FACT SHEET - INFOCOMM SECURITY MASTERPLAN 2

IDA launched its infocomm masterplan, Intelligent Nation 2015 (“iN2015”), in June 2006, which aims to innovatively harness infocomm technologies to enhance our national competitiveness. It aims to transform Singapore into an intelligent nation, powered by infocomm. By 2015, an ultra high-speed, pervasive, intelligent and trusted infocomm infrastructure will be established and the Government, key economic sectors and society will be transformed through more sophisticated and innovative use of infocomm.

Singapore’s success in this area will be determined by its ability to provide a secure and trusted infocomm environment. To continue our infocomm security efforts, Singapore launched its first three-year Infocomm Security Masterplan in 2005. Against the backdrop of pervasive use of infocomm technology by the Singapore Government, businesses and society, the first Masterplan focused on further developing Singapore’s infocomm security capabilities and improving existing efforts to detect and prepare for cyber threats.

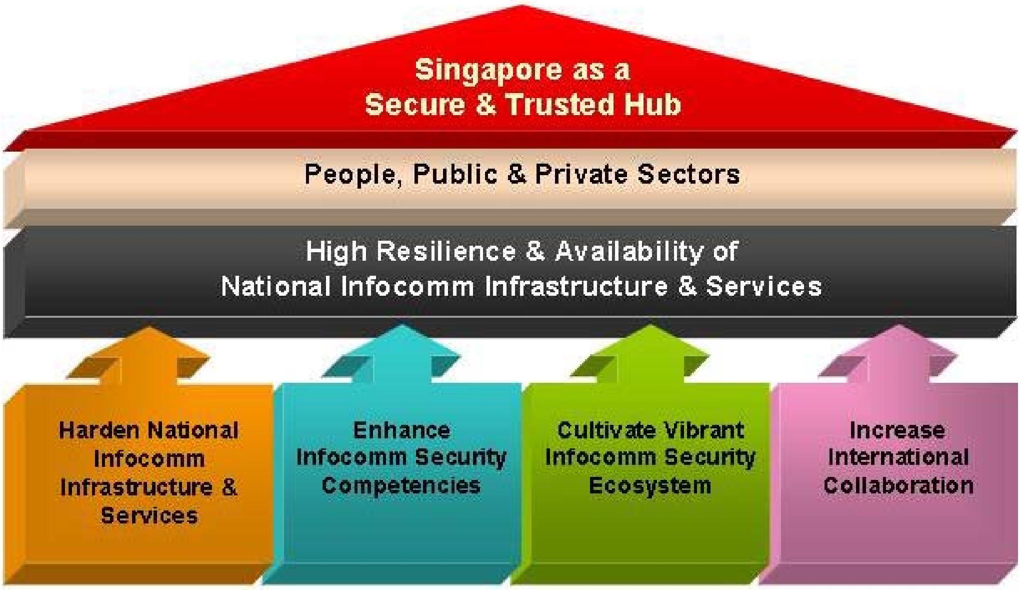
Significant achievements have been accomplished over the last three years. Through the first Masterplan, the Government enhanced its overall security situational awareness of the public sector and developed measures for business continuity readiness through robust frameworks and methodologies.

Moving forward, it is important to build on past successes and continue to enhance Singapore’s reputation as a secure and trusted hub. The Infocomm Security Masterplan 2 (MP2) is a five-year roadmap which aims to build upon the achievements of the first Masterplan by enhancing the tenacity of our economy against cyber attacks, thereby boosting the confidence of investors in choosing Singapore as a strategic and secure location for their investments.

Developed through a multi-agency effort led by the Infocomm Development Authority of Singapore (IDA), under the guidance of the National Infocomm Security Committee, the five-year Masterplan will see the public, private and people sectors working even more closely together to secure Singapore’s cyber space.

The framework for MP2, as shown in the figure below, depicts the vision, coverage, strategic outcome and the supporting strategic thrusts. Four strategic thrusts have been identified to support MP2’s aim of attaining high resilience and availability of the nation’s infocomm infrastructure and services:

- Harden national infocomm infrastructure and services
- Enhance infocomm security competencies
- Cultivate vibrant infocomm security ecosystem
- Increase international collaboration


Singapore as a
Secure & Trusted Hub
People, Public & Private Sectors
High Resilience & Availability of
National Infocomm Infrastructure & Services
Harden National Infocomm Infrastructure & Services
Enhance Infocomm Security Competencies
Cultivate Vibrant Infocomm Security Ecosystem
Increase International Collaboration

Strategic Thrust 1: Harden national infocomm infrastructure and services

It is vital that Singapore's national infocomm infrastructure and services are "hardened" against emerging threats since they form the foundation layer for other services and sectors. As such, programmes under this strategic thrust aim to enhance the resilience of our underlying foundation to combat cyber threats.

