology (IT) expert may want to exchange secure data, so they recommend the development of a new cryptography standard. This is a valid approach to standards development, however such an approach makes it difficult to prioritise and resource standards development projects. Additionally there may be whole new areas where standards are required but work does not proceed because there is not an existing committee in place. It is also difficult to ensure coordination within and among committees responsible for preparing standards on different products, processes or services which is necessary to achieve a coherent approach to the treatment of security.

To address this problem a top down approach should complement the bottom up approach to standards development. A top down approach would involve looking at the entire area of security and identifying where standards are required and should have priority.

It is impossible to effectively and comprehensively apply a top down approach without some framework to identify all the areas covered by standards development. For this purpose it is suggested that a security standards framework be established.

The use of a framework is recommended to ensure that each specialised standard is restricted to specific aspects and makes reference to wider ranging standards for all other relevant aspects. The structure is built on the following types of standards:

- Basic security standards, comprising fundamental concepts, principles and requirements with regard to general security applicable to a wide range of products, processes and services.
- Group security standards, comprising security applicable to several or a family of similar products, processes or services dealt with by more than one committee, making reference, as far as possible, to basic security standards.
- Security product standards, comprising security aspect(s) for a specific, or a family of product(s), process(es) or service(s) within the scope of a single committee, making reference, as far as possible, to basic security standards and group security standards.

- Product standards containing security aspects but which do not deal exclusively with security aspects; these should make reference to basic security standards and group security standards.

Keeping in mind the purpose, it is important that any framework addresses the following criteria.

1. Identify the broad areas that require security standards.
2. Simple, communicable and easily understood.
3. Provide the basis for categorising, managing the scope and taking stock of existing standards activities as well as identifying gaps and priority areas.
4. Supported by key stakeholders.
5. Widely used and openly available and unencumbered by intellectual property protection.

Standards Australia's National Centre for Security Standards (NCSS) Model

Standards Australia's National Centre for Security Standards (NCSS) has commenced work on developing an integrated security standards framework. A proposed revised framework was recommended on the basis of results from the Australian Security Standards and Support System.

The proposed revised framework is presented in Figure **1**. It is anticipated that this project will utilise and extend this framework.

FIGURE 1 INTEGRATED SECURITY STANDARDS FRAMEWORK

The key components of the model are explained below.

Governance, strategy and policy

This element encapsulates product and systems standards related to the overall governance and management of an organisation with respect to security.

The focus of this element is on the continued ability of an organisation to achieve its strategy, objectives and targets.

To achieve the organisational strategy it is necessary to have in place a rigorous system that assists with the identification, quantification and categorisation of tangible (physical) and intangible (information and people) assets in relation to their importance in achieving the organisational strategy. The reason why such a process is necessary is that it ensures the level of security chosen for a given asset is fit for purpose or based on the value of the asset in terms of its impact on the organisation.

Other important aspects of this element include legal compliance management, communications and media management, audit, compliance and management review mechanisms for the purposes of continuous improvement. This element also includes standards designed to manage outsourcing and the purchasing of security services or services that impact on security as well as reporting incidents and issues management.

Risk management

The risk management element includes all standards and supporting material associated with risk management including:

- Systems to assist with monitoring the environment and intelligence gathering, such as examining the social, political and economic environment.
- Understanding interdependencies, intents, capabilities and threats.
- Tools to help establish the security context.
- Risk identification, analysis, evaluation, treatment, communication and monitoring.

This element encompasses business continuity management, which is one possible risk mitigation strategy. Business continuity involves preparing for the eventuality of an event or incident by having in place a pre-developed and practiced emergency response, continuity response and ultimate recovery strategy.

Information security

The information security element includes all standards and supporting material associated with an integrated system for the management of information security. This element deals with the confidentiality, integrity and availability of information and encompasses such things as document, data and records control. It also addresses the security of networks, hardware, software, communications and supporting processes.

Personnel security

Personnel Security involves a procedural system implemented to ensure that only those people whose work responsibilities require them to access official information and assets have such access. This is done by limiting the number of people who have access to those who can demonstrate a need to know or have access and whose eligibility has been determined after an evaluation of their history, attitudes, values and behaviour.

The personnel security element includes all standards and supporting material associated with an integrated system for the management of personnel security. Personnel security standards encompass occupational health and safety, pre-employment screening, privacy, administrative records, security roles and responsibilities, induction and training, identity management, access control (employees and other), protecting individuals, working from home and the security of employees when working overseas.

Physical security

Physical security is the part of security concerned with the provision and maintenance of a safe and secure environment for the protection of the organisation's employees and clients. This includes physical measures designed to prevent unauthorised access to official resources and to detect and respond to intruders.

The physical security element includes all standards and supporting material associated with an integrated system for the management of physical security. Physical security standards include access to security advice from professionals, security equipment requirements, site selection, design security, building security, perimeter security, lighting, alarms, safes and strong rooms, guards, patrols and control rooms, CCTV and emergency planning and incident procedures.

Asia-Pacific Economic Cooperation

Conclusion

The impetus for this Project came from the need to refocus on security in the Asia Pacific Region following events such as natural disasters and criminal activity in recent times. It builds on the outcomes of a similar initiative that was undertaken in Australia.

The pressure on security professionals and businesses to manage and respond appropriately to security threats has never been greater. Good security standards provide essential information, advice and benchmarks to guide reasonable and prudent decisions. Fundamentally, standards articulate best practice.

The Project will aim to identify where gaps exist in the existing standards and recommend priorities for the development of future standards. There will be a solution oriented approach to barriers identified relating to protecting critical infrastructure. Most importantly, the Project will provide a blue-print for the development of a standards framework for identifying and categorising security standards.

