National Cyber Security Program of Taiwan
(2017 to 2020)

National Information and Communication Security Taskforce,
Executive Yuan, Republic of China (Taiwan)

November 2017

Contents

I. Background

Since 2001, the National Information and Communication Security Taskforce (NICST) has been facilitating basic cyber security construction tasks and has already completed four promotional phases. Many milestones have been achieved through each stage, including completing the mechanism for classifying government agencies' cyber security responsibilities, promoting the Chief Information Security Officer (CISO) in administrative institutions, forming the National Security Operational Center, developing report and respond mechanisms for cyber security incidents, and developing a united cyber security protection and information sharing mechanism in government agencies, among others, all of which have effectively elevated our national cyber security readiness. Phase 4 of the National Information and Communication Security Development Program (2013 to 2016) has been completed and was officially closed in 2016.

Recently, the digital economy has led industry to move toward cross-regional areas, virtual and real worlds, etc., which will push global industries to transform their scales. With the arrival of the digital economy and the Internet of Things (IoT), the Executive Yuan developed the "Digital Nation and Innovative Economic Development Plan (2017-2025)" (abbreviated as DiGi$^+$) proposal to construct a thorough industrial ecosystem, speed up industries' innovation, and optimize industrial structure. The next stage of the National Cyber Security Program has to start from the perspective of cyber security in order to secure the country's digital safety. Therefore, three DiGi$^+$ strategies like "Friendly regulation environment", "Cross-domain digital talents", and "Advanced digital technology" were presented as supporting approaches for the foundation of a digital country that can provide a safe and reliable "basic digital innovation environment" and a "digital government in cyber society".

As mentioned above, NICST proposed the "National Cyber Security Program of Taiwan (2017-2020)" (abbreviated as NCSP), a prospective upstream policy for national cyber security with mega views. In response to our unique political and economic situation and increasingly complicated global information and communication changes, the Program will become an important reference for government agencies to develop further strategic plans for national cyber security protection.

II. Global cyber security threat and international policy trends

A. Global cyber security threat trends

According to the World Economic Forum (WEF) Global risk report, data fraud or theft was ranked fifth on the 2017 global risk in terms of likelihood, while large-scale cyberattacks were ranked sixth, indicating that cyber security risks have profoundly influenced people's lives.

i. Data fraud or theft

According to the statistical data of the Identity Theft Resource Center (ITRC), as of June 30th, 2017, the annual total data breach events reached 791 in the United States, an increase of 29% compared with 2016 and a record high. ITRC has forecasted that the total number of data breach cases could reach 1,500 in 2017, which would be an increase of 37% compared with the 1,093 cases in 2016 (around 36.6 million cases of data theft occurred). The main reasons behind such data breach events were hacker attacks, including Ransomware attacks, followed by Phishing attempts, employee errors, accidental exposure, etc.

In recent years, the most serious cyber security breach was a well-known U.S. portal website hacked in 2013, in which almost 3 billion data breaches occurred, including of Taiwanese data. According to the 2017 Internet Security Threat Report published by Symantec, the Taiwanese data breach was ranked fifth globally and first in Asia. As of May 2017, we have experienced a large-scale personal data breach incident, in which 170 million cases of data theft occurred, the most serious case in history. Clearly, data fraud or theft issues have been tough for personal and social security protection.

ii. Large-scale cyberattacks

As indicated in the 2016Q4 Kaspersky report, many botnets from 80 countries were involved in the Distributed Denial of Service (DDoS) attacks, most of which included IoT equipment with intensifying attacks up to one Tb. Since the Mirai was released on hacker forums, IoT equipment can be assumed to initiate more complicated DDoS attacks, including application layer and encrypted attacks.

However, the true objective of many DDoS attacks is initiating the Advanced Persistent Threat (APT) to steal government or business secrets. Therefore, once a DDoS attack occurs, any other cyber security alarms must be noticed simultaneously. Furthermore, many securities firms suffered DDoS attacks by hackers' bitcoin extortion during the Chinese New Year holidays of 2017. This case shows that the hacker attack mode has been transformed into an industrial model.

iii. Critical information infrastructure breakdown

An increasing amount of supervisory control and data acquisition (SCADA) of critical infrastructure (CI) are usually constructed to be operated under the public Internet environment since they need to be additionally equipped with remote control systems. If the related systems can not properly defend against hackers' attacks, citizens' finances and lives can be threatened or hurt once a hacker attack occurs. For example, the Ukraine Power Grid was hit by a cyberattack with a Spear Phishing e-mail that resulted in large-scale power outages in Ivano-Frankivsk Oblast in December 2015.

