Approved by the Executive Yuan on December 25, 2013

# National Strategy for Cybersecurity Development Program

(2013 to 2016)

National Information and Communication Security Taskforce, Executive Yuan

December 2013

# Table of Contents

# Chapter 1 Introduction

With the widespread utilization of information technology and the continuing evolvement of the Internet in the 21st century, information and communication technology (ICT) applications have become ubiquitous and have changed our everyday lives. In tandem with the ICT revolution however ICT-related security issues have become a major issue of growing concern, and as a result in many countries information and communication security is now in the spotlight.

To strengthen Taiwan's capability to deal with information and communication security issues, the Executive Yuan approved the National Information and Communication Infrastructure Security Mechanism Plan (2001-2004) (the Phase 1 Mechanism Plan) at its 2718th meeting on January 17, 2001, and established the National Information and Communication Security Taskforce (the Taskforce), the purpose of which is to actively implement ICT security infrastructure policy.

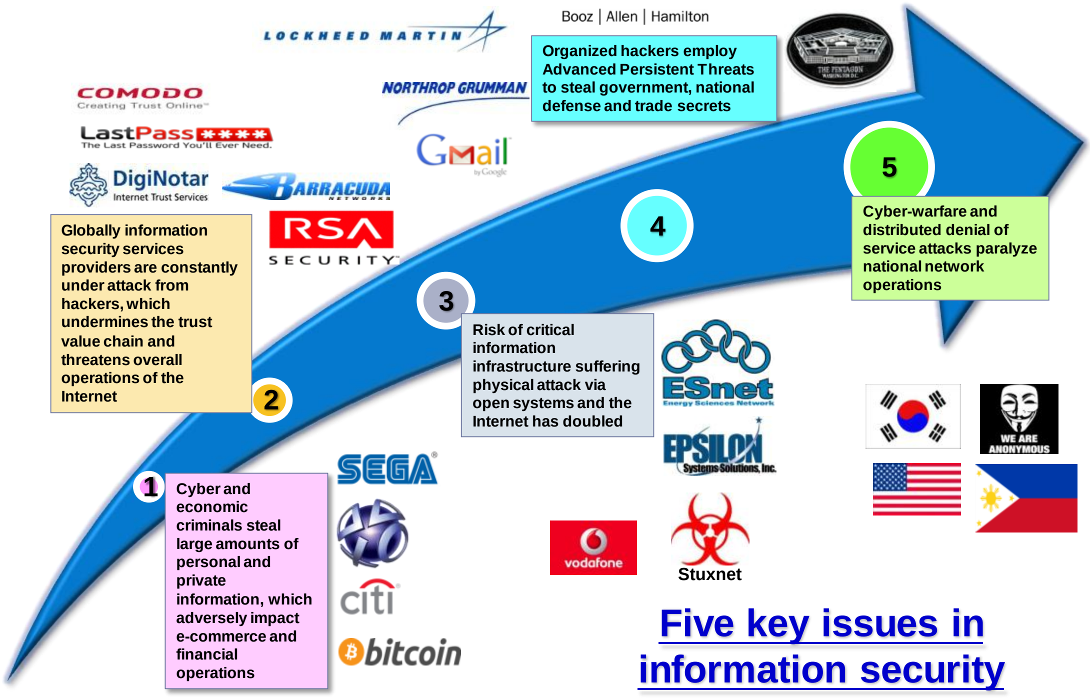
Between 2005 and 2012, the Executive Yuan carried out the National Information and Communication Infrastructure Security Mechanism Plan (2005-2008) (the Phase 2 Mechanism Plan) and the National strategy for Cybersecurity Development Program (2009-2012) (the Phase 3 Development Program). Consequently, with the collaborative efforts of agencies from central government, special municipalities and local government, the interim objective of "establishing an overall information security protection system and improving information security protection capabilities" has been achieved in the prescribed order.

Taiwan has a unique political and economic environment, and when confronted with a complex and ever-changing global ICT environment and the information security threats, it is imperative that work related to the implementation and refinement of ICT security should be continued. Therefore the Taskforce has conducted the necessary research and is now proposing the National Strategy for Cybersecurity Development Program (2013-2016) (the Program), which is designed to be the basis on which all government agencies implement information and communication security plans in the current phase.

# Chapter 2 Global Information Security Development Trends

## I Status of Global Information Security Threats

The Internet has brought great convenience and speed to our lives. However the prevalence of the Internet and related changes in consumer behavior mean that issues such as cyber crime and protection of personal information and privacy have become a source of great concern affecting national security and social stability. Due to this situation the world is now facing some serious information security threats (see Figure 1).



1 Cyber and economic criminals steal large amounts of personal and private information, which adversely impact e-commerce and financial operations

2 Globally information security services providers are constantly under attack from hackers, which undermines the trust value chain and threatens overall operations of the Internet

3 Risk of critical information infrastructure suffering physical attack via open systems and the Internet has doubled

4 Organized hackers employ Advanced Persistent Threats to steal government, national defense and trade secrets

5 Cyber-warfare and distributed denial of service attacks paralyze national network operations

Five key issues in information security

Figure 1. Global information security threats

### A Rampant organized cyber crime

Around the world information security threats have evolved from individual threats that are nothing more than a display of hacking skills to organized and economically or politically motivated intrusions. Recently cybercriminal organizations have become highly specialized. This, coupled with the fact that launch of cyber warfare is not constrained by time or space, means that the first attack can now become the decisive battle, implying that the concept and scope of national security have fundamentally and substantially changed.

B Theft of personal information and financial fraud incidents abound

Hackers embed malicious code into victims' computers via e-mail social engineering or employ methods such as exploiting web application vulnerabilities and implanting Trojan horse viruses into web pages in order to steal private personal information. They even conspire with criminal organizations to perpetrate financial fraud. For example, Japan's Play Station Network (PSN) was attacked, resulting in 80 million personal records being leaked in April 2011.

C Critical information infrastructures facing increasing information security risks

In the age of the digital economy, destruction of important information and communication facilities will inevitably impact the economy, people's livelihoods and overall government operations. The Supervisory Control And Data Acquisition (SCADA) of various types of Critical Infrastructures (CIs) usually lack robust information security protection designs, and as a result both are major targets for hackers.

D Intensification of Advanced Persistent Threat

Advanced Persistent Threat (APT) attacks are characterized by having specific targets, being inconspicuous, covert, employing diverse tactics and being customizable. Recently government systems in the U.S., Britain, France, Germany, New Zealand and Australia were reportedly breached by APT attacks seeking to steal important confidential and sensitive data.

E Zero-day Attack resulting in difficulties in information security defense

A "Zero-day Attack" refers to an attack that exploits an unknown vulnerability in a computer software, one that developers have had no time to address and patch. Hackers often use a fake identity to send e-mail with intriguing subject and content, combined with file attachments containing zero-day attacks, to carry out e-mail social engineering attacks. Once the recipient opens the attachment of the e-mail, zero-day malware is implanted.

## II Information security policy development in major countries

In recent years, major countries and regions have actively implemented new information security policies to respond to the current global status of information security threats. Below a list of evolving trends are provided as a reference source for information security policymakers and strategists in Taiwan:

### A Raising information security issues to the level of national security

After taking office in 2009, U.S. President Obama solicited the opinions and point of view of various experts and scholars to undertake a comprehensive assessment of the past and present status of U.S. cybersecurity policies. Obama expressed his commitment to establishing a reliable and robust information and communication infrastructure. He also announced a new plan to strengthen cybersecurity in the U.S. by upgrading cybersecurity to the level of national security.

In South Korea, the government initiated the "e-Korea Vision 2006" policy to promote high-speed broadband Internet services, and in response to the impact of information security threats, the government also incorporated information security into the basic national policy "Broadband IT Korea Vision 2007."

In Japan, for the purposes of enhancing national competitiveness and sustaining social and economic development, information security policies have focused on enhancing national security and systems security, improving information security education and promoting international cooperation in recent years.

During the Fourth Plenary Session of the 16th Communist Party of China Central Committee held in 2008, China recognized information security as a major component in national security and unequivocally proposed a policy of "strengthening national security awareness and perfecting national security strategy" to ensure "the country's political, economic, cultural and information security."

### B Emphasizing the importance of protecting citizens' rights, in

particular protection of personal information and privacy

In 2011, the U.S. released the National Strategy for Trusted Identities in Cyberspace (NSTIC), designed to advance the development of technologies or platforms for making online transactions at as high a trust level as possible.

In 2008, the Singapore government initiated a five-year information and communication security roadmap to provide a secure environment to enable high-speed Internet and ICT security infrastructures to create more value-added services, such as area-based marketing, logistics tracking and Internet services with higher adaptability, which can be applied to the banking, education and healthcare industries.

In Japan, the Japanese Personal Information Protection Act (JPIPA) was passed in 2005, which expressly stipulates that enterprises that retain personal information have an obligation to protect data and prevent it from being leaked. The government also listed specific measures on enhancing protection of citizens and users and promotion of personal information protection in *Information Security 2011*.

C Increasing emphasis on security issues related to cloud computing

The U.S. Federal Government implemented cloud computing technologies and services for the websites of government agencies in late 2009 as an important basis for the Obama Administration to carry out budget cuts, enhance administrative efficiency and create a greener environment. The administration also appointed Vivek Kundra as the new Federal Chief Information Officer and launched a series of Government Cloud restructuring programs. In late 2011, the U.S. National Institute of Standards and Technology (NIST) issued a series of special documents, which stressed the importance, issues and recommended practices regarding cloud computing technology, including SP 800-144 (Draft Guidelines on Security and Privacy in Public Cloud Computing), SP 800-145 (The NIST Definition of Cloud Computing), SP 800-146 (Draft Cloud Computing Synopsis and Recommendations) and SP 500-293 Volume I & Volume II (US

Government Cloud Computing Technology Roadmap).