The benefits to APEC Member Economies from participation in this project are:

- a more consistent approach to security along with emergency and disaster management in the APEC region;
- the promotion of security standards and systems capacity which support business as well as critical infrastructure in times of emergency, helping to minimise impact on economies;
- harmonisation of related standards across the APEC region, which will help improve the interoperability and compatibility of systems related to securing critical infrastructure;
- improved technical capacity through assistance in ascertaining key areas of standardisation focus so that programs may be targeted for the development of security standards; and
- the capacity to make more informed choices about effective security solutions through better access to information on tested and consistent methods to protect critical infrastructure.

The success of this project will, to a large extent, depend on each APEC Member Economy's commitment to engaging actively in the process in order to achieve shared objectives for security in the Asia Pacific Region.

Asia-Pacific Economic Cooperation

Project Plan

Critical Infrastructure and Support Systems Standardisation Project

A Standards Australia and APEC initiative to promote a better standards infrastructure for security

June 2008

Prepared by: Mark Bezzina

Asia-Pacific Economic Cooperation

Table of Contents

Project data

Purpose

This is a commercial in confidence document that has been created to provide Standards Australia with a detailed project plan for the Critical Infrastructure and Support Systems Standardisation Project.

Project duration

The project will run for 12 months.

Key contacts

The Critical Infrastructure and Support Systems Standardisation Project is managed by Standards Australia. The funding for this project has been provided by APEC and Standards Australia. StanCert Pty Ltd is the Project Manager.

The Project Supervisor is:
Karen Hitchiner
Manager International Development
Standards Australia
Phone: +64 4 498 5945
Mobile: +64 2102 475 926 (New Zealand)
+61 404 806 241 (Australia)
Email: Karen.Hitchiner@standards.org.au

The APEC Project Sponsor is:
Brian Phillips
Manager, Standards & International Liaison
Industry & Small Business Policy Division
Department of Innovation, Industry, Science and Research
Phone: +61 2 6213 6156
Mobile: +61 402 438428
Email: brian.phillips@innovation.gov.au

The Team Leader is:
Mark Bezzina
Managing Director of StanCert Pty Ltd
Consultant to Standards Australia
Phone: +61 2 8721 6434
Mobile: +61 413 101 096
Email: bezzina@stancert.com

The Lead Consultant is:
Clare Morrison
Stancert Pty Ltd
Phone: +61 2 8721 6434
Mobile: + 61 430 333 006
Email: cmorrison@stancert.com

Project scope and objectives

The Critical Infrastructure and Support Systems Standardisation Project is designed to assist in the development of a framework to address the need to protect critical infrastructure in times of emergencies, whether these be caused by natural disasters or criminal activity.

This is an agreed Sub-Committee on Standards and Conformance (SCSC) APEC's Second Trade Facilitation Action Plan (TFAP II) activity. In particular, it will promote security standards and systems capacity which support business. Building technical capacity for developing APEC member economies will be a key focus. The project will also promote the harmonization of related standards across the APEC region. This will help improve the interoperability, and compatibility of systems related to securing critical infrastructure.

The project aims to:

- Identify and detail some of the issues, barriers and solutions related to protecting critical infrastructure and identify user perceptions of the importance of standards related to securing critical infrastructure. Critical infrastructure includes, but is not limited to:
  - Power supply
  - Water
  - Telecommunications
  - Financial Services Sector
  - Banking and finance
  - Public events and mass gathering
  - Transport
  - Health
  - Operation of government
  - Food
  - Essential manufacturing
- Identify and prioritise the standards required by the owners and operators of critical infrastructure and identify the gaps between existing standards and the needs of the owners and operators of critical infrastructure.

- Make recommendations on how the gaps in standards may be addressed and develop a blue-print for the development of a standards framework that is essential in identifying and categorising security standards.

Project methodology overview

In brief, the Project methodology will take the following form:

0. Project management
1. Preparation
2. Capacity building
3. Consultation
4. Analysis and validation
5. Reporting and communicating results

The project facilitators will conduct a workshop to provide guidance to participating APEC members on how to carry out their own member economy survey to establish a baseline. Ongoing instruction and support will be provided remotely during the project.

At the completion of the in-member economy survey, the Project leaders will interpret the survey data and report on the results.

A report will be created addressing the Project aims and possible follow up activities will be identified.

Much of this work will be based on the methodology used in a similar project previously undertaken by Australia.

Project timeline

The detailed project timeline is shown in Appendix 1.

The duration in the bars shows the amount of time allowed to complete each task rather than effort.

This project plan does not take into consideration the human resources required by the APEC Member National Standards Bodies to carry out the project or attend meetings.

Project Tasks

A detailed overview of the project tasks is outlined in Table 3 below

TABLE 3 EXPLANATION OF PROJECT TASKS

Stage	Activity Name	Activity Description
0	Project management	This activity is aimed at the effective management of the Project and runs for the duration of the Project. It includes such activities as progress reporting, accounting, project meetings and legal review.
1	Preparation	The project will be administered by Standards Australia and StanCert however APEC Member Economy National Standards Bodies will be required to administer a survey and carry out analysis within their own country. Standards Australia and StanCert will provide the tools and support to assist with this process. Each APEC Member Economy National Standards Body will be asked to nominate a key contact point to work on the project. Whilst this project's objectives are entirely focused on technical issues and are neutral regarding gender criteria the project will ask for preference to be given for women to act as National Contact Points from APEC Member Economy National Standards Bodies in conducting the Critical Infrastructure and Support Systems Standardisation Project. The initial phase of the Project will involve the development of a project plan and background paper. The project plan and background paper will be used to communicate the project and seek support and commitment from key parties. The project plan will identify the detailed steps and responsibilities involved in the project. The background paper will be developed to provide background and overview for the project. After receiving the support of APEC Member Economy National Standards Bodies, a survey based on the Australian survey will be developed.