The eight critical infrastructure domains defined by the Office of Homeland Security, Executive Yuan, include Government, Energy, Water, Hi-Tech Industrial Parks, Information and Telecommunication, Transportation, Banking and Finance, Emergency Services, and Public Healthcare. According to the report published by Kaspersky Laboratory in 2016, thousands of Industrial Control System (ICS) hosts were exposed to the Internet, and 91.1% of them have vulnerabilities that can be exploited remotely. This finding reflected the potential risks of ICS for all critical infrastructure providers; in particular, the protection mechanism for such systems would need to be significantly enhanced.

iv. Adverse consequences of technological advances

Along with the rapid changes caused by newly developed information technologies, the attacking models of hackers are also evolving. In the future, more security protection mechanisms for new information technologies should be enhanced, including the following:

1. IoT equipment: Most recent DDoS attacks have been hybrid types with IoT devices as the main source. According to Gartner's forecast, 6.4 billion IoT devices were connected to the Internet in 2016, but this figure can potentially climb to 20.8 billion by 2020. If the IoT's security design and threats are underestimated, devices can be abducted by hackers, which will result in serious threats to global network security.
2. Mobile devices: One software company, Check Point, found that data breach incidents caused by mobile devices will become an important security issue, especially for well-organized hackers with their country's support. These kind of attacks are growing worldwide.
3. Cloud computing: As more government agencies and private enterprises have either public or private cloud constructions for cloud computing and expanded data storage, their information structures will become targets for hackers' attacks. Hackers use the encryption characteristic of cloud transmission as a tool for the expanded influence and scope of cyberattacks.
4. Unmanned vehicles: Recently, as many new smart technologies are being vigorously developed, unmanned vehicles are becoming widely applied, including smart robot cars, unmanned aerial vehicles (UAV), unmanned ground vehicles (UGV), unmanned marine vehicles (UMV), etc.; as a result, related cyber security topics have been raised and are closely connected. Taking the UAV as an example, power companies responsible for the national power supply have begun applying unmanned vehicles to clean the insulators of pylons to prevent aviation accidents. Such unmanned vehicles are manufactured in Taiwan, but they can receive signals from the BeiDou Navigation Satellite System (BDS); such a case represents a significant national security risk.

The darknet and deep web have also drawn considerable attention from the governments and societies of many countries, as they have been good covers for criminals and have negatively impacted public order and social security. All sorts of illegal deals of hackers' tools, shotguns, drugs, etc. can occur in this situation, thus raising the awareness of inspection agencies in all countries. In July 2017, the largest darknet black market, AlphaBay, was seized by an international inspection alliance organized by the U.S., Canada, and Thailand.

B. Development trends of international cyber security policies

As information technology has changed the world and broken boundaries between countries, it has become a popular topic in many aspects. This section has gathered and analyzed response strategies to evolving cyberattacks developed by the major countries around the world so that we can learn from the experiences of other countries to develop our own national upstream policies for cyber security over the next four years.

i. Development of cyber security policies in the United States

The United States government formed the Department of Homeland Security (DHS) in 2002 to respond to terrorist threats and enhance the protection of critical infrastructures. Furthermore, the Federal Information Security Management Act of 2002 (FISMA) was passed and announced to request that all federal government institutes follow suit; each one should establish, develop, and implement information security plans for their entire organization. Such information security control and management policies, procedures, and practices should be tested and evaluated every year in order to provide the required information security for the organizations and their stakeholders.

In 2013, President Obama signed Executive Order 13636—Improving Critical Infrastructure Cybersecurity in order to enhance the resilience capacities of critical infrastructure and asked the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce to build the Framework to Improve Critical Infrastructure Cybersecurity, taking all confidential business secrets, personal privacy, civil freedoms, etc. under the protection of the U.S. Federal Constitution into consideration.