In Japan, policies and measures concerning the importance of cloud computing security were emphasized in Secure Japan 2010, which included ensuring information security in cloud computing technology, standardization of cloud computing security programs, small and medium enterprise cloud computing security, development of checklists for cloud service levels, development of high reliability/energy conservation network control technology for cloud services, strategic research and development for promoting information security, and research on new-generation information security technologies. In China, the planning of seven strategic emerging industries will be the focus of national development as listed in the Twelfth Five-Year Plan. In particular, the development of cloud computing as a new generation of information technology will be an area of major importance.

### D Emphasizing government/private sector or industry-academic cooperation issues

In the U.S., 85% of all CIs are operated by the private sector. For this reason the government has proposed a national policy on substantive protection of the country's CIs, which will provide a model on which cooperation and alliances between the government, CI operators, civil organizations and individuals can be based. The national policy provides specific strategies to enhance national security.

Japan released the Information Security Strategy for Protecting the Nation program in 2010 and continued the model of cooperation between the public and private sector, which focuses on enhancing planning directions and implementation institutions from the perspectives of security protection and crisis management in order to achieve better policy results.

China's National Medium- to Long-range Program for Scientific and Technological Development proposes that the "information industry and modern service industries" be given priority as major industries for long-term development. In "Facing information security for core applications," the directions for key information security technologies are pointed out, and measures to encourage development in four areas (i.e. tax breaks on research and development, government procurement, civilian-military collaboration and international cooperation) are designed to advance the development of China's information security technologies.

In South Korea, major enterprises enjoy collaboration with academic institutions, and they have invested large sums of capital in achieving the country's own important information technologies and results.

E Importance of international cooperation on protection and exchange

In the U.S., President Obama announced the government initiative International Strategy for Cyberspace in 2011, which outlines the government's international cyberspace strategies, covering full integration and cooperation between the public and private sector, spanning domestic to international and international to global strategies, as well as combining traditional values and Internet technology applications associated with America's democratic and free-market ideals, thus laying a foundation for a post-911 new order in cyberspace.

South Korea is also in close cooperation with international organizations, including development areas in collaboration with these international organizations, and has provided policy advice to governments in other countries, as well as carried out administrative measures associated with e-government and the training of civil servants.

In Singapore, the government announced the Intelligent Nation 2015 (iN2015) Master Plan in June 2006, the main purposes of which are to achieve innovation, integration and internationalization. The government hopes that by 2015 the country will be able to "establish an intelligent nation and global city with ICT technology," making information and communication technologies pervasive and an integral part of daily life, work and leisure activities, as well as developing Singapore into a smart city based on four elements, "technology," "infrastructure," "enterprise" and "manpower."

In Japan, Information Security 2011 was introduced to strengthen the country's information security policy in order to adapt to the changing security landscape and to strengthen international cooperation, e.g. improving alliances with the U.S., ASEAN countries and the EU. Japan also aims to implement specific measures through international forums and conferences such as the Asia-Pacific Economic Cooperation (APEC), ASEAN Regional Forum (ARF), International Telecommunication Union (ITU), Meridian and International Watch and Warning Network (IWWN).

In China, the Eleventh Five-Year Plan for National Information Security Standardization focuses on research of information security strategies and basic theory, development of information security standards and promotion, and participation in international standardization activities on a regular basis.

# Chapter 3 Analysis of current status of information security

## I. Organization

Pursuant to the Guidelines for Establishing the National Information and Communication Security Taskforce, Executive Yuan, which was amended in January 2013, the Taskforce is responsible for developing national information and communication security policy and notification and response mechanisms, review and consultation on major programs, and coordination and supervision of inter-ministerial affairs concerning information and communication security. Two systems have been established under the Taskforce: Internet Protection and Cybercrime Investigation and Prevention (refer to Figure 2 for the detailed organizational structure of the Taskforce).

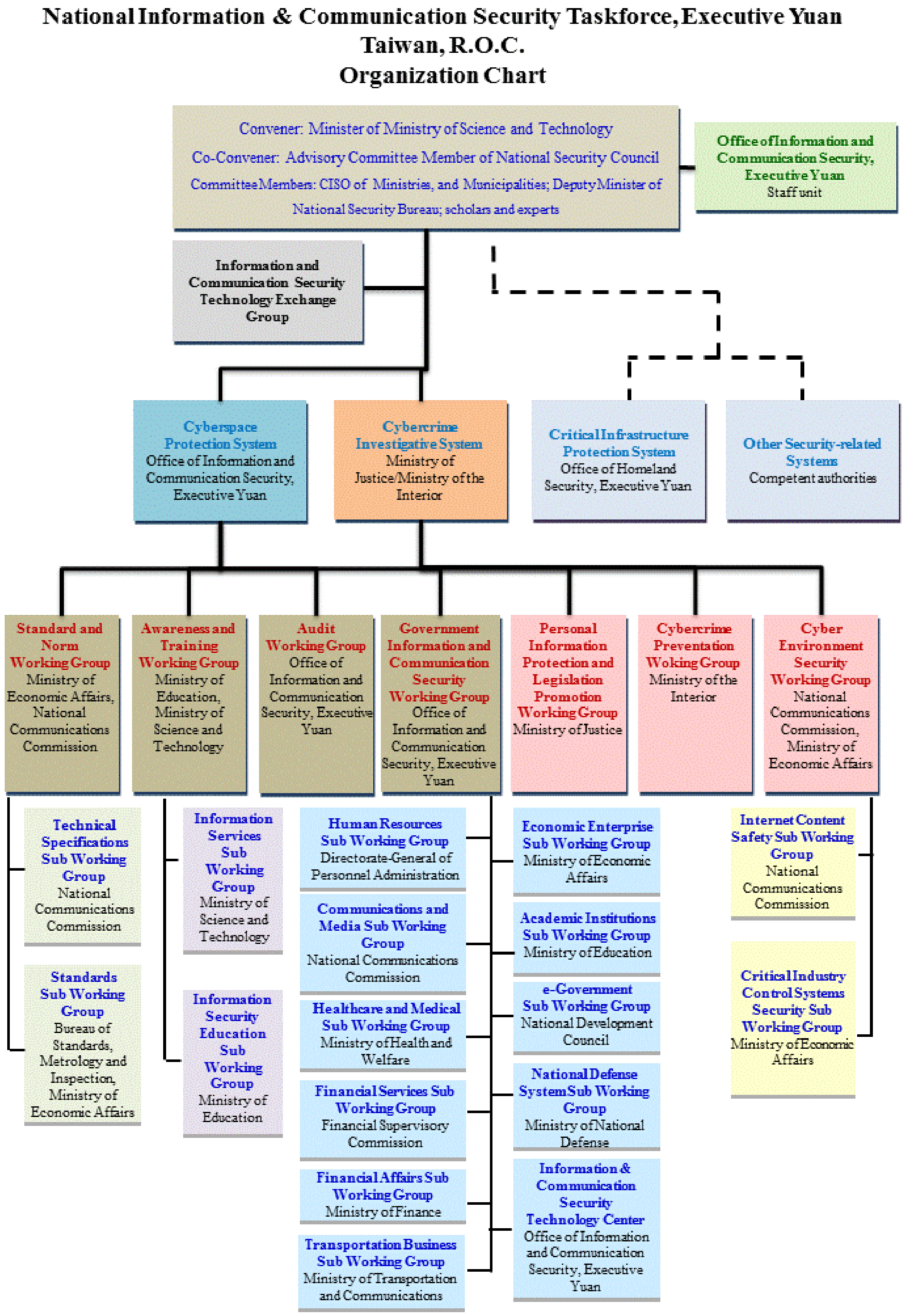

National Information & Communication Security Taskforce, Executive Yuan
Taiwan, R.O.C.
Organization Chart
Convener: Minister of Ministry of Science and Technology
Co-Convener: Advisory Committee Member of National Security Council
Committee Members: CISO of Ministries, and Municipalities; Deputy Minister of National Security Bureau; scholars and experts
Office of Information and Communication Security, Executive Yuan
Staff unit
Information and Communication Security Technology Exchange Group
Cyberspace Protection System
Office of Information and Communication Security, Executive Yuan
Cybercrime Investigative System
Ministry of Justice/Ministry of the Interior
Critical Infrastructure Protection System
Office of Homeland Security, Executive Yuan
Other Security-related Systems
Competent authorities
Standard and Norm Working Group
Ministry of Economic Affairs, National Communications Commission
Awareness and Training Working Group
Ministry of Education, Ministry of Science and Technology
Audit Working Group
Office of Information and Communication Security, Executive Yuan
Government Information and Communication Security Working Group
Office of Information and Communication Security, Executive Yuan
Personal Information Protection and Legislation Promotion Working Group
Ministry of Justice
Cybercrime Preventation Woking Group
Ministry of the Interior
Cyber Environment Security Working Group
National Communications Commission, Ministry of Economic Affairs
Technical Specifications Sub Working Group
National Communications Commission
Standards Sub Working Group
Bureau of Standards, Metrology and Inspection, Ministry of Economic Affairs
Information Services Sub Working Group
Ministry of Science and Technology
Information Security Education Sub Working Group
Ministry of Education
Human Resources Sub Working Group
Directorate-General of Personnel Administration
Communications and Media Sub Working Group
National Communications Commission
Healthcare and Medical Sub Working Group
Ministry of Health and Welfare
Financial Services Sub Working Group
Financial Supervisory Commission
Financial Affairs Sub Working Group
Ministry of Finance
Transportation Business Sub Working Group
Ministry of Transportation and Communications
Economic Enterprise Sub Working Group
Ministry of Economic Affairs
Academic Institutions Sub Working Group
Ministry of Education
e-Government Sub Working Group
National Development Council
National Defense System Sub Working Group
Ministry of National Defense
Information & Communication Security Technology Center
Office of Information and Communication Security, Executive Yuan
Internet Content Safety Sub Working Group
National Communications Commission
Critical Industry Control Systems Security Sub Working Group
Ministry of Economic Affairs