Stage	Activity Name	Activity Description
		The purpose of the survey will be to seek structured feedback on the priorities for security related standards from the owners and operators of critical infrastructure within the APEC region. APEC Member Economy National Standards Bodies will be asked to review and approve the project plan (by correspondence). At the same time, feedback will be sought on the background paper and survey. Both the background paper and survey will be updated as a result of the feedback received. **Outputs:** • Detailed project plan • Project background paper • Survey instrument
2	Capability building	APEC Member Economy National Standards Bodies will each be instructed by Standards Australia and StanCert on how to conduct the survey assessment. This instruction will be done at a 1 day workshop in a central location attended by the nominated contact points of each APEC Member Economy National Standards Body. **Outputs:** • Development of a 1 day workshop including presentations and guidance material on carrying out the survey in country
3	Consultation	APEC Member Economy National Standards Bodies will administer their survey and encourage their stakeholders to complete the survey. It is anticipated that the survey will be completed by the owners and operators of critical infrastructure within the APEC Member Economy. **Outputs:** • Completed survey results
4	Analysis and validation	Standards Australia and StanCert will assist APEC Member Economy National Standards Bodies to follow up late and incomplete survey responses. After a sufficient number of surveys are received

Stage	Activity Name	Activity Description
		work will begin on consolidating and interpreting the results. A draft report will be produced. **Outputs:** • Interim project draft report
5	Reporting and communicating results	The consolidated responses to the survey will be published in a report. An APEC/industry event (adjacent to an ABAC/regional standards meeting) will be planned to communicate the draft results from the project to APEC members and the Asia Pacific Standards Community. Stakeholders will be given 4 weeks following the presentation to make any final comments before the report is finalised for consideration at SOM III. The report will identify a number of recommendations and these will form the basis of a future work plan for APEC member economies in conjunction with ABAC. **Outputs:** • Meeting to discuss results • Final draft report • Launch of report

Further Information

For further information please contact:

Clare Morrison, Lead Consultant, StanCert Pty Ltd cmorrison@stancert.com

Mark Bezzina, Executive Director, StanCert Pty Ltd bezzina@stancert.com


APEC CISSS Project Plan
Appendix 1
SA-APEC Project
Stage 0 - Project reports and Communications
Countermeasures with local statistical contact points
Team meetings
Stage 1 - Preparation
Project plan
White paper
Survey
SA Approval and review
Rework Project Plan, update paper and survey from feedback
Write to CISS and get nominations to participate
Follow up nominations to participate
Validate APEC approval of project and contractor
Manage APEC validation of project
Stage 2 - Initiation and capacity building
Identify and confirm host APEC Member Economy for training workshop
Prepare training course
Identify and confirm training workshop venue and accommodation
Approval/advise of APEC requirements for delegates attending the workshop
Advise APEC of the workshop and travel arrangements of delegates
Deliver workshop (27 Aug)
Stage 3 - Consultation
Open consultation stage
Train on survey
Develop interim presentation for APEC
Monitoring and support in consultation stage
Close consultation stage - turn off survey
Stage 4 - Analysis and validation and communications
Plan communication event logistics
Follow up survey responses
Analyse survey results
(MNI) draft report
Prepare presentation for communications event
Present communications event (depends on presentation date to APEC CISSS in 2009)
Present to ABAC
Approval of draft report
Stage 5 - Reporting
Make changes to draft report based on feedback
Format publication for publishing
Final report
Project ends
Task
Split
Progress
Milestone
Summary
Project Summary
External Tasks
External Milestone
Date
Plan by EconCert for questions contact EconCert e.econcert@econcert.com or +61 2 972 1404

Asia-Pacific Economic Cooperation

Instructions

Critical Infrastructure and Support Systems Standardisation Survey

Year 2008
Authored by: Mark Brookes
StanCom Pty Ltd

Asia-Pacific Economic Cooperation

TABLE OF CONTENTS

Asia-Pacific Economic Cooperation

Critical Infrastructure and Support Systems Standardisation Survey

Survey - Page 1

1. Introduction

This page is an introduction to the survey. The key project documents can be viewed, downloaded and printed from this page. In addition to these instructions the project documents include:

- a .PDF version of the survey for reference
- Project Plan
- Background Paper
- Glossary of definitions for the key terms used in the survey.

You will require a software application for viewing .PDF files, such as Adobe Reader, in order to access these documents.

It is recommended that you become familiar with the project documents before commencing the survey.

The survey must be completed in one sitting. Estimated time for completion is 15 minutes. The survey is not limited to one respondent per organisation. There are no limits to the number of responses from people working for the same organisation. We are seeking responses from well informed individuals rather that organisational responses.

The survey does not have a spell checker. If you require a spell checker it is suggested that you draft responses to the open ended questions in Word before commencing the survey. Some internet browsers have a spell checking feature. Another option is the latest Google toolbar, which has a built-in spell checker.

The survey does not have a print preview or print option. However the survey can be printed page by page from your internet browser. A PDF version of the survey can be downloaded and printed from the introduction page. The PDF version is for reference only and it is not possible to complete this document as a form in soft copy. If you attempt to do this the information that has been entered will not be saved. If you do not have access to the internet and are unable to complete the survey online please email Clare Morrison, Lead Consultant, at cmorrison@stanconf.com about other options.

SSL encryption has been applied to the survey to protect the confidentiality of responses. The data will be analysed and reported to Asia-Pacific Economic Cooperation (APEC) and will not identify individuals. It will form the basis for a blue print or framework for future

Survey - Page 1 (continued)

standards development across the Asia Pacific Region related to the protection of critical infrastructure and support systems. Refer to the project plan and background paper for further information.

When questions are marked by an asterisk * this means that a response is required or mandatory. There will be an error message if the question is not answered or the information is not entered in accordance with the instructions. It will not be possible to move forward in the survey until the question is answered or the error corrected.