Later in 2014, FISMA was renamed the Federal Information Security

Modernization Act of 2014 (FISMA 2014) and encompassed the following key points: (1) Require the reporting of information security events; (2) Authorize the Director of the Department of Homeland Security to support the Chief of the Budget Office in the surveillance and management of institutes; (3) Encourage relevant management procedures when information systems are invaded; and (4) Adjust the annual report contents submitted by institutes. This change indicates that the focus on information and communication security policies has expanded from the electric government security level to the homeland security level.

In 2015, the Cybersecurity Information Sharing Act (CISA) amendment was passed and renamed the Cybersecurity Act of 2015. This Act addressed information sharing issues and encouraged enterprises to actively share information in order to obtain early alarm or pre-notice information. Meanwhile, ISP industries have been allowed to monitor enterprises' Internet systems to ensure that information security is protected. The Act further tasked the Department of Homeland Security with establishing a cyber threat information platform to collect and share related information and alarms to reduce the risks to critical infrastructure information security.

In 2016, in order to improve the cyber security of the government, private companies, and all citizens, the U.S. government proposed the Cybersecurity National Action Plan (CNAP), whose key elements include:

1. Strategically integrating recent information security plans to comprehensively handle and manage the information security issues of both public and private developments.
2. Taking short-term actions and setting long-term strategies to raise awareness, increase cyber security and privacy security protections, and secure the public and economic safety of the country; authorizing civil organizations in the United States to better control their own digital security.
3. Leveraging modern information technology funds and assigning the Chief of Federal information security to change the management patterns of government information security.

4. Applying additional security protection tools, like the verification of various factors, to authorize people to guard their online accounts and ensure the safety of their financial transactions.
5. Providing information technology approaches through cross-department reviews to ensure the information security of the federal government.
6. Investing 19 billion US dollars into the field of information security, an increase of 35% compared with the 2015 information security budget.
7. Reclaiming the United States to adopt “Rules of Accountable Country Behavior” to lead the way regarding international information security protection.

Also in 2016, based on Announcement No. 41 of the Presidential Policy Directive--United States Cyber Incident Coordination (PPD-41), the National Cyber Incident Response Plan (NCIRP) was established to explain the required responses to major information security events that threaten the country’s critical infrastructure, various roles and responsibilities, and the coordination structures for resilience.

When President Trump took office in 2017, he issued the Presidential Executive Order to Strengthen the Cybersecurity of Federal Networks and Critical Infrastructure and requested that all the Directors or Chiefs of federal institutes apply the framework to improve critical cybersecurity infrastructure and properly manage the institutes’ potential cybersecurity risks. The guidelines of the critical infrastructure threat information sharing framework were prepared to assist owners, operators, others in the private sector, the federal government, and state and local governments with critical infrastructure to collaborate and share information about hacker attacks. They would also learn how to receive and report relevant threat information to one another.

ii. Development of cyber security policies in Japan

In 2005, the Action Plan on Information Security Measures for Critical Infrastructures was adopted in Japan and included the following five items: an instruction guide for security standards, an enhanced information sharing mechanism, analysis of the dependency of different critical infrastructures, cross-critical infrastructure practice, and constructions and international collaborations based on information security, to ensure the information security of critical infrastructure[1]. The objective of this plan was to provide as many services as possible to help citizens and systems recover quickly when critical infrastructures are disabled by attacks so that citizens' lives and social economics would not be significantly impacted.

In 2009, the Second Action Plan on Information Security Measures for Critical Infrastructures was adopted to maintain related applications that have already been planned, as well as develop some other new cooperative models between public and private sectors. However, due to some significant events, like Eastern Japan earthquakes and cyberattacks on the Japanese government and important critical infrastructure IT systems (including industrial controlling systems) that occurred in 2011, the amendment of the second action plan was proposed with revisions in 2012 to respond to the systematic changes of the environment. The key modifications included strategic approaches to IT events and malfunctioning so that critical infrastructure IT-related accidents would not impact citizens' lives and social commercial activities.

In 2014, the Basic Act on Cybersecurity was adopted to maintain cyber security for critical infrastructure providers, encourage them to establish the required security standards, and implement cross-domain practices. Furthermore, this Act has facilitated all official government departments and local governments, critical infrastructure providers, and cyber security industries to share information and collaborate with each other.