Figure 2. Structure of National Information and Communication Security Taskforce, Executive Yuan

The Taskforce was established in January 2001, and in earlier years the Science and Technology Advisory Group (STAG) took on an advisory role. Subsequently, in consideration of a deteriorating information security situation, the Executive Yuan amended the Guidelines for Establishing the National Information and Communication Security Taskforce in March 2011 and set up the Office of Information and Communication Security in order to enhance national information security policy planning, improve efficiency of information security notification and contingency planning, and expedite implementation of major information security programs. In coordination with Executive Yuan restructuring on January 1, 2012, the Office of Information and Communication Security became a permanent taskforce of the Executive Yuan. In accordance with the Guidelines for Establishing the Office of Information and Communication Security, the Office is charged with the following responsibilities in addition to serving as advisor to the Taskforce:

A Development and promotion of national information security policy and measures.

B Notification, response, and review of national information security incidents.

C Promotion and review of major national information security programs.

D Coordination, liaison and promotion of national information security-related legislation and regulations.

The following lists the subsystems and groups within the Taskforce and their corresponding responsible agencies and tasks:

A Cyberspace protection system: Headed by the Office of Information and Communication Security, Executive Yuan, responsible for the integration of information security protection resources and promotion of information security policy; it comprises the following working groups:

(1) Standard and Norm Working Group: Headed by the Ministry of Economic Affairs, responsible for developing certification and verification standards and systems for

information security products and management systems; promoting technical standards of information security technology; and carrying out control, development and maintenance of government agencies' information security operating standards and reference guidelines.

(2) Audit Working Group: Headed by the Office of Information and Communication Security, Executive Yuan, responsible for promoting and implementing information security audit systems and providing assistance to government agencies in strengthening the integrity and effectiveness of information security protection responsibilities; the Office is also responsible for reducing information security risks through continuous improvement.

(3) Awareness and Training Working Group: Headed by the Ministry of Education, responsible for promoting basic education in information security, strengthening information security in the educational system, raising national information security knowledge and awareness, providing information security services, and establishing an information security personnel training system.

(4) Government Information and Communication Security Working Group: Headed by the Office of Information and Communication Security, responsible for planning and promoting security mechanisms of various e-government services, providing guidance to government agencies on information security technical services, information security protection and contingency planning, and integrating and improving information security manpower utilization within government agencies.

B Cybercrime Investigative System: Co-organized by the Ministry of Justice and Ministry of the Interior, responsibilities of which include preventing cybercrime, protecting citizens' privacy, and establishing information and communication infrastructure security; comprises the following working groups:

(1) Personal Information Protection and Legislation Promotion Working Group: Headed by the Ministry of Justice, responsible for reviewing and amending laws and regulations concerning protection of citizens' privacy and prevention and control of cybercrime; and establishing a legal environment that fosters trust and reliability.

(2) Cybercrime Preventation Woking Group: Headed by the Ministry of the Interior, responsible for conducting cybercrime investigations and preventing computer-related crimes.

(3) Cyber Environment Security Working Group: Headed by the National Communications Commission, responsible for promoting Internet content security, cybercrime prevention, enhancing control system security of critical industries, and establishing secure and trustworthy information and communication infrastructure mechanisms.

In order to be kept abreast of the latest trends in information security technologies and enhance information security capability, the Taskforce established the Information Security Technology Exchange Group in August 2012. Representatives from industry, government, academic, and research institutions are invited to participate in seminars on a quarterly basis to discuss information security technology and share how specific or major information security incidents are handled, causes of incidents and recommendations for improvement.

## II. Major Information Security Policy Milestones

Since the Taskforce was established in January 2001, major information security plans or programs, each lasting four years, implemented over three phases have been introduced (see Figure 3 for details). These initiatives have effectively achieved a high degree of information security readiness in Taiwan. The highlights of each program or plan are outlined below.

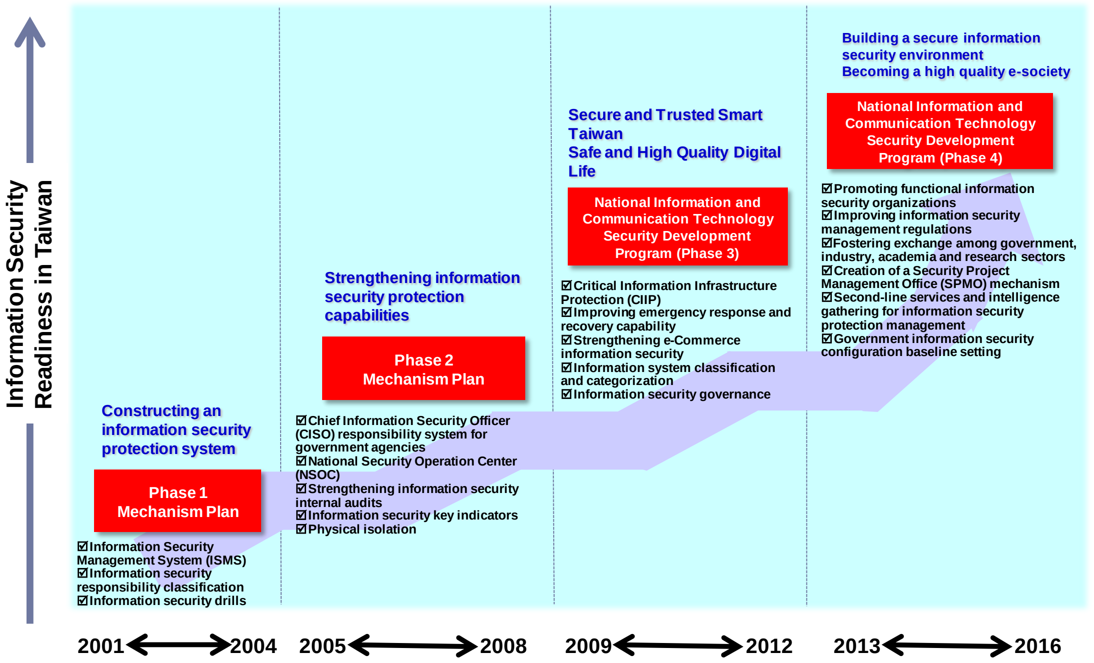

Information Security
Readiness in Taiwan
Constructing an information security protection system
Phase 1 Mechanism Plan
☑Information Security Management System (ISMS)
☑Information security responsibility classification
☑Information security drills
Strengthening information security protection capabilities
Phase 2 Mechanism Plan
☑Chief Information Security Officer (CISO) responsibility system for government agencies
☑National Security Operation Center (NSOC)
☑Strengthening information security internal audits
☑Information security key indicators
☑Physical isolation
Secure and Trusted Smart Taiwan
Safe and High Quality Digital Life
National Information and Communication Technology Security Development Program (Phase 3)
☑Critical Information Infrastructure Protection (CIIP)
☑Improving emergency response and recovery capability
☑Strengthening e-Commerce information security
☑Information system classification and categorization
☑Information security governance
Building a secure information security environment
Becoming a high quality e-society
National Information and Communication Technology Security Development Program (Phase 4)
☑Promoting functional information security organizations
☑Improving information security management regulations
☑Fostering exchange among government, industry, academia and research sectors
☑Creation of a Security Project Management Office (SPMO) mechanism
☑Second-line services and intelligence gathering for information security protection management
☑Government information security configuration baseline setting
2001
2004
2005
2008
2009
2012
2013
2016

Figure 3. Major information security policy development milestones

1. Phase 1 Mechanism Plan

In order to coordinate and accelerate the introduction of an information security infrastructure, the Executive Yuan approved the Phase 1 Mechanism Plan in 2001, which ran from 2001 to 2004. This phase concentrated on efforts to implement information security protection systems within the 3,713 major government agencies. In practical terms, government agencies were classified into seven categories: National Defense, Administration, Academic, Enterprises - Group 1 (water, electricity, petroleum and gas), Enterprises - Group 2 (transportation, communications, Internet and air traffic control), Enterprises - Group 3 (financial services, securities, tariff and trade) and Enterprises - Group 4 (medical services). Each category was further divided into Class A (critical core agencies), Class B (core agencies), Class C (major agencies) and Class D (general agencies). Depending on the classification, different levels of information security support were provided. The rationale was to fulfill information security protection responsibilities in a comprehensive manner despite limited resources.

In addition, the Plan also focused on implementing security management measures on information systems of more than 20 CIs. This required the on-schedule completion of installation of remote backup systems followed by certification to international information security management standards. In terms of information security awareness training, IT staff and supervisors were required to receive information security technical training or enroll in management courses. At the same time, the Security Operation Center (SOC) was established to provide an early warning and incident notification mechanism.