The answer choices for multiple choice questions include an 'Unsure' option. Choose the 'Unsure' button if you are not sure of the answer or if you consider that this question is not applicable to your sector.

The answer choices for multiple choice questions also include a 'Neutral' option. This is the mid-range or average option. Choose the 'Neutral' button if you consider the level of importance for the item is average on the scale or if you are neutral on the rating for the issue. If the scale was numerical (1, 2, 3, 4, 5) 'Neutral' would be 3. For example the score on an importance scale is neither towards important nor towards unimportant.

As the survey aims to collect reliable information please do not choose the 'Neutral' and 'Unsure' buttons unless absolutely necessary. Many of the questions are about ratings and we are interested in finding out how you rate the various issues and standards.

We also ask that you consider your ratings carefully as this will affect the quality of the data collected. For instance, if you rate every item as "important' for a particular question (or throughout the survey) it will be difficult to assess the priority of particular issues in the data analysis.

There are optional comment boxes throughout the survey for the entry of additional information. Comments should be entered in English. It will not be possible to translate entries in other languages.

Survey - Page 2

2. Contact details and background information

1. Mandatory information has been kept to a minimum in this question. Only the name of the person completing the survey and their email address is required information. This information is required in case the project team needs to check the accuracy or meaning of responses entered. This is important because many survey respondents will be from a non English speaking background. The survey results will not identify survey respondents or their organisations. This information will be kept confidential. Security is further ensured by the SSL encryption that has been applied to the survey.

2. **Country**

   This question is mandatory / an answer is required.

   This information is required because the survey results will be reported by country.

3. **Gender**

   This question is mandatory / an answer is required.

   This information is required for all projects that are funded by APEC. The survey results will be reported by gender.

4. **Respondent sector(s)**

   This question is mandatory / an answer is required.

   This information is required because the survey results will be reported by respondent sector (s). The sectors listed here match the Integrated Security Framework that was developed following the Australian survey that was the basis for this project. An 'other (please specify)' option is provided if you cannot identify your sector from the choices listed.

5. **Respondent role within organisation**

   This question is mandatory / an answer is required.

   This information is required because the survey results will be reported by respondent role. The roles listed here match the Integrated Security Framework that was developed following the Australian survey that was the basis for this project. An 'other (please specify)' option is provided if you cannot identify your role from the choices listed.

Survey - Page 2 (continued)

6. **Briefly describe the role of your organisation in your sector (500 character limit)**

   This question is non mandatory / an answer is optional.

   This question requires contextual information about where your organisation fits within the sector identified in 5. Above. For example, is the organisation a standards development organisation, private security firm, government defence authority etc?

Survey - Page 3

3. Security objectives, issues and solutions

1. Security issues and solutions

This question is non mandatory / an answer is optional.

This question collects information about security issues and solutions relating to critical infrastructure and support systems.

Select the major security issue in your sector by choosing from the list provided (one choice only).

Enter solution (s) for the major issue in the Solutions box below.

If the major sector issue for your sector is not listed, enter it with the solution (s) in the Additional comments box in Q 7 at the bottom of the page. Identify both the issue and solution (s) clearly.

For example:

Issue -
Solution (s) -

2. Would the solutions to addressing these issues involve adopting standards?

This question is mandatory / an answer is required.

This question collects information about whether solutions to the security issues would involve adopting standards.

Enter Yes or No.

Note: The term 'standards' in this question refers to formal standards:

> Standards are defined by the International Organization of Standardization (ISO) as "documented agreements containing technical specifications or other precise criteria to be used consistently as rules, guidelines or definitions of characteristics, to ensure that materials, products, processes and services are fit for their purpose."

The focus of this survey is standards based and therefore questions using this term should be read in this context. A simpler open source definition of the term 'standard' is included in the Glossary for easy reference.

Survey – Page 3 (continued)

3. **How well do you understand the systems that are in place to protect your organisation when there is a significant disruption to normal services?**

   This question is mandatory / an answer is required

   This question collects information about respondents' understanding of the systems in place to ensure business continuity in times of crisis.

   Assign your level of understanding by checking exactly one button for your choice.

   As stated earlier, please do not choose the 'Neutral' or 'Unsure' buttons unless absolutely necessary. 'Unsure' also means not applicable to your sector.

   If you do not choose one option there will be an error message. You will not be able to move forward in the survey until you check one option to correct the error.

4. **How well do you understand the impact on your organisation's customers and suppliers if there is a significant disruption to normal services?**

   This question is mandatory / an answer is required

   This question collects information about respondents' understanding of how their organisation's customers and suppliers would be affected if there was a significant disruption to normal business services.

   Assign your level of understanding by checking exactly one button for your choice.

   As stated earlier, please do not choose the 'Neutral' or 'Unsure' buttons unless absolutely necessary. 'Unsure' also means not applicable to your sector.

   If you do not choose one option there will be an error message. You will not be able to move forward in the survey until you check one option to correct the error.

Survey – Page 3 (continued)

5. **Would your organisation help to fund the development of standards that are considered critical to the security of your sector?**

   This question is mandatory / an answer is required.

   This question collects information about whether organisations would be prepared to contribute funding to the development of standards that are considered critical to the security of their sector.

   Survey respondents are only being asked to give an opinion here, based on their knowledge of their organisation. The information collected will be used to gain an overall impression of the level of commitment to funding standards development. It is not binding in any way and the results will not be reported by organisation.
   Answer this question by checking exactly one button for your choice.

   As stated earlier, please do not choose the 'Neutral' or 'Unsure' buttons unless absolutely necessary. "Unsure' also means not applicable to your sector.

   If you do not choose one option there will be an error message. You will not be able to move forward in the survey until you check one option to correct the error.

6. **Would your organisation participate in the development of standards that are considered critical to the security of your sector?**

   This question is mandatory / an answer is required.