Strategic Thrust 2: Enhance infocomm security competencies

This strategic thrust looks at enhancing security competencies of infocomm users and infocomm security practitioners. For instance, new programmes will seek to catalyse greater adoption of essential security practices among infocomm users and ensure that infocomm security practitioners have adequate knowledge and capability in managing infocomm security risks.

Strategic Thrust 3: Cultivate vibrant infocomm security ecosystem

The presence of a vibrant infocomm security ecosystem will strengthen Singapore's capability to protect our national infocomm infrastructure and services. An active infocomm security research and development scene will help to ensure that a variety of up-to-date infocomm security solutions are available to counter constantly evolving infocomm security threats.

Strategic Thrust 4: Increase international collaboration

Given the borderless nature of cyber threats, it is therefore important to continue to work closely with our international counterparts. MP2 will also focus on exchanging best practices in infocomm security, and exploring collaborations in this area.

New Programmes in MP2

The Government, in close collaboration with the private sector, will roll out new initiatives to equip the public, private and people sectors with greater infocomm security competency, and build up the resilience of Singapore's national infocomm infrastructure and services against cyber attacks. The following new programmes will kick start MP2:

I. Association of Information Security Professionals (AISP)

The AISP is a Government and Industry collaboration which aims to transform infocomm security into a distinguished profession and build a critical pool of competent infocomm security professionals who subscribe to the highest professional standards. The first such association in Asia, it hopes to elevate the standing, professionalism and trust accorded to security practitioners here.

The AISP will govern the infocomm security profession and develop a code of conduct, qualifying criteria for membership and courseware. By governing the infocomm security profession, infocomm and end-user organisations who recruit such accredited infocomm security professionals can be assured that they are highly-proficient and will meet the security needs of their organisations. This also raises members' standing and distinguishes them as trusted and competent advisers and practitioners in infocomm security.

The AISP welcomes all infocomm security practitioners both experienced and new, including overseas professionals. To date, more than 120 members have come on board and a total of 900 members is expected by 2011. The qualifying criteria to be an AISP member are detailed in **Annex 1**.

The AISP is led by an Executive Committee, which is chaired by Mr Gerard Tan, Partner, PricewaterhouseCoopers, and comprises members from the public and private sectors. See **Annex 2** for details.

II. National Infocomm Scholarship for Infocomm Security

The National Infocomm Scholarship (NIS) was launched by the IDA in 2004 to develop infocomm leaders and ensure a pipeline of talent for the infocomm industry. Specifically it aims to:

- Make infocomm a top career choice among top students;
- Create 'industry-ready' scholars to be injected into Singapore's infocomm industry; and
- Ensure that the industry has a fair share of top talent to sustain its future growth

Under MP2, the NIS will support one of the Masterplan's strategic thrusts to enhance infocomm security competencies. For a start, e-Cop Singapore Private Limited, Frontline Technologies Corporation Limited, the IDA and Symantec Singapore Pte Ltd will offer up to 20 scholarships to students over the next five years for a tertiary education in infocomm security.

The NIS will continue to offer scholars the opportunity to be nurtured by leading infocomm security multinational corporations, local companies and Government agencies during their studies. This includes mentorship with companies and work stints overseas of up to six months. Upon graduation, all NIS recipients will serve their bond with the sponsoring organisation.

The scholarship, available to both local and foreign students, is open to those who have completed their junior college or polytechnic studies and are keen to pursue a full time infocomm-security related degree in either a local or foreign university of their choice. Interested students can apply for this scholarship at www.talent.singaporeinfocomm.sg. The application period is from January to March every year.

III. Cyber Security Awareness Alliance

As infocomm becomes increasingly pervasive, it is imperative to raise Singapore's infocomm security competency among the public, private and people sectors. To that end, the IDA and like-minded partners from the public and private sectors have formed the Cyber Security Awareness Alliance (Alliance) in April 2008.

As a collaborative body, the Alliance will amalgamate efforts from its members by bringing together different strengths and resources. The aim of the Alliance is to:

- Build a positive culture of cyber security in Singapore where infocomm users adopt essential security measures such as firewall and anti-virus software; and
- Raise awareness and adoption of essential infocomm security practices for the private and people sectors.

The Alliance members will reach out to the public, private and people sectors through:

- Organising and sponsoring events such as seminars, talks, road shows and training workshops;
- Creating infocomm security-related collateral for user and business groups, and making it available either online, in print or through broadcast media; and
- Offering infocomm security advice for user and business groups, through online, print or broadcast channels.