2. Phase 2 Mechanism Plan

To follow up on the effectiveness and results of Phase 1 Mechanism Plan, the Executive Yuan approved the Phase 2 Mechanism Plan in 2004, which ran from 2005 to 2008. To respond to changes in the security landscape, the Plan was amended in February 2007.

The Phase 1 Mechanism Plan was instrumental in establishing the overall information security protection capability of Taiwan. In Phase 2, principal policies included the establishment of the responsibility system though the appointment of a Chief Information Security Officer (CISO) and National-Security Operation Center (N-SOC), enhancement of information security audits, improvement in information security responsibility classification and protection of confidential information, and development of information security key indicators, which had a definite impact on the government's ability to improve information security.

The initial push for the establishment of the CISO responsibility system in government agencies began in 2005. Currently at Executive Yuan headquarters, in 35 ministries, and in 24 special municipality and local governments, each deputy head assumes the role of CISO and is responsible for supervising an Information & Communication Security Management Team and implementing information security-related programs. By reinforcing the CISO responsibility system, information security protection and management responsibility can be enhanced. This not only reflects the importance of information security specialists but also highlights that fact that information security work is valued more than ever these days.

N-SOC not only provides ordinary surveillance and warning services but also incorporates the systems of major government agencies under a protective umbrella. Depending on actual requirements, different monitoring equipment can be deployed, e.g. intrusion detection systems, Domain Name System (DNS) alarm systems, internal network alert systems, and end-user warning systems. In addition to enhancing the incident notification and response function website and performing regular notification drills, information regarding system vulnerabilities, hacker information update and other security-related messages can be disseminated through the information security contact person in a timely manner. This effectively improves timeliness of notifications and execution of continuity plans.

The Audit Working Group of the Taskforce (whose responsibilities were formerly assumed by the Electronic Data Processing Center of DGBAS) began to conduct external audits on information security on an annual basis in 2001 by selecting 20 to 30 or more major government agencies. The Group provides audit recommendations and assists agencies undergoing audit to reinforce information security with respect to integrity and timeliness. Since 2005, the Group has also initiated efforts to encourage competent authorities to conduct internal audits.

Based on an information security responsibility classification scheme devised in 2003, a new categorization system was established in 2006, the applicability of which was expanded to cover the entire education system. The number of government agencies under its jurisdiction increased from 3,713 to 6,797. According to data of the former Central Personnel Administration regarding the number of agencies subordinate to the Executive Yuan and local government agencies, this has expanded coverage to over 80% of all agencies.

To prevent users' computers from being hacked by malicious programs via email social engineering attacks, the Taskforce conducted e-mail social engineering drills in 2006 and required government agencies of a critical and confidential nature to adopt effective physical isolation and encryption protection measures in order to provide secure and effective protection for confidential information. These agencies now comply with security requirements.

In addition, in order to assess the status of Taiwan's information security development, the Phase 2 Plan began to adopt key indicators for assessment of information security in 2006. By collecting quantitative data, performance in information security awareness, environment, overall protection and emergency response capability can be easily assessed.

3. Phase 3 Development Program

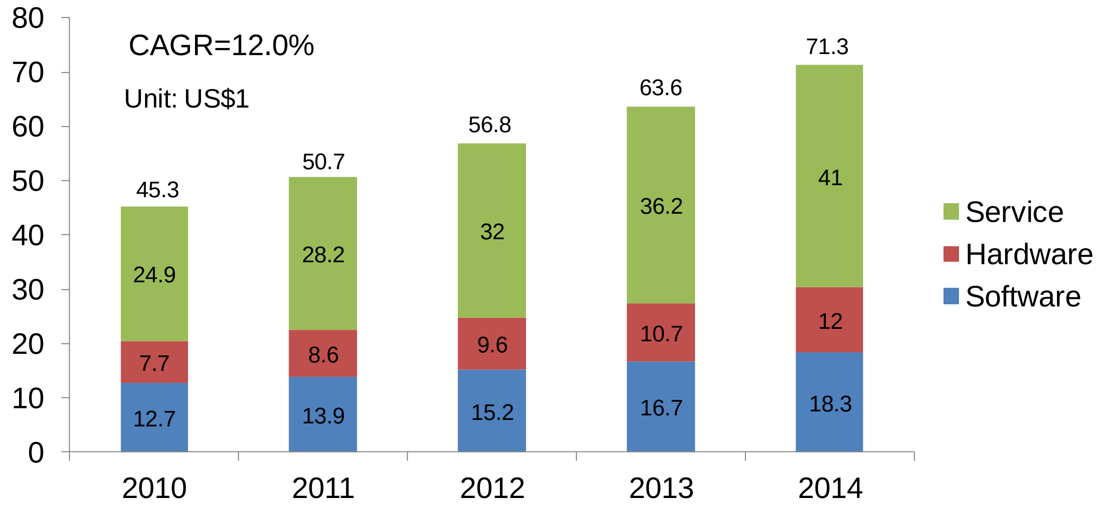
The implementation of the first two phases of the mechanism plan has brought some success in terms of promoting awareness of information security among government agencies and soliciting participation from the private sector. However, the amount of overall information security resources invested is still limited, which is not conducive to in-depth assessment of information security risks and effective control of these risks within acceptable limits. Given the overall situation and the fact that new information security issues will always arise, it is necessary for the government to continue to devise information security programs and implement information security practices. As a result, the Executive Yuan approved a Phase 3 Development Program in January 2009, which would run from 2009 to 2012. In this phase, policy continuity was taken into consideration so that the vision of the "Secure and Trusted Smart Taiwan, Safe and High Quality Digital Life" can be achieved. The ultimate goals are to attain four major policy objectives: "Strengthening overall response capability," "Providing reliable information services," "Fostering enterprise competitiveness" and "Building an information security culture-centric development environment." In actual implementation, "demand side" and "supply side" were taken into consideration when planning five information security measures (including 20 action plans) that meet government standards, Critical Information Infrastructure (CII) requirements and enterprise needs. In terms of the environment, four measures (including 10 action plans) that help to shape the information security culture were adopted to facilitate relevant legislation, awareness education, collaboration through innovation and assessment indicators.

By implementing the 30 action plans described above, the following benefits were achieved in late 2012: increased investment in information security resources, improved readiness in information security regulations, enhanced national information security awareness, strengthened overall information security protection capability, increased frequency of information security drills, and reduced severity in information security incidents. Measures implemented in government agencies have been gradually made available to the private sector and enterprises.

## III. Current Status of Information Security Industry

### 1. Size of global information security market

The global information security market can be broken down into three areas: software, hardware and services. The software sector grew from US$12.7 billion in total revenue in 2010 to US$18.3 billion in 2014, with a compound annual growth rate (CAGR) of 9.6%. The hardware sector increased from US$7.7 billion in 2010 to US$12 billion in 2014, which represents a CAGR of 11.7%. The services sector grew from US$24.9 billion in 2010 to US$ 41 billion in 2014, a CAGR of 13.3%. The overall global information security market increased from US$45.3 billion in 2010 to US$71.3 billion in 2014, which represents a CAGR of 12.0% (refer to Figure 4).

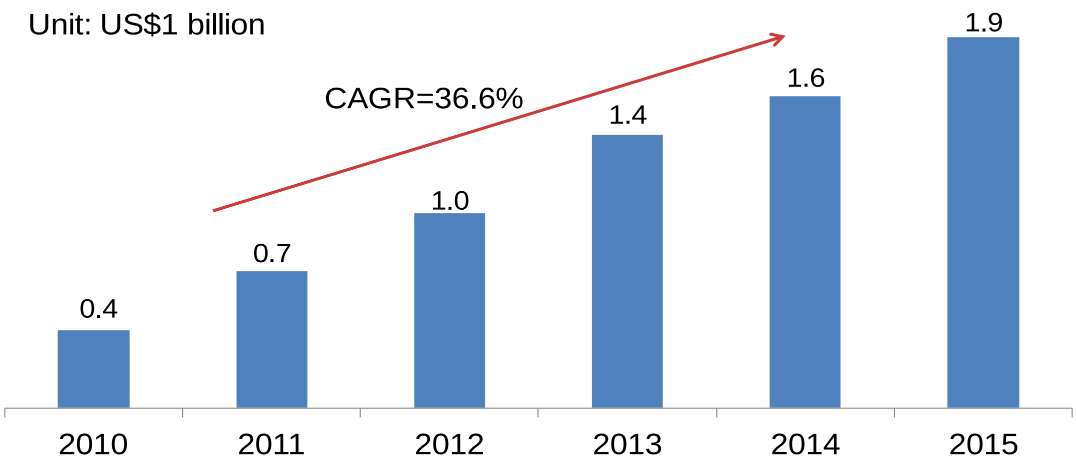


Source: Gartner, compiled by MIC, February 2011

Figure 4. Size of global information security market, 2010-2014

Overall the information security market exhibits a trend of growth. The main factors driving growth include the ongoing effects of global regulations, increasing level of threats to the environment (new attack types, such as APT), new security vulnerabilities resulting from the integration of smart mobile devices and enterprise systems, and security issues arising from virtualization of cloud computing (e.g. data transmission security, authentication and access control, and audit issues). In particular, regulations and environmental threats remain the main driving factors since the former involves issues of compensation, and the latter is concerned with the fact that enterprises struggle to easily combat threats, especially since comprehensive solutions are not yet available on the market.

In addition, smart mobile devices have resulted in an entire set of security requirements, which has caused the global smartphone information security market to grow from US$400 million in 2010 to US$1.9 billion in 2015, CAGR of 36.6% (see Figure 5).