   This question collects information about whether organisations would be prepared to contribute intellectually to the development of standards that are considered critical to the security of their sector.

   As in 5. above, survey respondents are only being asked to give an opinion here, based on their knowledge of their organisation. The information collected will be used to gain an overall impression of the level of commitment to participation in standards development. It is not binding in any way and the results will not be reported by organisation.

   Answer this question by checking exactly one button for your choice.
   As stated earlier, please do not choose the 'Neutral' or 'Unsure' buttons unless absolutely necessary. "Unsure' also means not applicable to your sector.

   If you do not choose one option there will be an error message. You will not be able to move forward in the survey until you check one option to correct the error.

Survey – Page 3 (continued)

7. **Additional Comments**
   (500 character limit)

   This question is non mandatory / an answer is optional.

   The comments box has been provided to allow survey respondents to make additional comments about security objectives, issues and solutions (including existing standards and development of new standards).

Survey - Page 4

4. Common approaches supporting security processes

1. **How important do you believe common and agreed approaches, standards, methods, protocols and procedures are to improved security?**

   This question is mandatory / an answer is required.

   Assign the level of importance (including level of urgency) you attach to these by checking exactly one button for your choice.

   As stated earlier, please do not choose the 'Neutral' or 'Unsure' buttons unless absolutely necessary. 'Unsure' also means not applicable to your sector.

   If you do not choose one option there will be an error message. You will not be able to move forward in the survey until you check one option to correct the error.

2. **Within your organisation or sector what are the major sources of guidance when developing security products, installations, processes or systems?**

   This question is mandatory / an answer is required.

   This question collects information about the major sources of guidance by organisation or sector.

   Check at least one button. More than one button can be checked on this question. An 'Other (please specify)' button is provided if you consider that there should be other options included in the choices.

   If you do not choose at least one option there will be an error message. You will not be able to move forward in the survey until you check one option to correct the error.

3. **In your experience what has been the outcome of using these major sources of guidance?**

   This question is mandatory / an answer is required.

   This question collects information about outcomes of using major sources of guidance.

   Check exactly one button.

   As stated earlier, please do not choose the 'Neutral' or 'Unsure' buttons unless absolutely necessary. 'Unsure' also means not applicable to your sector.

   If you do not choose one option there will be an error message. You will not be able to move forward in the survey until you check one option to correct the error.

Survey – Page 4 (continued)

4. Additional Comments
(500 character limit)

This question is non mandatory / an answer is optional.

The comments box has been provided to allow survey respondents to make additional comments about common approaches supporting security processes.

Survey - Page 5

5. Assessing Priorities for broad categories of security standards and other sources of guidance

1. **Please rate the level of importance for the following broad categories of security standards and other sources of guidance.**
   Consider the level of urgency when rating the importance level for each category.

   This question is mandatory / an answer is required.

   Note that this section focuses on the importance of broad categories of security standards and other sources of guidance. Information about the importance of specific security standards and other sources of guidance under these broad categories will be collected in the following pages of the survey.

   Note:
   The term 'other sources of guidance' refers to documentation, guidelines, legislation etc that are used for reference.

   Assign the level of importance (including level of urgency) you attach to these by checking exactly one button on each line for your choice.

   As stated earlier, please do not choose the 'Neutral' or 'Unsure' buttons unless absolutely necessary. 'Unsure' also means not applicable to your sector.

   If you do not check one button on every line there will be an error message. You will not be able to move forward in the survey until you check one button on every line to correct the error.

2. **Are there any other broad categories of security standards and other sources of guidance that you believe should have been included in this category?**
   If so, please identify these below and rate the level of importance.
   (500 character limit)

   This question is non mandatory / an answer is optional.

   The box has been provided to allow survey respondents to make additional comments about broad categories of security standards and other sources of guidance that they believe should have been included in this category.

Survey - Page 6

6. Governance, Strategy & Policy - Assessing priorities for specific security standards and other sources of guidance

1. **Assessing priorities for specific security standards and other sources of guidance**

   This question is mandatory / an answer is required.

   Note that this section focuses on the importance of specific security standards and other sources of guidance.

   Assign the level of importance (including level of urgency) you attach to these by checking exactly one button on each line for your choice.

   As stated earlier, please do not choose the 'Neutral' or 'Unsure' buttons unless absolutely necessary. 'Unsure' also means not applicable to your sector.

   If you do not check one button on every line there will be an error message. You will not be able to move forward in the survey until you check one button on every line to correct the error.

2. **Are there any other specific security standards and other sources of guidance that you believe should have been included in this category?**
   If so, please identify these below and rate the level of importance.
   (600 character limit)

   This question is non mandatory / an answer is optional.

   The box has been provided to allow survey respondents to make additional comments about specific security standards and other sources of guidance that they believe should have been included in the Governance, Strategy & Policy category.

Asia-Pacific Economic Cooperation

Survey - Page 7

7. Risk Management - Assessing priorities for specific security standards and other sources of guidance

1. **Assessing priorities for specific security standards and other sources of guidance**

   This question is mandatory / an answer is required.

   Note that this section focuses on the importance of specific security standards and other sources of guidance.

   Assign the level of importance (including level of urgency) you attach to these by checking exactly one button on each line for your choice.

   As stated earlier, please do not choose the 'Neutral' or 'Unsure' buttons unless absolutely necessary. 'Unsure' also means not applicable to your sector.

   If you do not check one button on every line there will be an error message. You will not be able to move forward in the survey until you check one button on every line to correct the error.

2. **Are there any other specific security standards and other sources of guidance that you believe should have been included in this category? If so, please identify these below and rate the level of importance. (500 character limit)**

   This question is non mandatory / an answer is optional.

   The box has been provided to allow survey respondents to make additional comments about specific security standards and other sources of guidance that they believe should have been included in the Risk Management category.

