National Programmes

Working closely with the people, private and public sectors, IDA has spearheaded a series of national infocomm security masterplans to combat ever-evolving cyber threats such as hacking, virus attacks and cyber terrorism, in order to maintain a secure infocomm environment for the government, businesses and individuals.

Infocomm Security Masterplan 2 (MP2)

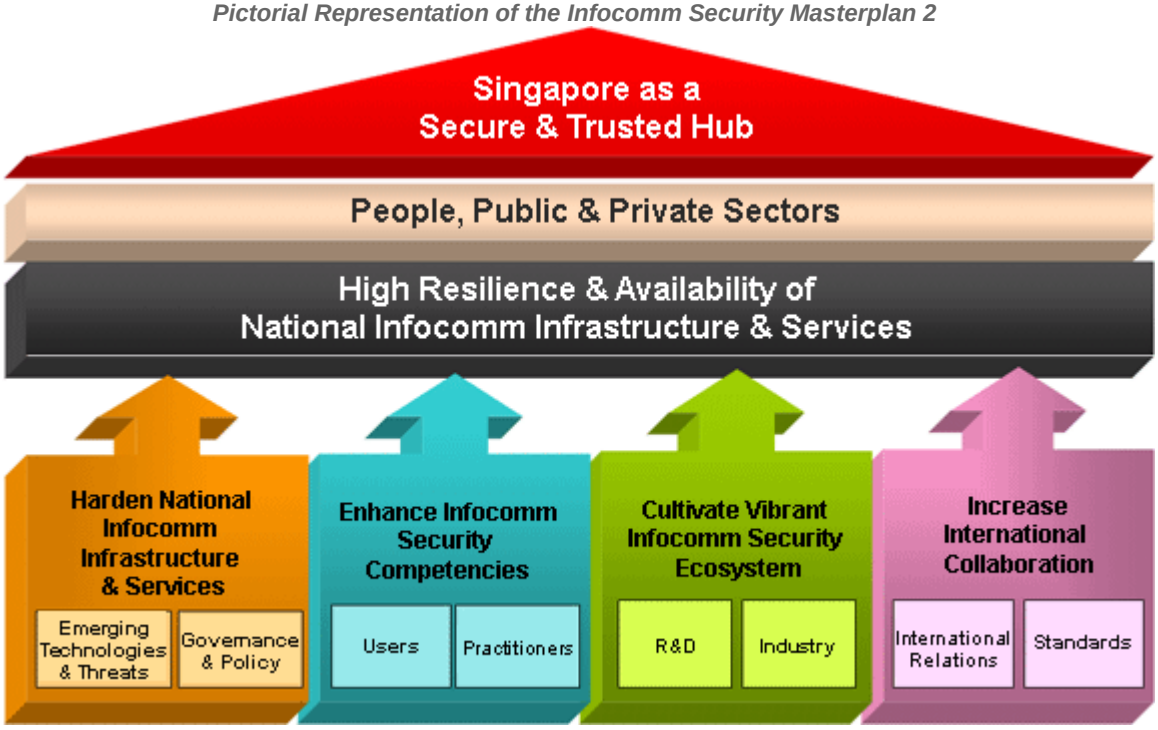
The **Infocomm Security Masterplan 2 (MP2)**, launched in 2008, is a five-year roadmap which aims to build upon the achievements of the first Masterplan by enhancing the tenacity of our economy against cyber attacks, thereby boosting the confidence of investors in choosing Singapore as a strategic and secure location for their investments.

Developed through a multi-agency effort led by 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

Pictorial Representation of the Infocomm Security Masterplan 2



Highlights of Selected MP2 Initiatives

To achieve the objectives of MP2, some of the key initiatives include:

The **Association of Information Security Professionals (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 **National Infocomm Scholarship for Infocomm Security** support one of the Masterplan's strategic thrusts to enhance infocomm security competencies. It aims to groom scholars in the area of infocomm security and to help ensure that the industry has a fair share of top talents. Through this initiative, scholars have 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.

The **Cyber Security Awareness Alliance** was established to raise Singapore's infocomm security competency among the public, private and people sectors. It amalgamate efforts from its members by bringing together different strengths and resources to build a positive culture of cyber security in Singapore where infocomm users adopt essential security measures such as firewall and anti-virus software. It also has programmes to raise awareness and adoption of essential infocomm security practices in the private and people sectors.

The **Cyber Security Exercises** enhance the emergency readiness and responsiveness to large-scale cyber attacks at the national level. These exercises 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.

The **Sector-Specific Infocomm Security Programmes** assess and develop customised solutions that meet the unique security requirements of each sector. It will start with the Government, Infocomm and Energy sectors as earlier assessment from the first Masterplan has shown these sectors to be among the most critical in Singapore.