[1] In 2005, the critical infrastructure domains in Japan were：information and communication telecommunications, finance, aviation, railways, power, natural gas, government and administrative services (including local self-management groups), medicine, water, and transportation.

In 2015, the (3rd) Basic Policy of Critical Infrastructure Protection was issued to ensure the continuous services of critical infrastructure to strengthen the objective of protection and included three new fields, including chemical industries, credit cards, and oil in the scope. Furthermore, five strategies were proposed, including preparation and improvement of security standards, enhancement of the information sharing framework, reinforcement of the accident response framework, risk management, and upgrading the protection base.

The key points of the Cybersecurity Strategy adopted in 2015 were as follows: (1) Enhance the activities and continuous development of social economics; (2) Develop public and social safety; (3) Ensure the security and stability of international societies and countries; and (4) Support cybersecurity-related research and manpower development.

In 2016, the General Framework for Secured IoT Systems was passed to guarantee the security, confidentiality, completeness, and availability of IoT systems; furthermore, general requirements for the design, development, and operation of all IoT systems were established. As for the requirements for different departmental characteristics, the following policies were announced: (1) People that would like to participate in the IoT should confirm the requirements of related regulations or any requirement that the industries first considered inevitable and then implemented accordingly; (2) Analyze every layer of the IoT and transform each one into a module, and then take those modules as the bases for carrying out security assessments; (3) Implement regular risk assessment and develop response strategies; and (4) Clarify the roles of stakeholders to facilitate collaboration.

In order to sustain the security of domestic and Tokyo Olympics-related critical infrastructure services in Japan, the Japanese Cabinet Internet Center announced the Fourth Action Plan on Information Security Measures for Critical Infrastructures on April 19th, 2017 to add some new policies to the previous action plan. The primary changes were a focus on Operation Technology (OT) and the completeness of risk response mechanisms. To ensure the readiness and implementation of security standards, critical infrastructure industries should incorporate OT perspectives into talent cultivation. As for information sharing systems, the scope of the shared information should cover IT, OT, and IoT, and any obstacle interfering with information sharing should be removed, starting from functional verification to preparations for any new risk management, including business contingency plans and emergency reactions. To enhance the protection basis, action plans involving the IT, OT, and legal teams of critical infrastructure industries should have collaborative developments in order to fight for critical infrastructure security based on their internal information security strategies.

iii. Development of cyber security policies in Singapore

Singapore has a few regulations related to cyber security, including the Computer Misuse and Cybersecurity Act, the Telecommunications Act, the Spam Control Act, and the Electronic Transactions Act. Another policy, Singapore's Cyber Security Strategy, which was announced in 2016, claimed to: (1) Enhance the strength of critical information infrastructure; (2) Leverage the power of enterprises and communities to fight cyber threats and cyber crimes and protect personal information in order to create a more secure internet environment; (3) Develop technological manpower, enterprises with high technologies, and a cyber security ecosystem with strong research energy to support cybersecurity demands and drive Singapore's economic growth; and (4) Be dedicated to developing international partnerships as the cyber criminals' world has no boundaries.

As of 2017, the first draft of the Cybersecurity Act and the amendment of the Computer Misuse and Cybersecurity Act (CMCA) were both issued; the purpose of the former was to build and maintain a cyber security framework, reduce the risks of cyber threats, and secure the critical information infrastructure to protect the country and respond to any cyberattacks in a more efficient and complete way. The Act asked all critical infrastructure providers to report any cyber security incident that they experienced and to take actions to ensure system resilience. Established in 2015, the Singapore Cybersecurity Agency (CSA) was assigned to manage cyber security incidents and was authorized to improve cyber security standards. The previously mentioned CMCA was upgraded to keep pace with the changing nature of cyber crimes, which crossed country borders and had expanded scales. As the threat of cyber crimes increased and their tactics grew more innovative, the government was authorized to detect, obtain, or request the required internal information from critical infrastructure industries to ensure that the computer system would not be saved or revised by any unauthorized personnel.