Survey - Page 8

8. Information Security - Assessing priorities for specific security standards and other sources of guidance

1. **Assessing priorities for specific security standards and other sources of guidance**

   This question is mandatory / an answer is required.

   Note that this section focuses on the importance of specific security standards and other sources of guidance.

   Assign the level of importance (including level of urgency) you attach to these by checking exactly one button on each line for your choice.

   As stated earlier, please do not choose the "Neutral" or "Unsure" buttons unless absolutely necessary. "Unsure" also means not applicable to your sector.

   If you do not check one button on every line there will be an error message. You will not be able to move forward in the survey until you check one button on every line to correct the error.

2. **Are there any other specific security standards and other sources of guidance that you believe should have been included in this category?**
   If so, please identify these below and rate the level of importance.
   (500 character limit)

   This question is non mandatory / an answer is optional.

   The box has been provided to allow survey respondents to make additional comments about specific security standards and other sources of guidance that they believe should have been included in the Information Security category.

Survey - Page 9

9. Personnel Security - Assessing priorities for specific security standards and other sources of guidance

1. **Assessing priorities for specific security standards**

   This question is mandatory / an answer is required.

   Note that this section focuses on the importance of specific security standards and other sources of guidance.

   Assign the level of importance (including level of urgency) you attach to these by checking exactly one button on each line for your choice.

   As stated earlier, please do not choose the "Neutral" or "Unsure" buttons unless absolutely necessary. "Unsure" also means not applicable to your sector.

   If you do not check one button on every line there will be an error message. You will not be able to move forward in the survey until you check one button on every line to correct the error.

2. **Are there any other specific security standards and other sources of guidance that you believe should have been included in this category?**
   If so, please identify these below and rate the level of importance.
   (500 character limit)

   This question is non mandatory / an answer is optional.

   The box has been provided to allow survey respondents to make additional comments about specific security standards and other sources of guidance that they believe should have been included in the Personnel Security category.

Survey - Page 10

10. Physical Security - Assessing priorities for specific security standards and other sources of guidance

1. **Assessing priorities for specific security standards and other sources of guidance**

   This question is mandatory / an answer is required.

   Note that this section focuses on the importance of specific security standards and other sources of guidance.

   Assign the level of importance (including level of urgency) you attach to these by checking exactly one button on each line for your choice.

   As stated earlier, please do not choose the 'Neutral' or 'Unsure' buttons unless absolutely necessary. 'Unsure' also means not applicable to your sector.

   If you do not check one button on every line there will be an error message. You will not be able to move forward in the survey until you check one button on every line to correct this error.

2. **Are there any other specific security standards and other sources of guidance that you believe should have been included in this category?**
   If so, please identify these below and rate the level of importance.
   (500 character limit)

   This question is non mandatory / an answer is optional.

   The box has been provided to allow survey respondents to make additional comments about specific security standards and other sources of guidance that they believe should have been included in the Physical Security category.

Survey - Page 11

11. Methods for improving the implementation of security standards

1. **What could be done to make the implementation of security standards more successful?**
   Check exactly 3 boxes to indicate your top 3 choices from the list below

   This question is mandatory / an answer is required.

   This question collects information about what survey respondents consider to be their top 3 choices of methods for improving the implementation of security standards. This information will be reported but not ranked.

   This question requires exactly 3 boxes to be checked from the list provided. An 'Other (please specify)' button is provided if you consider that there should be other options included in the choices.

   If you do not check exactly 3 boxes there will be an error message. You will not be able to move forward in the survey until you check exactly 3 boxes.

2. **Final comments**

   This question is non mandatory / an answer is optional.

   The box has been provided to allow survey respondents to make any final comments they wish to make about the survey.

The survey has by now been completed. Respondents may go back to previous pages and edit their responses if they wish to do so.

To submit the survey, click on the 'Done' button at the bottom of the screen.

Note
It will not be possible to go back and edit the survey responses after it has been submitted.

Critical Infrastructure and Support Systems Standardisation Survey

1. Introduction

Welcome to the Pilot Critical Infrastructure and Support Systems Standardisation Project Survey. Your participation in this survey is greatly appreciated by all concerned with this important initiative.

This survey will assist in the development of a proposed framework of standards to address the need to protect critical infrastructure and support systems across the Asia-Pacific Region during times of emergencies.

The survey will also identify and prioritise the standards required by the owners and operators of critical infrastructure and any gaps that may exist. All all hazards approach is being taken to threats. This approach includes security threats that are intentional or man-made (such as criminal acts or terrorism), as well as accidents, natural disasters and pandemics.

SSL encryption has been applied to this survey to protect the security of information.

There are optional comment boxes throughout the survey for the entry of additional information. Comments should be entered in English. It will not be possible to translate entries in other languages.

We suggest that before commencing this survey you download the and print the instructions, background papers and support materials via the links provided below. You will need a PDF reader such as Adobe Reader to view and print these documents.

Survey Glossary
Survey Instructions
Project Plan
Background Papers

Critical Infrastructure and Support Systems Standardisation Survey

2. Contact details and background information

Note:
Only your last name, first name and email address are required information in Q1 below.
The other fields in this question are optional.

*** 1. Please provide the following information.**

Last Name:
First Name(s):
Company/Organisation:
Email Address:
Phone Number:

*** 2. Country**

*** 3. Gender**

Male Female

*** 4. Respondent sector(s)**

- Energy (e.g. gas, electricity, petroleum fuels)
- Utilities (e.g. water, water waste management)
- Communications (e.g. telecommunications, IT, postal services)
- Transport
- Health
- Food Supply
- Finance
- Government Services
- National Icons (e.g. buildings, cultural, sport and tourism)
- Essential Manufacturing
- Other (please specify) 50 character limit

*** 5. Respondent role within organisation**

- ○ CEO
- ○ Executive
- ○ Manager
- ○ Policy Adviser
- ○ Standards Developer
- ○ Technical Specialist
- ○ Vendor or Consultant
- ○ Other (please specify) (30 character limit)

6. Briefly describe the role of your organisation in your sector (500 character limit)

Critical Infrastructure and Support Systems Standardisation Survey

3. Security objectives, barriers and solutions

In the following question please choose the major security issue in your sector from the list below (only CHOOSE ONE).
Then suggest solution(s) for the issue in the box.
If your issue is not listed, enter it with a solution under Q 7. Additional Comments at the bottom of this page.