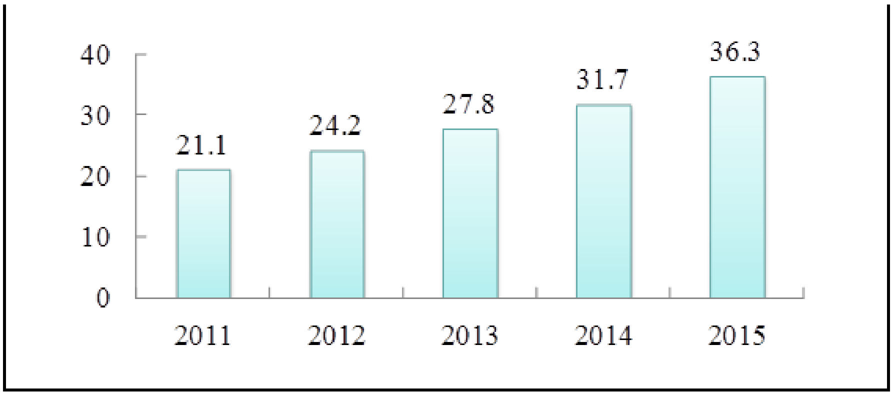


Source: IDC, compiled by MIC, May 2011

Figure 5. Global information security market for smartphones, 2010-2014

2. Size of Taiwan's Information Security Market

The information security market in Taiwan includes domestic players and international vendors. Revenue of Taiwanese vendors is expected to grow from NT$6.2 billion in 2010 to NT$12.7 billion in 2014, with a CAGR of 19.6%. Revenue of international vendors is expected to grow from NT$12.3 billion in 2010 to NT$19 billion in 2014, with a CAGR of 11.6%. The overall information security market in Taiwan will grow from NT$21.1 billion in 2011 to NT$36.3 billion in 2015, which represents a CAGR of 14.6% (see Figure 6 for details).

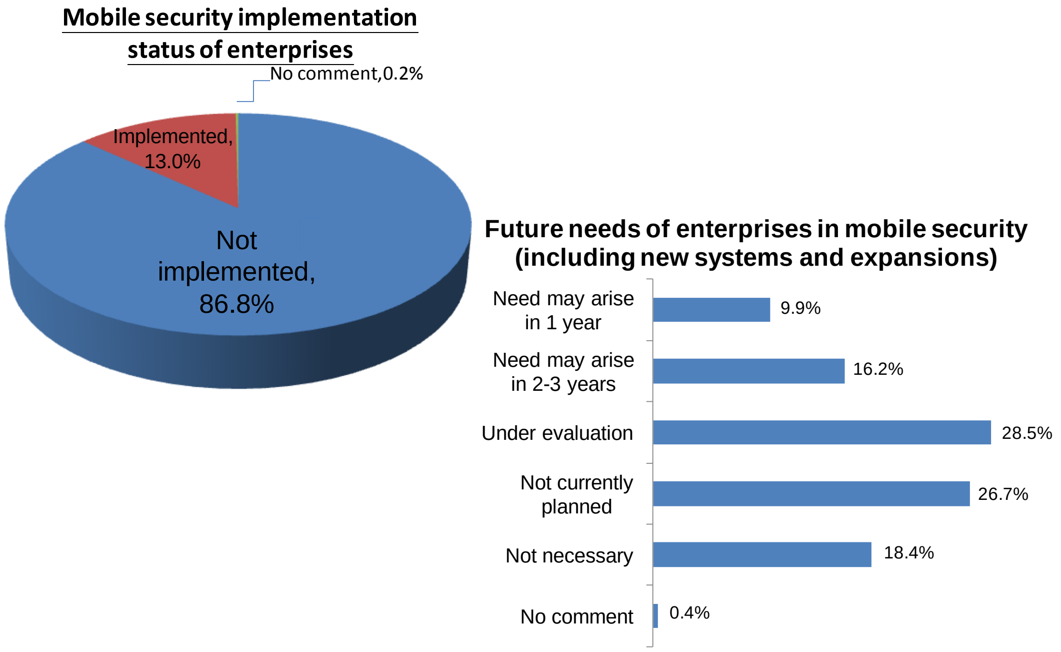


Note: in NT$ billion
Source: MIC, February 2013

Figure 6. Size of Taiwan's information security market, 2011-2015

In response to the rapidly changing social environment and for the purpose of enhancing the protection of personal data, the Personal Information Protection Act expanded the scope of the law from protecting personal data stored and processed by computers to include all personal information. In addition, the Act now allows mechanisms such as class actions to be filed in order to increase the amount of compensatory damages and the severity of criminal liability. More importantly, the industries to which the Act is applicable have increased from the original governmental agencies and eight major industries to include all governmental and non-governmental organizations as well as individuals. The Act came into effect on October 1, 2012, and has subsequently driven the growth of Taiwan's information security market.

With the surge in popularity of smart mobile devices in recent years, the use of mobile devices by company employees to access corporate data or conduct financial transactions has become increasingly widespread. The corporate information security defense perimeter has in turn expanded due to the ensuing increased threats (e.g. personal information leakage, Internet fraud and social engineering) (refer to Figure 7). In the domestic market, although the percentage of corporations in Taiwan that have implemented mobile security was 13.0% in 2011, the proportion of companies with this particular security requirement will be 26.1% within the next three years. Thus demand for mobile security in Taiwan over the next three years is expected to grow.



Note 1: No. of valid samples: 506 large enterprises
Note 2: Mobile security, including cellphone anti-virus protection, anti-theft and recovery, remote control, data encryption, authentication and anti-spam
Source: MIC, April 2011

Figure 7. Implementation status and future mobile security requirements of Taiwanese enterprises, 2011

In addition, with respect to the demand for cloud security in Taiwan, although the cloud computing industry remains in a growth phase, corporate demand and adoption of cloud security products and services have increased over the past three years. Furthermore, there will be changes in the processes and locations associated with cloud-based applications adopted in the past (mostly in-house data storage, transmission, utilization and management). This will affect corporations' data security considerations in every aspect, and the proportion of companies adopting cloud-based information security products and services will clearly rise.

## IV. Analysis of Strengths and Weaknesses of Information Security Development

After three implementation phases of the Mechanism Plan or Development Program and with extensive joint efforts of both government and citizens, substantial progress in Taiwan's overall information security environment has been made. However, there is much room for improvement before the vision of "Building a secure information security environment and becoming a high quality network society" can be achieved. Given the current situation, the following strengths and weaknesses in the internal environment as well as opportunities and threats in the external environment, as shown in Table 1, should be considered.

Table 1. SWOT analysis of Taiwan's overall information security environment

| Strengths (S) | Weaknesses (W) |
|---|---|
| 1. Information and communication technology (ICT) industry in Taiwan is well developed with skilled ICT professionals and experts.<br>2. Access to highly skilled human resources; innovative and highly adaptable to new technologies.<br>3. The Office of Information and Communication Security has been established under the Executive Yuan to conduct overall planning of government's information security responsibilities.<br>4. The Office of National Information and Communication Security has been established under the National Security Council to coordinate work associated with the country's information and communication security. | 1. Users have not complied with information security standards in terms of usage behavior; room for improvement in terms of awareness and alertness.<br>2. Information security regulations not comprehensive enough; further legislative efforts required.<br>3. Information security organizations, manpower and budget have yet to be incorporated into legal framework.<br>4. Information security governance has been in place for four years, yet effectiveness requires further improvement.<br>5. Many security vulnerabilities exist in computer applications; information security incidents abound; attacks from hackers are difficult to repel.<br>6. Demarcation of responsibilities in government's information security duties not clearly defined.<br>7. Key information security technologies are controlled by more advanced countries and cannot be easily accessed or duplicated.<br>8. Conditions for developing information security industry are unfavorable. |

| | |
|---|---|
| | 9. International cooperation in the area of information security is limited.<br>10. Cloud-related regulatory and legal environment as well as technical capabilities incomplete.<br>11. Information security defense capability far inferior to that of organized hackers. |
| Opportunities (O) | Threats (T) |
| 1. The government continues to develop ICT applications, optimize public information frameworks and enhance overall information security by taking advantage of the Executive Yuan's organizational restructuring.<br>2. Issues associated with protection of privacy and intellectual property are now given proper attention; the Personal Information Protection Act has also come into effect.<br>3. Global information security market has grown as information security incidents proliferate and relevant legislation comes into effect.<br>4. Transformation of the Information and Communication Security Taskforce's Technical Services Center will bring opportunities to the information security industry.<br>5. In the international community, countries strive to strengthen their international position and influence and seek opportunities for information security cooperation. | 1. Performance evaluation and audits are not easy to conduct, and benefits of these are often overlooked, resulting in inadequate investment in information security resources.<br>2. Preservation of digital forensic evidence is not an easy task; forensic capability is inadequate.<br>3. The Internet has become an instrument of crime, a location of criminal activity as well as a target of crime.<br>4. Information security analysis and sharing mechanisms have not been adequately established.<br>5. Advanced nations have invested heavily in the research and development of information security and digital forensic technologies, which have enabled them to retain the lead in these areas and widen gaps with less advanced countries.<br>6. Due to the unique cross-strait political and economic situation, Taiwan is restricted in its participation in international organizations and activities.<br>7. Hackers employ increasingly sophisticated techniques and have evolved into organized crime syndicates, meaning information security is under ever more severe threat. |