The most updated five-year plan for advanced information and communication security in Singapore is the Infocomm Security Masterplan (ISMP), which was developed based on the former two plans to enhance Singapore's cyber security by leveraging the power of the government, critical information and communication infrastructure, enterprises, and individuals. It includes three key items: (1) Enhance the security and resilience of the Critical Infocomm Infrastructure (CII) to respond to continuously evolving cyber attacks; (2) Improve the capabilities of enterprises and individuals to maintain the security of their information and communications; and (3) Develop a pool of Infocomm Security experts in Singapore.

iv. Development of cyber security policies in Germany

In 2009, Germany passed the Federal Office for Information Security Act 2009, which announced that the German Federal Office for Information Security (BSI) would be responsible for guarding cyber security at the federal level with a clear role and responsibilities assigned. In 2011, the Cyber-Sicherheitsstrategie für Deutschland was charged with the following aims: (1) Secure critical infrastructure; (2) Enhance the IT systems of German citizens and enterprises; (3) Reinforce the cyber security of the public administration system; (4) Establish a National Cyber Response Center; (5) Organize a National Cyber Security Council; (6) Improve the criminal control effectiveness of information spaces; (7) Collaborate with other European countries and nations throughout the world to protect cyber security; (8) Adopt reliable information technologies; (9) Develop talents for federal institutes; and (10) Respond to cyber attacks with appropriate techniques.

In 2015, the BSI Act was revised to ask all critical infrastructure providers to take appropriate actions for organization and technology management within two years after the Act was implemented so that the essential systems, parts, and operational procedures would be secure from harm with regard to feasibility, completeness, awareness, and confidentiality. Furthermore, critical infrastructure providers and related industrial associations should facilitate certain security-related standards to ensure that any implementations would meet the aforementioned requirements. Every two years, security management systems should be audited and verified to prove that they are still meeting all requirements.

The Information Technology Security Act, a packaged act, was approved in 2015. This act integrated and revised the existing cyber security regulations to render the BSI greater authority and more responsibilities to improve protections for German citizens, enterprises, and government institutes in order to reduce cyber security risks. The act also asked critical infrastructure providers to assess their security techniques and report all cyber security incidents to BSI; ISP should also be obligated to report any potential cyber security risks.

In 2016, Germany announced three cyber security related policies:

1. Cyber Security Strategy for Germany

   This strategy addresses the importance of critical infrastructure protection and asks both public and private sectors to develop a broader mechanism for sharing cyber threat information. Meanwhile, the private sectors and the general public should be supported and properly trained to deal with cyber threats. Furthermore, a Quick Reaction Force was created within the federal cyber security office to help government agencies and critical infrastructure to respond to any cyber security threats. This strategy separates cyber security into the following four action-taking areas: self-driven security actions in digital environments, shared tasks between national and economic bodies, a strong and advanced cyber security framework, and the aggressive positioning of German policies among European and international cyber security policies.

2. BSI-Kritisverordnung rule

   This rule was proposed as a supplement to the 2015 Information

Technology Security Act. The former Act required critical infrastructure operators to meet minimal security standards and report all cyber security incidents back to the federal office of cyber security; therefore, critical infrastructure operators of energy, water, food, and information and communication could refer to the criteria and calculations in the attachment of the rule to determine whether or not they were included in the Information Technology Security Act. Furthermore, the rule expanded the critical infrastructure scope to cover the critical infrastructure providers of finance, insurance, transportation and traffic, and medicine. It came into effect on June 30th, 2017.

3. White Paper on German Security Policies and the Future of the Bundeswehr

   The white paper explains how the government should enhance its resilience capabilities to fight the increasing amount and mixed types of cyber threats. Topics included enhancing collaboration among all levels of government agencies, critical infrastructure providers, cyber industries, and media; minimizing the fragility of the department of energy; effective border control; and the development of public protection and disaster control, among others.

III. Current promotional updates for cyber security in Taiwan

A. Organizational structure

NICST was formed in January 2001 to be responsible for developing National Cyber Security policies, creating report and response mechanisms, providing consultations and advice for major projects, promoting cross-agency coordination, and supervising cyber security affairs. In order to implement the important strategy of "Cyber Security is Nation Security" to upgrade the leadership of cyber security, the Executive Yuan formed a unit focused on cyber security on August 1st, 2016 — the Department of Cyber Security (abbreviated as DCS) to replace the cyber security office as the assistant to NICST.