1. Security Issues and solutions

- ◯ Funding
- ◯ Regulation
- ◯ Time
- ◯ Personnel (numbers)
- ◯ Information / data
- ◯ Communication
- ◯ Consultation
- ◯ Training
- ◯ Planning
- ◯ Executive Buy-in / commitment
- ◯ Industry specific standards

Solutions (250 character limit)

*** 2. Would the solutions to addressing these issues involve adopting standards?**

◯ Yes ◯ No

*** 3. How well do you understand the systems that are in place to protect your organisation when there is a significant disruption to normal services?**

◯ Very well ◯ Well ◯ Neutral ◯ Not well ◯ Unsure

*** 4. How well do you understand the impact on your organisation's customers and suppliers if there is a significant disruption to normal services?**

◯ Very well ◯ Well ◯ Neutral ◯ Not well ◯ Unsure

*** 5. Would your organisation help to fund the development of standards that are considered critical to the security of your sector?**

◯ Yes ◯ Possibly ◯ Not Sure ◯ Unlikely ◯ No

*** 6. Would your organisation participate in the development of standards that are considered critical to the security of your sector?**

◯ Yes ◯ Possibly ◯ Not Sure ◯ Unlikely ◯ No

7. Additional Comments
(500 character limit)

Critical Infrastructure and Support Systems Standardisation Survey

4. Common approaches supporting security processes

*** 1. How important do you believe common and agreed approaches, standards, methods, protocols and procedures are to improved security?**

- Very important
- Important
- Neutral
- Unimportant
- Very unimportant
- Unsure

*** 2. Within your organisation or sector what are the major sources of guidance when developing security products, installations, processes or systems?**

- [ ] International standards
- [ ] National standards
- [ ] Legislation
- [ ] Government guidelines
- [ ] Regional guidelines
- [ ] Internally developed operating procedures
- [ ] Industry contacts (e.g. sources obtained from industry partners)

Other (please specify) (100 character limit)

*** 3. In your experience what has been the outcome of using these major sources of guidance?**

- Substantial improvements
- Some improvements
- Neutral
- Minimal improvements
- No improvements
- Unsure

4. Additional Comments
(500 character limit)

Critical Infrastructure and Support Systems Standardisation Survey

5. Assessing priorities for broad categories of security standards and other s...

*** 1. Please rate the level of importance for the following broad categories of security standards and other sources of guidance.**
Consider the level of urgency when rating the importance level.

	Very important	Important	Neutral	Unimportant	Very unimportant	Unsure
Governance, strategy and policy	○	○	○	○	○	○
Risk management	○	○	○	○	○	○
Information Security	○	○	○	○	○	○
Personnel Security	○	○	○	○	○	○
Physical Security	○	○	○	○	○	○

2. Are there any other broad categories of security standards and other sources of guidance that you believe should have been included in this section? If so, please identify these below and rate the level of importance.
(500 character limit)

Critical Infrastructure and Support Systems Standardisation Survey

6. Governance, Strategy & Policy

Assessing priorities for specific security standards and other sources of guidance

*** 1. Please indicate the level of importance you attach to specific security standards and other sources of guidance in this category.**
Consider the level of urgency when you are choosing the level of importance.

	Very important	Important	Neutral	Unimportant	Very Unimportant	Unsure
Corporate governance	○	○	○	○	○	○
Compliance management (including legal compliance and reporting to relevant authorities)	○	○	○	○	○	○
Reporting incidents and issues management	○	○	○	○	○	○
Systems review, audit and assessment	○	○	○	○	○	○
Security management	○	○	○	○	○	○
Communications, public affairs and media management	○	○	○	○	○	○
Security policy (including security requirements in contracts)	○	○	○	○	○	○
Systems for the categorisation of organisational assets	○	○	○	○	○	○
Crisis management	○	○	○	○	○	○
Understanding networks and inter-dependencies	○	○	○	○	○	○
Continuous improvement mechanisms	○	○	○	○	○	○
Outsourcing (purchasing) or off-shoring security systems and operations	○	○	○	○	○	○
Effective leadership	○	○	○	○	○	○
Executive buy-in / commitment	○	○	○	○	○	○
Building effective partnerships	○	○	○	○	○	○
Building a resilient culture	○	○	○	○	○	○

2. Are there any other specific security standards and other sources of guidance that you believe should have been included in this category? If so, please identify these below and rate the level of importance.
(500 character limit)

Critical Infrastructure and Support Systems Standardisation Survey

7. Risk Management

Assessing priorities for specific security standards and other sources of guidance

Note:
The term 'emergency' includes natural disasters (such as hurricanes, floods, Tsunamis, earthquakes, pandemics) and man-made or intentional acts (such as terrorism and crime).

*** 1. Please indicate the level of importance you attach to specific security standards and other sources of guidance in this category.**
Consider the level of urgency when you are choosing the level of importance.