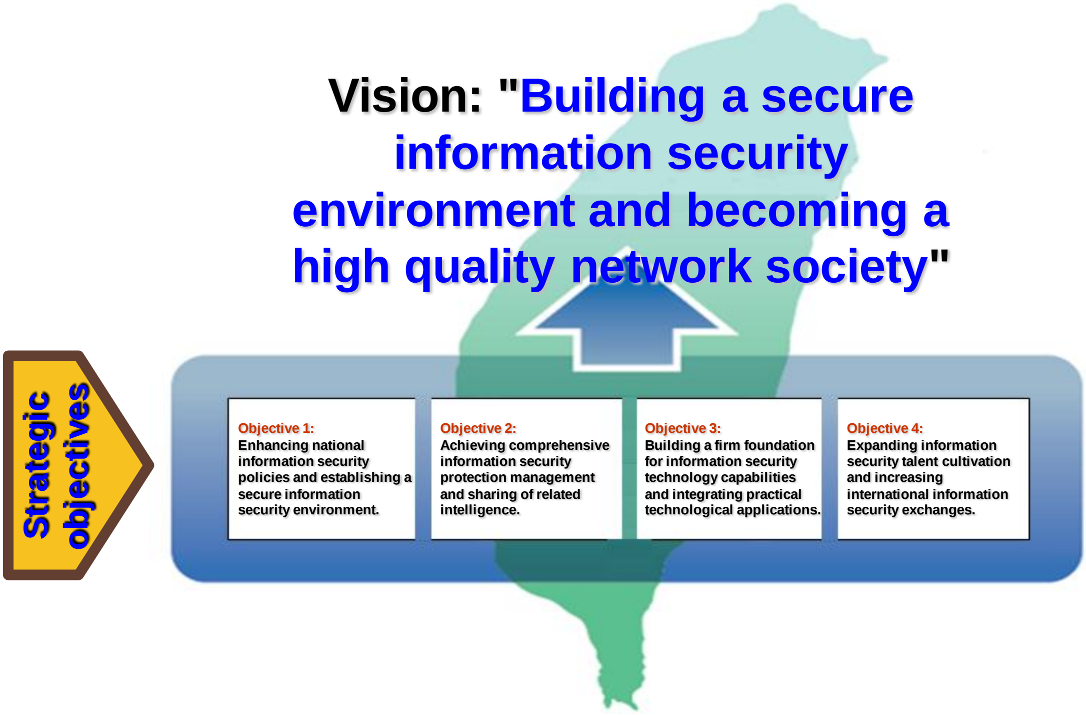
Under current conditions, the development environment of Taiwan's information security industry does not allow for optimism. The advantages that Taiwan currently enjoys, including excellent ICT and general technology professionals, highly skilled manpower and innovative capabilities, will soon diminish as other countries begin to invest in and build up their own talent pool. At the same time, information security protection experiences and information associated with hacker behavior is time-sensitive and should be utilized in a timely and appropriate manner. Therefore, how to regard, handle and take full advantage of current advantages and strengths so that development can proceed in a positive direction is a critical issue.

The government needs to be fully aware of information security issues as well as possible threats and challenges facing at present, so that it can employ forward-thinking and strategic perspectives to analyze and solve issues. Therefore, to establish a vision and strategic objectives for the Program, it is imperative to address issues faced by the information and communication security at present and to develop effective and appropriate response measures. After all, "the mere existence of law without rigorous enforcement is meaningless." What is more important is the earnest implementation of these measures and the continuing review and improvement of them.

# Chapter 4 Vision, strategic goals and development roadmap

## I Vision

With information and communication technologies continuing to evolve, providing a secure and reliable Internet environment, creating information security service value, taking advantage of the cloud computing technology, and migrating to virtualization and integration of information security services have become the most important aspects in the move toward a Ubiquitous Network Society. In Taiwan, three implementation phases of the Mechanism Plan or Development Program have been completed, and information security management system has become increasingly robust. Personal information security awareness has also been raised. However, it is critically important to bring together resources and capabilities from industry, government, academic and research sectors to enable the network society to grow in a healthy fashion. The Program has adopted the vision of "Building a secure information security environment and becoming a quality network society" and aims to gradually promote and implement a high-quality network community under the guidance of forward-looking policies and with joint efforts from both the public and private sectors, as well as with the support of Taiwan's combined resources and strengths (see Figure 8).



Vision: "Building a secure information security environment and becoming a high quality network society"

**Objective 1:** Enhancing national information security policies and establishing a secure information security environment.

**Objective 2:** Achieving comprehensive information security protection management and sharing of related intelligence.

**Objective 3:** Building a firm foundation for information security technology capabilities and integrating practical technological applications.

**Objective 4:** Expanding information security talent cultivation and increasing international information security exchanges.

Figure 8. Vision and strategic objectives

## II Strategic Goals

In order to enhance the international competitiveness in the IT industry, Taiwan is actively involved in the research, development and implementation of information technology. The key initiative of the government's i-Taiwan 12 Projects is "Intelligent Taiwan", the purpose of which is to give all citizens regardless of background access to e-services that are economical, convenient, safe and personalized via a variety of channels. The plan also calls for the construction of high-quality e-services that promote a safe, healthy, convenient and cultured society so that the vision of an "Information Services Island" can be realized. With the promotion of information technology and widespread availability of IT services, Taiwan is now facing the same information security risks and threats that confront other countries highly dependent on information technology infrastructures. As information security incidents become more prevalent, information security issues are of critical importance to the national and economic security. In order to fully implement the Ubiquitous Network Society vision, the following four strategic goals have been proposed:

- Goal 1: Enhance national information security policies and establish a secure information environment.

The rapid development of the Internet has led to a broad range of information security threats, including in the political, economic, social, cultural, technological and military spheres. In Taiwan, the government is now focused on the following areas: establishing a secure and trusted information security environment; protecting individuals, businesses and government agencies from information security threats; safeguarding critical infrastructures; enhancing citizens' confidence; and ensuring economic and national security. In the complex Internet environment, since information and communication security is an all-encompassing endeavor, it is necessary to develop strategies based on factors of legal compliance, external competitive environment changes, asset risk assessment principles, asset value and related information services. Only when Taiwan's information security policy is in a state of continuous improvement, with considerable investment of resources and self-reliance in strengthening of information and communication security protection capabilities, can information security threats be effectively neutralized.

- Goal 2: Improving information security protection management and sharing intelligence.

In order to create a trusted information and communication security environment as well as to safeguard data, equipment and network systems and to protect citizens’ rights, the government has implemented a dedicated Government-Information Security Management System (G-ISMS). This system offers assurance on the confidentiality, integrity and availability of information systems of government agencies, as well as creating a government-wide joint-defense mechanism to reduce risks associated with information security incidents to an acceptable level. In addition, the scope of information security surveillance has been expanded by an enhanced Government-Security Operation Center (G-SOC) with integrated second-line monitoring and intelligence gathering and sharing functions, as well as cloud-based information security services. In addition, an automated incident notification system has been implemented through the Government-Information Sharing and

Analysis Center (G-ISAC) platform.

- Goal 3: Building a firm foundation for information security technology capabilities and integrating practical technological applications.

Strengthening collaboration with industry, academic and research sectors on information security research and developing the next generation of comprehensive information security technology solutions are the government's objectives. This includes core technology areas such as information security vulnerability detection, penetration testing, intrusion threats, web application security, firewall applications and incident reporting management. At the same time, with respect to Internet applications, the government aims to conduct research on emerging information security applications and technical specifications; become self-reliant on key technologies associated with cloud computing, virtualization and mobile information security protection; improve Big Data computational capabilities in integrated analysis of information security threats; and carry out practical application of emerging information security technologies.

- Goal 4: Expanding information security talent cultivation and increasing international information security exchanges.

This goal includes expanding cooperation in talent cultivation and expertise in information security research; formulating plans and support packages to attract talent and skills training; developing information security professional competency and associated certification mechanisms; learning from other countries' experiences in personnel training; implementing a specialized learning environment for personnel training and drills; establishing an international cooperation and exchange platform; participating in international information security organizations events; maintaining memberships such as the Asia Pacific Computer Emergency Response Team (APCERT), Anti-Phishing Working Group (APWG), Association of anti-Virus Asia Researchers (AVAR) and Forum of Incident Response and Security Teams (FIRST); keeping abreast of the latest international development trends; and expanding collaboration programs with the following information security organizations via the G-ISAC platform: Japan Computer Emergency Response Team / Coordination Center (JPCERT/CC), Malaysian Computer Emergency Response Team (MyCERT) and Korea Computer Emergency Response Team / Coordination Center (KrCERT/CC).

## III Development Roadmap for Information Security Strategies

The Program forms the basis from which Taiwan's information security defense will be implemented over the next four years (from 2013 to 2016), and it will be a value-added hub that serves the government, industry and the general public. Through a macroscopic analysis of information security technology trends, the Program carries out overall planning on information security, and with the investment and implementation of information security protection resources, the competitiveness of the information security industry can be enhanced, which will be a driving force for Taiwan's information security defense and industrial innovation. In the Program each goal has several corresponding implementation strategies, and each implementation strategy corresponds to a number of action plans (see Figure 9).