NICST has two direct reporting units, Cyber Protection System and Cyber-crime Detection and Prevention System. Pursuant to the revised "Regulations of

National Information and Communication Security Taskforce (NICST) setting” in August 2016, the NICST organizational structure is illustrated in Figure 1 below.

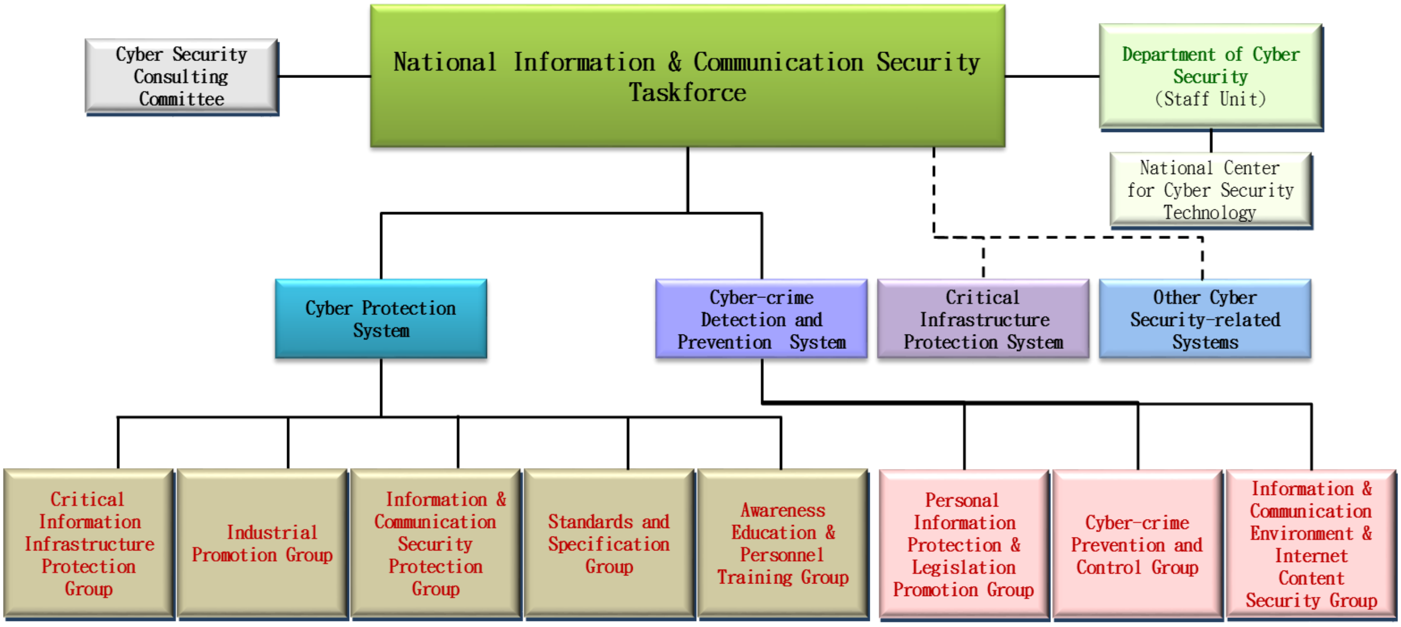

Cyber Security Consulting Committee
National Information & Communication Security Taskforce
Department of Cyber Security (Staff Unit)
National Center for Cyber Security Technology
Cyber Protection System
Cyber-crime Detection and Prevention System
Critical Infrastructure Protection System
Other Cyber Security-related Systems
Critical Information Infrastructure Protection Group
Industrial Promotion Group
Information & Communication Security Protection Group
Standards and Specification Group
Awareness Education & Personnel Training Group
Personal Information Protection & Legislation Promotion Group
Cyber-crime Prevention and Control Group
Information & Communication Environment & Internet Content Security Group

Figure 1 NICST Organizational Chart

i. Cyber Protection System: Under DCS, Executive Yuan, responsible for integrating cyber security protection resources and drawing up cyber security policies. Its divisions and assignments are as follows:

- Critical Information Infrastructure Protection (CIIP) Group: Under DCS, Executive Yuan, responsible for planning and promoting CIIP mechanisms, supervising the implementation of security protection, audit and exercise, among other tasks.
- Industrial Promotion Group: Under the Ministry of Economic Affairs, responsible for facilitating the development of cyber security industries and integrating the research resources of industries, government, and academics to develop innovative applications.
- Information and Communication Security Protection Group: Under DCS, Executive Yuan, responsible for planning and facilitating security mechanisms of governmental information and communication application services with technical support. It also supervises government agencies implementing cyber security protection and reporting and responding to any cyber security incident.

