



**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



# Table of Contents

PURPOSE .....	1
BACKGROUND AND INTRODUCTION.....	1
THE PROJECT .....	3
KEY OBJECTIVES.....	3
PROJECT OUTPUT .....	5
DRIVERS FOR THE PROJECT .....	5
INTEGRATED SECURITY STANDARDS FRAMEWORK.....	6
STANDARDS AUSTRALIA’S NATIONAL CENTRE FOR SECURITY STANDARDS (NCSS) MODEL ....	7
GOVERNANCE, STRATEGY AND POLICY .....	8
RISK MANAGEMENT .....	8
INFORMATION SECURITY .....	9
PERSONNEL SECURITY .....	9
PHYSICAL SECURITY.....	9
CONCLUSION .....	10



## 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



**Asia-Pacific  
Economic Cooperation**

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

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



## Project Output

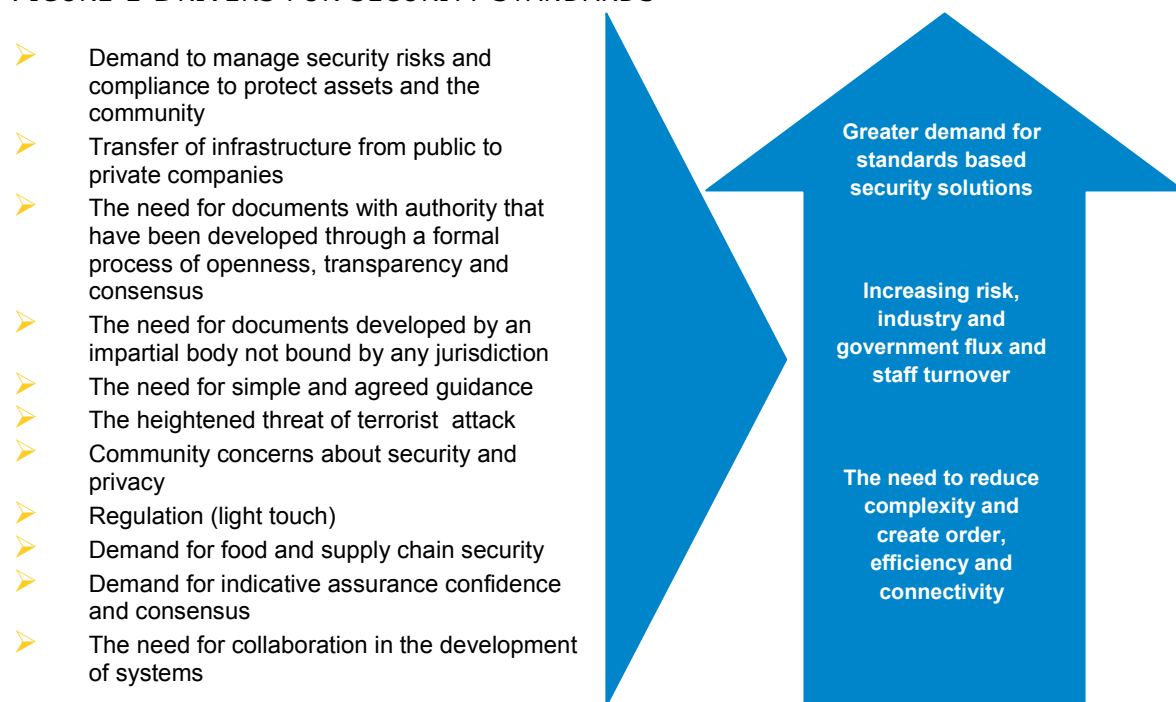
The major project output will be a final report that contains the following elements:

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





## 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.

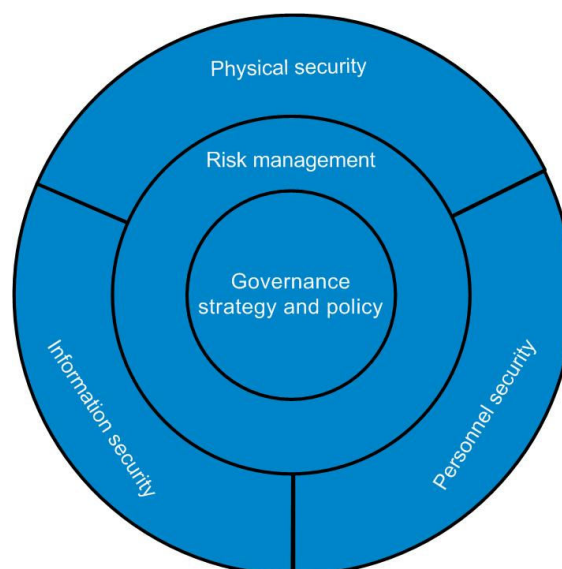
1. Identify the broad areas that require security standards.
2. Simple, communicable and easily understood.
3. Provide the basis for categorising, managing the scope and taking stock of existing standards activities as well as identifying gaps and priority areas.
4. Supported by key stakeholders.
5.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



## 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.