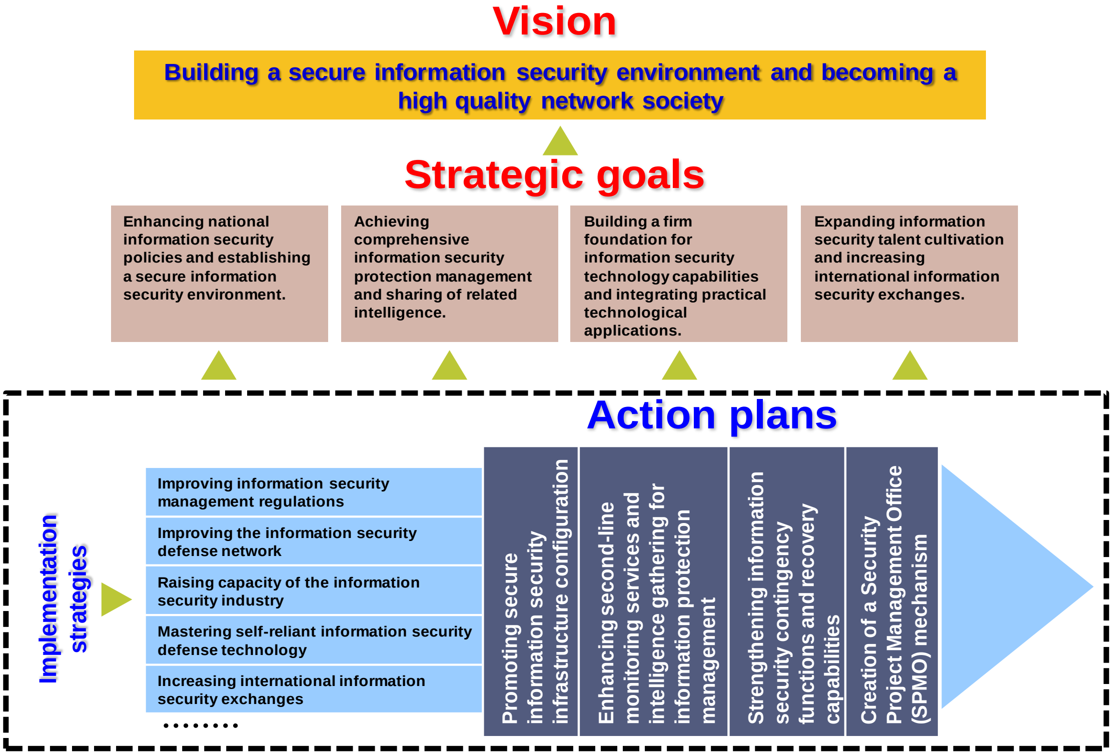

Vision
Building a secure information security environment and becoming a high quality network society
Strategic goals
Enhancing national information security policies and establishing a secure information security environment.
Achieving comprehensive information security protection management and sharing of related intelligence.
Building a firm foundation for information security technology capabilities and integrating practical technological applications.
Expanding information security talent cultivation and increasing international information security exchanges.
Action plans
Implementation strategies
Improving information security management regulations
Improving the information security defense network
Raising capacity of the information security industry
Mastering self-reliant information security defense technology
Increasing international information security exchanges
........
Promoting secure information security infrastructure configuration
Enhancing second-line monitoring services and intelligence gathering for information protection management
Strengthening information security contingency functions and recovery capabilities
Creation of a Security Project Management Office (SPMO) mechanism

Figure 9. Implementation strategies and action plans

By promoting information security configurations in information security infrastructures, enhancing second-line monitoring services and intelligence gathering for information security protection management, strengthening information security contingency functions and recovery capabilities and creating a Security Project Management Office (SPMO) mechanism, the Program aims to achieve the following four strategic objectives: (1) Enhancing national information security policies and establishing a secure information environment, (2) Improving information security protection management and sharing diverse intelligence on information security, (3) Building a firm foundation for information security technology capabilities and integrating practical technological applications and (4) Expanding information security talent cultivation and increasing international information security exchanges.

In addition, the essence of the Program may be considered from the three aspects of: demand side, supply side and infrastructure (refer to Figure 10 for more detailed information).

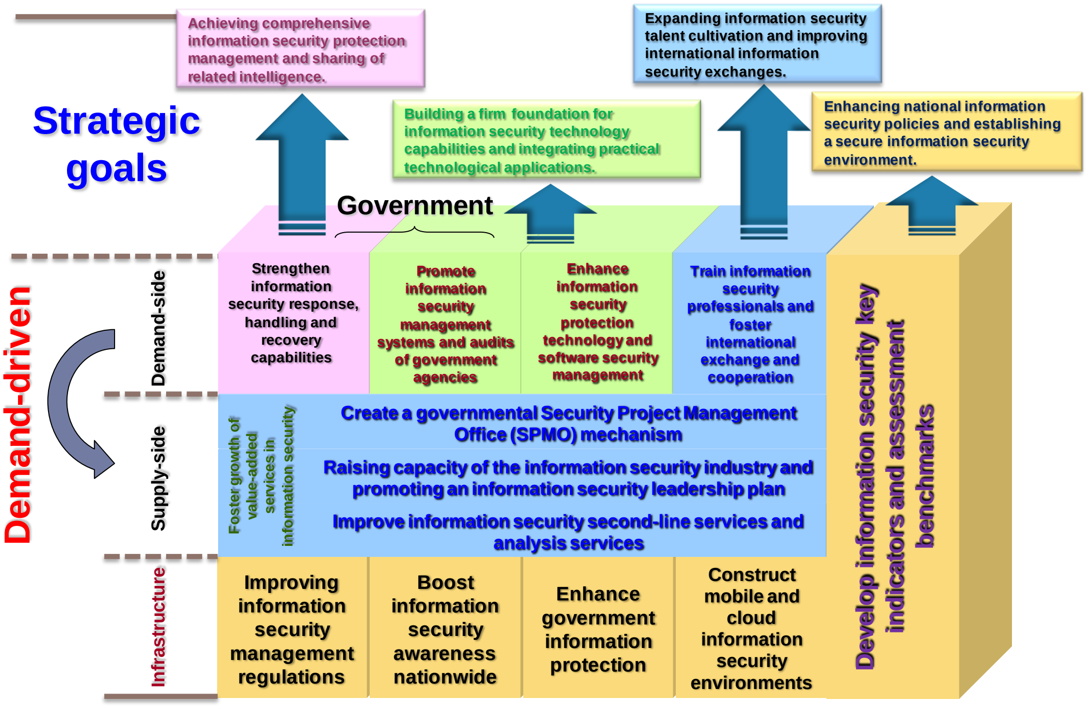

Achieving comprehensive information security protection management and sharing of related intelligence.
Expanding information security talent cultivation and improving international information security exchanges.
Strategic goals
Building a firm foundation for information security technology capabilities and integrating practical technological applications.
Enhancing national information security policies and establishing a secure information security environment.
Government
Demand-driven
Demand-side
Supply-side
Infrastructure
Strengthen information security response, handling and recovery capabilities
Promote information security management systems and audits of government agencies
Enhance information security protection technology and software security management
Train information security professionals and foster international exchange and cooperation
Foster growth of value-added services in information security
Create a governmental Security Project Management Office (SPMO) mechanism
Raising capacity of the information security industry and promoting an information security leadership plan
Improve information security second-line services and analysis services
Improving information security management regulations
Boost information security awareness nationwide
Enhance government information protection
Construct mobile and cloud information security environments
Develop information security key indicators and assessment benchmarks

Figure 10. Development roadmap

"Demand side" reflects the endeavors of three principal entities, the government, CIs and enterprises, in achieving the objectives of enhancing overall response and handling capabilities, providing safe and reliable information security services and raising competitiveness of the information security industry, by implementing the following measures: enhancing information security contingency, processing and recovery capability; promoting information security management systems and audits in government agencies; enhancing information security protection technology and software security management; and training information security professionals and fostering international exchange and cooperation.

With respect to raising competitiveness to improve the country's information security industry, it is also necessary to have the support of the "supply side." By supporting the development environment for the information security services industry, including technology, professional talent and skills as well as joint agreements, the Security Project Management Office (SPMO) mechanism can be utilized to drive service innovation and to increase value-added services of the industry.

Infrastructure involves aspects such as creating comprehensive information security regulations and legislation, strengthening nationwide information security awareness, enhancing government's information security defense, and implementing mobile and cloud-based information security environments, which require the design of corresponding action plans to achieve the goal of "becoming a Ubiquitous Network Society."

# Chapter 5 Important implementation strategies and action plans

In order that information security tasks can be carried out smoothly, in the Program a total of 20 implementation strategies and 52 action plans have been designed to address the four strategic goals (refer to Table 2). The demarcation of responsibilities is based on the nature of the action plans, which are assigned to the appropriate ministries or councils of the Executive Yuan and various government agencies.