Security audits, cyber attack exercises, and helping government agencies to improve the completeness and effectiveness of their cyber protection are also its core tasks.

- Standards and Specification Group: Under DCS, Executive Yuan, responsible for making and revising cyber security-related ordinances or regulations, and developing national standards. Furthermore, it also established and maintains the cyber security operational standards and guidelines of government agencies.
- Awareness Education and Personnel Training Group: Under the Ministry of Education, responsible for promoting basic cyber security education, enhancing the cyber security of the educational system, raising public literacy of cyber security, providing cyber security services, constructing an integrated platform with universal functions, holding international cyber security competitions, facilitating industrial and academic communications, and reinforcing cyber security talent cultivation.

ii. Cyber-crime Detection and Prevention System: Under both the Ministry of Interior and the Ministry of Justice, responsible for preventing cyber-crimes, protecting citizens' privacy, facilitating the information and communication environment, and enhancing Internet content security, etc. Its divisions and assignments are as follows:

- Personal Information Protection and Legislation Promotion Group: Under the Ministry of Justice, responsible for promoting personal information protection, makes amendments to citizens' privacy protection, and revises regulations and standards related to cyber-crimes.
- Cyber-crime Prevention and Control Group: Under both the Ministry of Interior and the Ministry of Justice, responsible for investigating cyber-crimes, preventing computer crimes, carrying out digital forensics, etc.
- Information and Communication Environment and Internet Content Security Group: Under NCC, responsible for facilitating the security of information and communication environment and Internet content, as well as assisting in preventing cyber-crimes, etc.

The National Center for Cyber Security Technology (abbreviated as NCCST) was established in March 2001 to help the NICST gradually develop government cyber security protection mechanisms, as well as to provide government agencies with such technical services as security protection planning before incidents, alarms and responses during incidents, and post-incident resilience and forensics. Furthermore, the NICST has set up another "Information and communication security advisory committee" to appoint various professional cyber security experts and scholars to provide their insight with regard to national cyber security policies, management, and technologies in order to enhance the national cyber security policies and promotional strategies, industry-government-academy research energy on cyber security technologies, and information and experience sharing to ultimately empower cyber security facilities.

Meanwhile, the promotion of cyber security in the private sector has been the responsibility of the Taiwan Computer Emergency Response Team/ Coordination Center (TWCERT/CC), which assists private companies in reporting and responding to cyber security incidents and coordinating connections and collaboration among various international cyber security organizations. Through mutually beneficial collaborations and information sharing, cyber threat incident reporting and responses will be facilitated, thus elevating the overall protection level of national cyber security.

B. Promotion achievements

Since 2001, NICST has introduced four promotional phases, each with four years of cyber security programs. So far, all of these actions have clearly improved our national cyber security completeness. The key elements of these plans and projects are summarized below in Figure 2.