As a start, the term of the Alliance will be for one year from April 2008 – March 2009. It will be co-chaired by Mr Leong Keng Thai, Deputy Chief Executive/Director-General (Telecoms), IDA and Mr Pek Yew Chai, Chairman, Singapore infocomm Technology Federation (SiTF). Currently, the Alliance comprises representatives from the Government, private enterprises, associations and non-profit organisations. See **Annex 3** for details. Industry players in the infocomm security space who are keen to be part of the Alliance can approach the IDA or SiTF.

IV. Cyber Security Exercises

Cyber security exercises will enhance the emergency readiness and responsiveness to large-scale cyber attacks at the national level. These exercises will serve as a mechanism to assess our capability and readiness to respond and recover from debilitating events that cause widespread disruptions. In addition, these exercises will also help to identify areas that will further improve the resilience of our national infrastructure and services. Both the Government and the private sector will be involved in conducting these exercises.

V. Sector-Specific Infocomm Security Programmes

As each sector has its unique security requirements, a ‘one-size-fits-all’ approach, where a single solution is developed to meet the needs of different sectors will be insufficient. Sector-specific infocomm security programmes will ensure that the infocomm infrastructure and services in each sector remain secure.

The Government will work with critical infrastructure owners to assess and develop customised solutions that meet each sector’s unique security requirements. It will start with the Government, infocomm and energy sectors as an earlier assessment from the first Masterplan has shown these sectors to be the most critical in Singapore.

A new study will be performed on each of the sectors to identify areas that require further improvement. Based on this new study, necessary measures will be put in place to better detect and prevent infocomm security incidents. Education and training will also be provided to owners of the critical infocomm infrastructure within these sectors.

VI. International Collaboration

The Government will continue to actively engage other countries and contribute to global efforts in combating cyber threats. For instance, Singapore will be hosting Meridian 2008, a key international security conference in October this year. Held in Asia for the first time, more than 100 senior government policy-makers from around the world will gather here to exchange best practises on Critical Infocomm Infrastructure Protection (CIIP). Participants will share their experiences on issues such as national strategies, policy formulation and implementation challenges, and form working groups to facilitate international collaboration on CIIP-related issues.

Annex 1

Qualifying Criteria to be an AISP Member:

a. Fellows:

i. Persons who have made exemplary contributions to the field or profession of information security may be invited for membership under the Fellow category.

ii. The Executive Committee shall decide, upon the recommendation of a Membership Review Committee, whether to admit any such person to Fellowship.

b. Ordinary Members:

i. Persons who meet the qualification criteria set by the Executive Committee and who are employed in Information Security activities or professional practices related to Information Security for such periods of time as may be determined by the Executive Committee from time to time. For the avoidance of doubt, these qualifications apply only at the time of application for the membership.

c. Associate Members

i. Persons who do not meet the qualification criteria for Ordinary membership but have met other relevant qualification criteria set by the Executive Committee and who are employed in information security activities or professional practices related to information security for such periods of time as may be determined by the Executive Committee from time to time.

ii. Associate Members shall have no voting rights and shall not be eligible to stand for office.

d. Student Members:

i. Persons who do not qualify for any other category of Membership and who are pursuing approved courses in educational institutions or professional bodies (whether in Singapore or overseas) with the expressed intention of obtaining qualifications recognised by the AISP.

ii. Student Members shall have no voting rights and shall not be eligible to stand for office.

Annex 2

Members from the Executive Committee of the AISP are from the following organisations.

	Organisation
1.	Auditor-General's Office
2.	Cable & Wireless
3.	EC Frontier
4.	Infocomm Development Authority of Singapore
5.	Microsoft
6.	Ministry of Defence
7.	Nanyang Polytechnic
8.	Oversea-Chinese Banking Corporation
9.	PCS Security
10.	PricewaterhouseCoopers
11.	Reuters Asia
12.	Singapore Computer Society

Annex 3

Organisations represented on the Cyber Security Awareness Alliance:

	Organisation
1.	Association of Small and Medium Enterprises
2.	BT Frontline Pte Ltd
3.	Cisco Systems (USA) Pte Ltd
4.	eBay Singapore
5.	Hewlett-Packard Singapore (Sales) Pte Ltd
6.	Infocomm Development Authority of Singapore
7.	Juniper Networks (Singapore) Pte Ltd
8.	McAfee (Singapore) Pte Ltd
9.	Microsoft Singapore Pte Ltd
10.	National Crime Prevention Council
11.	Quantiq International Pte Ltd
12.	Singapore Business Federation
13.	Singapore Chinese Chamber of Commerce & Industry
14.	Singapore infocomm Technology Federation
15.	Singapore Police Force
16.	Symantec Singapore Pte Ltd