Table 2 Major implementation strategies and action plans (by specialization/responsibility)

| Objectives | Implementation strategies | Action plans | Responsible unit(s) | Co-organizer(s) |
|---|---|---|---|---|
| Objective 1: Enhancing national information security policies and establishing a secure information security environment. | 1.1.Developing information security-related criteria | 1.1.1. Develop information security policies | Office of Information and Communication Security | Research, Development and Evaluation Commission |
| | | 1.1.2.Upgrade information security specifications, guidelines, standards and manuals | Office of Information and Communication Security, Ministry of Economic Affairs | Research, Development and Evaluation Commission |
| | 1.2.Improving information security management regulations | 1.2.1.Deliberation on information security management-related regulations | Office of Information and Communication Security | Ministry of Justice, other competent authorities |
| | | 1.2.2. Promote personal information security protection mechanisms | Office of Information and Communication Security, Ministry of Economic Affairs | Office of Information Services, Executive Yuan; Ministry of Justice; various agencies |
| | 1.3.Promoting functional information security organizations | 1.3.1. Promote reasonable information security human resources and budget | Office of Information and Communication Security | Research, Development and Evaluation Commission, Directorate-General of Personnel Administration, Directorate General of Budget, Accounting and Statistics, various agencies |
| | | 1.3.2. Create a Security Project Management Office (SPMO) mechanism | Office of Information and Communication Security | Office of Science and Technology |
| | | 1.3.3. Promote transformation of the Security Technology Center into an administrative institution | Office of Information and Communication Security | Directorate-General of Personnel Administration |

| Objectives | Implementation strategies | Action plans | Responsible unit(s) | Co-organizer(s) |
|---|---|---|---|---|
| | 1.4.Constructing information security key indicators | 1.4.1. Develop overall information security protection indicators | Office of Information and Communication Security | National Security Council, National Security Bureau, Ministry of National Defense |
| | | 1.4.2. Research information security warning levels and indicators | Office of Information and Communication Security | National Security Council, National Security Bureau, Ministry of National Defense |
| | 1.5.Raising capacity of the information security industry | 1.5.1. Foster the growth of value-added services in information security | Ministry of Economic Affairs, National Communications Commission | Office of Science and Technology |
| | | 1.5.2. Promote an information security jump-start program for key industries | Ministry of Economic Affairs | |
| Objective 2: Achieving comprehensive information security protection management and sharing of related intelligence. | 2.1. Continuing to promote information security governance and its classification and categorization | 2.1.1. Promote the establishment of an information security governance framework | Office of Information and Communication Security, various agencies | |
| | | 2.1.2. Implement classification and categorization as well as protection regulations for information systems | Office of Information and Communication Security, other competent authorities | |
| | 2.2.Improving the information security defense network | 2.2.1. Strengthen the depth of information security protection | Office of Information and Communication Security, various agencies | National Security Bureau |
| | | 2.2.2. Expand joint information security defense domestically and internationally | Office of Information and Communication Security | Ministry of Foreign Affairs, Ministry of National Defense, various agencies |
| | | 2.2.3. Strengthen information security emergency response, handling and recovery capabilities | Office of Information and Communication Security, various agencies | |
| | | 2.2.4. Establish information security baseline protection for critical information infrastructures | Office of Information and Communication Security | Office of Homeland Security, various agencies |
| | | 2.2.5. Enhance Internet content safety management mechanisms | National Communications Commission | Ministry of the Interior, Ministry of Education, Ministry of Economic Affairs, Ministry of Culture , Ministry of Health and Welfare, Office of Information and Communication Security |
| | | 2.2.6. Implement information security offensive/defensive drills | Office of Information and Communication Security | Office of Homeland Security |
| | 2.3.Implementing information security | 2.3.1. Promote government information security management systems | Office of Information and Communication Security | Various agencies |

| Objectives | Implementation strategies | Action plans | Responsible unit(s) | Co-organizer(s) |
|---|---|---|---|---|
|  | management and audit systems | 2.3.2. Promote secure information security infrastructure configuration | Office of Information and Communication Security | Various agencies |
|  |  | 2.3.3. Implement information security audits | Various agencies, Office of Information and Communication Security | National Security Bureau; Office of Information Services, Executive Yuan |
|  |  | 2.3.4. Implement information security analysis operations | Office of Information and Communication Security, various agencies |  |
|  | 2.4 Obtaining complete information security threat scenarios | 2.4.1. Strengthen second-line monitoring mechanisms | Office of Information and Communication Security | Various agencies |
|  |  | 2.4.2. Develop Big Data analysis capabilities | Office of Information and Communication Security |  |
|  | 2.5.Gathering and sharing intelligence | 2.5.1. Enhance information sharing and analysis | Office of Information and Communication Security | Various agencies |
|  |  | 2.5.2. Enhance intelligence gathering on information security threats | Office of Information and Communication Security | Various agencies |
|  |  | 2.5.3. Gather and disseminate essential information security intelligence | Office of Information and Communication Security | Various agencies |
| Objective 3: Building a firm foundation for information security technology capabilities and integrating practical technological applications. | 3.1.Mastering self-reliant information security defense technology | 3.1.1. Develop research capabilities in information security protection technology | National Science Council, Ministry of Economic Affairs, Ministry of National Defense | Office of Information and Communication Security |
|  |  | 3.1.2. Promote integrated information security protection technology applications | Ministry of Economic Affairs, Office of Information and Communication Security | National Security Bureau |
|  | 3.2.Enhancing cybercrime investigation capabilities | 3.2.1. Strengthen cybercrime investigation technology applications | Ministry of the Interior, Ministry of Justice | Office of Information and Communication Security |
|  |  | 3.2.2. Construct an integrated cybercrime investigation "knowledge base" | Ministry of the Interior, Ministry of Justice | Office of Information and Communication Security |
|  | 3.3.Developing preservation and identification capabilities in digital forensic evidence | 3.3.1. Improve procedures for preservation of digital forensic evidence | Ministry of Justice, Ministry of the Interior | Office of Information and Communication Security |
|  |  | 3.3.2. Develop a verification system for digital forensics laboratories | Ministry of Justice, Ministry of the Interior | Office of Information and Communication Security |
|  | 3.4. Enhancing software security management | 3.4.1. Create national software asset control mechanisms | Office of Information and Communication Security | Various agencies |

| Objectives | Implementation strategies | Action plans | Responsible unit(s) | Co-organizer(s) |
|---|---|---|---|---|
| | | 3.4.2. Promote the Security Software Development Life Cycle (SSDLC) | Office of Information and Communication Security | Office of Science and Technology, various agencies |
| | 3.5. Developing government mobile security mechanisms | 3.5.1. Develop government security detection mechanisms for mobile apps | Office of Information and Communication Security | Research, Development and Evaluation Commission |
| | | 3.5.2. Plan government mobile security and protection mechanisms | Office of Information and Communication Security | Research, Development and Evaluation Commission |
| | | 3.5.3. Upgrade security measures for government wireless networks | Office of Information and Communication Security | Research, Development and Evaluation Commission |
| Objective 4: Expanding information security talent cultivation and improving international information security exchanges. | 4.1. Boosting information security awareness nationwide | 4.1.1. Organize information security promotional activities | Ministry of Education, Office of Information and Communication Security | Various agencies |
| | | 4.1.2. Promote nationwide information security awareness and personal information protection | Office of Information and Communication Security | Various agencies |
| | 4.2. Developing professional talent in information security | 4.2.1. Develop information security seed instructors and professional talent | Office of Information and Communication Security, Ministry of Education, Ministry of the Interior, Ministry of Justice | |
| | | 4.2.2.Promote information security professional training and certification mechanisms | Office of Information and Communication Security | Ministry of Education |
| | 4.3. Developing diverse learning channels for information security | 4.3.1. Incorporate information security into curricula or programs at all educational levels | Ministry of Education | Office of Information and Communication Security |
| | | 4.3.2.Plan diverse learning channels for information security | Ministry of Education, Office of Information and Communication Security | |
| | 4.4. Promoting information security competency training and assessment for government employees | 4.4.1.Plan and determine information security knowledge and skills required for each job function | Office of Information and Communication Security | |
| | | 4.4.2.Establish standards for developing and assessing job competency training courses | Office of Information and Communication Security | |
| | | 4.4.3.Develop digital and physical course materials for information security competency | Office of Information and Communication Security | |
| | | 4.4.4.Establish an information security competency evaluation system | Office of Information and Communication Security | |
| | 4.5. Enhancing domestic and | 4.5.1.Participate in conferences and events organized by domestic | Office of Information and Communication | Ministry of Foreign Affairs |

| Objectives | Implementation strategies | Action plans | Responsible unit(s) | Co-organizer(s) |
|---|---|---|---|---|
| | international exchanges and cooperation in information security | and international information security organizations | Security | |
| | | 4.5.2.Participate in international events related to cybercrime investigation and prevention | Ministry of Justice, Ministry of the Interior | Office of Information and Communication Security |
| | | 4.5.3.Boost international publication of academic information security research | National Science Council | Office of Information and Communication Security, Ministry of Education |

# Chapter 6 Promotion organization, resource requirements and program management

## I Organization Responsible for Program Promotion

Pursuant to the Guidelines for Establishing the National Information and Communication Security Taskforce of the Executive Yuan, the Office of Information and Communication Security of the Executive Yuan is charged with the responsibility of overall planning and advancement of information security-related policies, and will therefore be responsible for the general planning and promotion of the Program.

## II Planning and Execution

With respect to key implementing specifications and performance indicators of the action plans described in the Program, an annual plan containing detailed execution and planning will be developed by each responsible agency based on the review procedures and regulations of the government's administrative plan.

## III Budget Source and Implementation

Budget sources for annual plans proposed by the responsible authorities are determined and allocated by the corresponding agencies or obtained through relevant administrative procedures. Execution of annual plans should be reviewed each year, and necessary amendments should be carried out in coordination with budget reviews and comprehensive evaluations.

## IV Evaluation of Relevant Action Plans

Key implementation specifications and performance indicators of the Program are under the evaluation of the Office of Information and Communication Security, Executive Yuan, in accordance with established supervisory mechanisms.

## V Approval and Amendment of the Program

A The Program shall become effective upon approval of the Executive Yuan; the same shall apply to all amendments.

B The Program should undergo comprehensive review and revision prior to completion of its 4-year implementation period in order to determine future versions of the Program (i.e. for the following 4-year period). If necessary an annual rolling review of the Program and related promotional plans may also be conducted.