	Very important	Important	Neutral	Unimportant	Very Unimportant	Unsure
Risk Management	○	○	○	○	○	○
Emergency management	○	○	○	○	○	○
Business continuity management	○	○	○	○	○	○
Business Resilience	○	○	○	○	○	○
Financial recovery provisions	○	○	○	○	○	○
Intelligence and information services	○	○	○	○	○	○
Command, control and communications	○	○	○	○	○	○
First responders	○	○	○	○	○	○
Supply chain and transport	○	○	○	○	○	○
Evacuation plans	○	○	○	○	○	○
Chemical agent detection systems	○	○	○	○	○	○
Radiological agent detection systems	○	○	○	○	○	○
Biological agent detection systems	○	○	○	○	○	○

2. Are there any other specific security standards and other sources of guidance that you believe should have been included in this category? If so, please identify these below and rate the level of importance.
(500 character limit)

Critical Infrastructure and Support Systems Standardisation Survey

8. Information Security

Assessing priorities for specific security standards and other sources of guidance

*** 1. Please indicate the level of importance you attach to specific security standards and other sources of guidance in this category.**
Consider the level of urgency when you are choosing the level of importance.

	Very important	Important	Neutral	Unimportant	Very unimportant	Unsure
General IT security management	○	○	○	○	○	○
General IT security management reporting	○	○	○	○	○	○
Control/platform security	○	○	○	○	○	○
Business access control	○	○	○	○	○	○
Business security – Supervisory Control and Data Acquisition (SCADA)	○	○	○	○	○	○
Network security	○	○	○	○	○	○
Hardware security (including certification)	○	○	○	○	○	○
Software security (including certification)	○	○	○	○	○	○
Information security (storage and categorisation of sensitive information)	○	○	○	○	○	○
Information asset classification and control	○	○	○	○	○	○
Data sharing security	○	○	○	○	○	○
Industrial automation security	○	○	○	○	○	○
Interoperability of security data	○	○	○	○	○	○
Cryptography	○	○	○	○	○	○
Digital certification	○	○	○	○	○	○
Forensics and evidence collection	○	○	○	○	○	○
Penetration testing	○	○	○	○	○	○
Control of viruses and Trojans	○	○	○	○	○	○
Control of spam and spyware	○	○	○	○	○	○
Email attacks (e.g. scams and theft of online banking details)	○	○	○	○	○	○
Scenario simulation applications	○	○	○	○	○	○

2. Are there any other specific security standards and other sources of guidance that you believe should have been included in this category? If so, please identify these below and rate the level of importance.
(500 character limit)

Critical Infrastructure and Support Systems Standardisation Survey

9. Personnel Security

Assessing priorities for specific security standards and other sources of guidance

*** 1. Please indicate the level of importance you attach to specific security standards and other sources of guidance in this category.**
Consider the level of urgency when you are choosing the level of importance.

	Very important	Important	Neutral	Unimportant	Very unimportant	Unsure
Pre employment screening	○	○	○	○	○	○
Employee termination procedure	○	○	○	○	○	○
Security training policies for staff	○	○	○	○	○	○
Dealing with psychological trauma	○	○	○	○	○	○
Identity management	○	○	○	○	○	○
Biometrics	○	○	○	○	○	○
Radio frequency ID	○	○	○	○	○	○
Building and facility access control	○	○	○	○	○	○
Entry searches	○	○	○	○	○	○
Video and closed circuit TV	○	○	○	○	○	○
Guards and patrols	○	○	○	○	○	○
Personnel protective equipment (eg suites, proof vests, respirators etc)	○	○	○	○	○	○
Crowd controllers	○	○	○	○	○	○
Public health security	○	○	○	○	○	○
Thermal imaging (for human temperature screening)	○	○	○	○	○	○

2. Are there any other specific security standards and other sources of guidance that you believe should have been included in this category? If so, please identify these below and rate the level of importance.
(500 character limit)

Critical Infrastructure and Support Systems Standardisation Survey

10. Physical Security

Assessing priorities for specific security standards and other sources of guidance

*** 1. Please indicate the level of importance you attach to specific security standards and other sources of guidance in this category.**
Consider the level of urgency when you are choosing the level of importance.

	Very important	Important	Neutral	Unimportant	Very Unimportant	Unsure
Perimeter security (e.g. lighting, fencing, bollards, chains, doors, windows, gates)	○	○	○	○	○	○
Construction security (e.g. construction materials, building structure, fire protection)	○	○	○	○	○	○
Crime prevention through environmental design	○	○	○	○	○	○
Security of facility utilities (water, gas, electricity, telecommunications and waste)	○	○	○	○	○	○
Signs, notices and instructions	○	○	○	○	○	○
Alarms, intruder alarms and detection devices	○	○	○	○	○	○
Locksets and security of keys	○	○	○	○	○	○
Safes and strong rooms	○	○	○	○	○	○
Bullet resistant panels	○	○	○	○	○	○
Control room security	○	○	○	○	○	○
Car parks and vehicle security (including vehicle control points)	○	○	○	○	○	○
Transport security	○	○	○	○	○	○
Postal and mail room safety	○	○	○	○	○	○
Food Safety	○	○	○	○	○	○
Packaging and seals	○	○	○	○	○	○
Hotel security	○	○	○	○	○	○
	○	○	○	○	○	○
	○	○	○	○	○	○

2. Are there any other specific security standards and other sources of guidance that you believe should have been included in this category? If so, please identify these below and rate the level of importance.
(300 character limit)

Critical Infrastructure and Support Systems Standardisation Survey

11. Methods for improving the implementation of security standards

*** 1. What could be done to make the implementation of security standards more successful?**

Check exactly 3 boxes to indicate your top 3 choices from the list below

- [ ] Training (e.g. induction, workshops, exercises, professional development and mentoring)
- [ ] Computer based training
- [ ] Technical assistance from consultants
- [ ] Consultants and practitioners capability certified
- [ ] User forums and support groups
- [ ] Products and services certified as security compliant
- [ ] Implementation handbooks and guidance material
- [ ] Reference sites and case studies
- [ ] Other (please specify) (10 characters limit)

2. Final comments

Enter any final comments you wish to make here.
(1000 character limit)