Infocomm Security Masterplan and National Trust Framework

The **Infocomm Security Masterplan (ISMP)** provides the overarching plan in Singapore's continued national efforts to enhance cyber security. Launched in February 2005, this three-year (FY2005 - FY2007) strategic roadmap is the result of extensive private and public sector feedback to increase the resilience of national critical infrastructure from cyber attacks and to maintain a secure infocomm environment for government, businesses and individuals. The Masterplan has identified six strategies to secure Singapore's infocomm environment:

a. Securing the People Sector

b. Securing the Private Sector

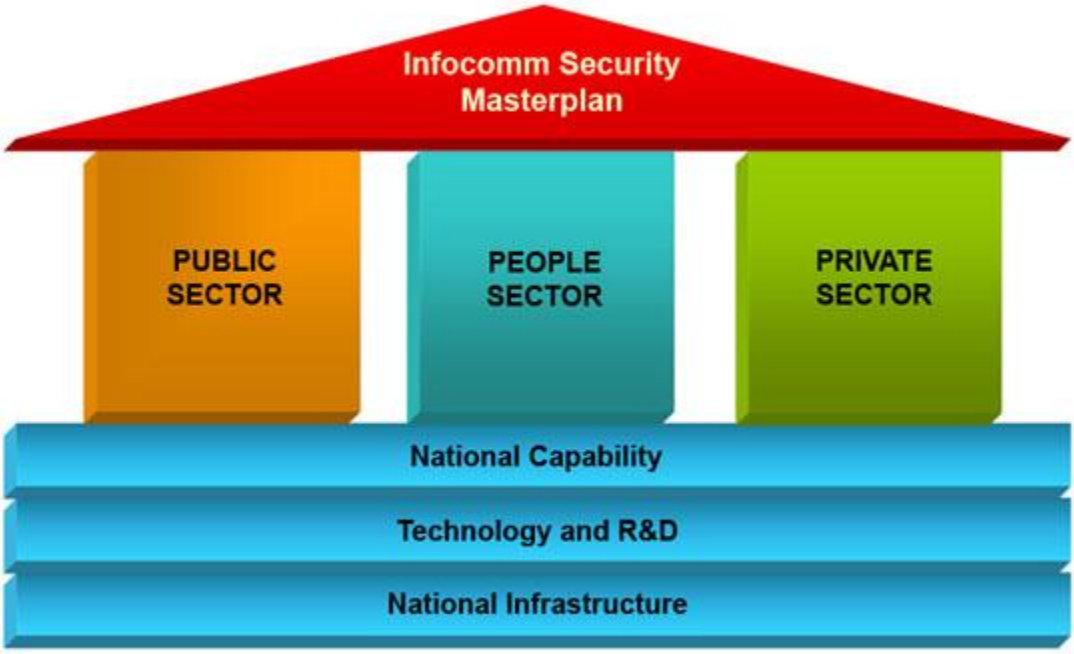
c. Securing the Public Sector

d. Developing National Capability

e. Cultivating Technology and R&D

f. Securing National Infrastructure

Pictorial Representation of the Masterplan Framework



Complementary to the ISMP is the **National Trust Framework (NTF)**, which was conceptualised in 2006 as part of IDA's iN2015 Masterplan. With the pervasive adoption of online services such as banking, healthcare and commerce, a trusted infocomm environment is essential to minimise security risks to valuable and sensitive data. Thus, the objective of the NTF is to develop a national framework that provides greater assurance and trust, so that Singapore can continue to leverage on its infocomm successes. To enhance Singapore's reputation as a trusted hub, the NTF has identified four key strategic thrusts:

a. Trusted infrastructure development

b. Manpower development

c. Education and adoption

d. Regulation

Highlights of Selected ISMP and NTF Initiatives

To achieve the objectives of the ISMP and the NTF, some of the key initiatives that Singapore has undertaken include:

The **National Cyberthreat Monitoring Centre (NCMC)** provides the Singapore Government with the capability for early detection of potentially devastating cyber attacks and the ability to respond to cyber security incidents in real time. The NCMC consists of the Cyber Watch Centre (CWC) that provides round-the-clock monitoring of cyber-threats to critical installations in the public sector and the Threat Analysis Centre (TAC) that focuses on the analysis of cyber threats.

The **National Authentication Framework (NAF)** aims to catalyse e-business through the pervasive deployment of strong authentication infrastructures across key sectors. The objective of the NAF is to enable a consistent second-factor authentication experience for end-users accessing key electronic services, such as banking, telecommunications and government services.

The **Critical Infocomm Infrastructure Surety Assessment (CII-SA)** was set up to assess the infocomm security readiness of Singapore's critical infocomm infrastructure (CII), and to ascertain the adequacy of the infocomm protection measures implemented by infrastructure owners and operators.

The **Business Continuity Readiness Assessment Framework** and the **Infocomm Security Health Scorecard** were put in place to measure the level of security readiness and preparedness of the public sector. The **Business Continuity Readiness Assessment Framework** established a common framework to measure the level of readiness of agencies in resuming business operations in the event of service and operation disruptions due to infocomm security incidents. The **Infocomm Security Health Scorecard** established a scorecard to assess the level of infocomm security preparedness of public sector agencies.