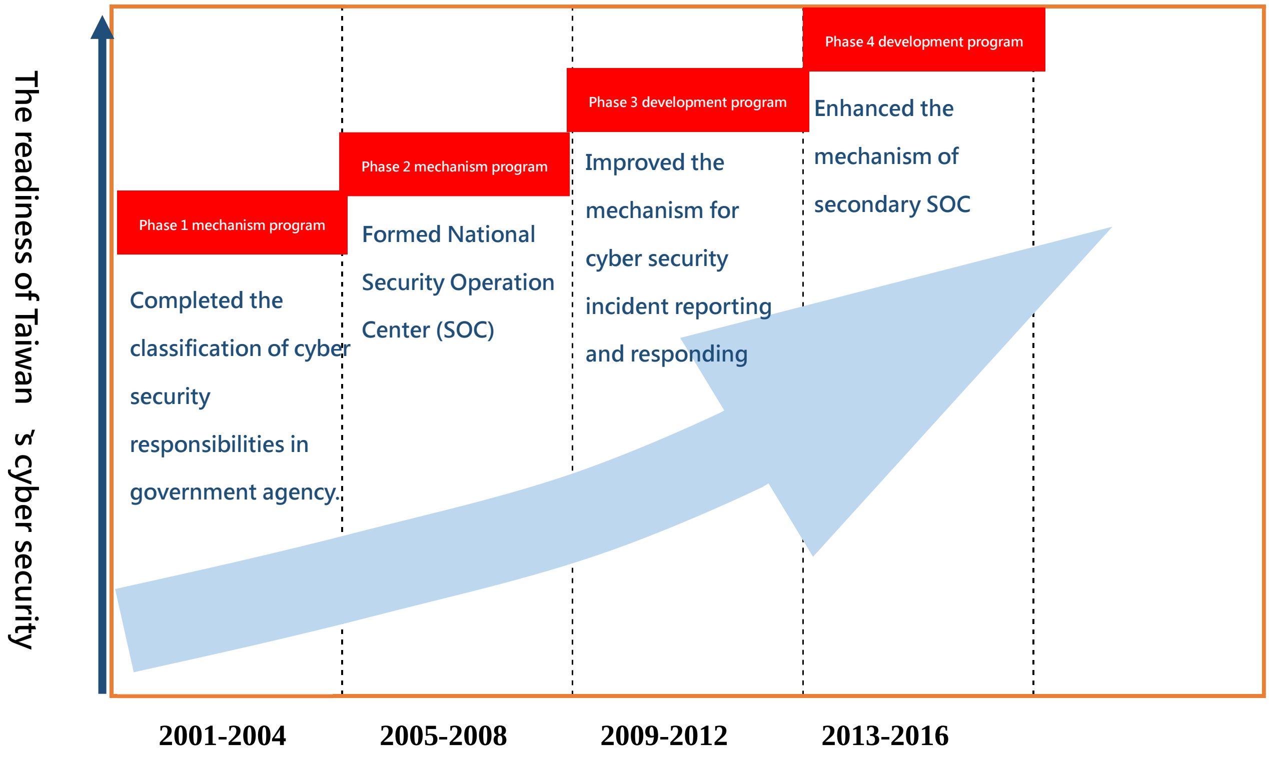

The readiness of Taiwan’s cyber security
Phase 1 mechanism program
Completed the classification of cyber security responsibilities in government agency.
Phase 2 mechanism program
Formed National Security Operation Center (SOC)
Phase 3 development program
Improved the mechanism for cyber security incident reporting and responding
Phase 4 development program
Enhanced the mechanism of secondary SOC
2001-2004
2005-2008
2009-2012
2013-2016

Figure 2 National cyber security promotional progress

i. Phase 1 mechanism program (2001-2004)

Construct a cyber security protection system and complete the classification of cyber security responsibilities in government agencies.

On January 17th, 2001 the Executive Yuan passed the ”Mechanism Program of Security in Establishing National Information and Communication Infrastructure” (abbreviated as the Phase 1 mechanism program) in its 2718th meeting. The NICST was then formed to begin government planning for the construction of national information and communication security. The Phase 1 mechanism project included:

1. Defining classification standards:

With a focus on 3,713 government agencies (units) nationwide, the overall cyber security protection system was developed, and government agencies were divided into seven different patterns, such as national defense, administration, education, business 1 (water, power, oil, gas), business 2 (traffic, communication, Internet, aviation management), business 3 (finance, stock, trade business), and business 4 (medicine); then, the following four hierarchies were established: Class A, critical core units; Class B, core units; Class C, important units; and Class D, general units, according to their functions with different levels of cyber security support provided. Each unit was further assigned different responsibilities to properly ensure cyber security protection with limited resources.

2. Facilitate implementation of the cyber security management system:

Cyber security management projects were implemented for more than 20 information systems of the critical infrastructure to facilitate application of the cyber security management system as a top priority. Construction of the alternative backup system also needed to be completed, and the international cyber security management system had to be verified.

3. Raise cyber security awareness:

The required cyber security technological or management training is arranged for information personnel and other relevant individuals.

ii. Phase 2 mechanism program (2005-2008)

Become equipped with cyber security protection capabilities and form a national cyber security operation center

The Phase 1 mechanism program was vital for developing the capabilities of national cyber security protection, so the Executive Yuan announced the “Mechanism Program of Security in Establishing National Information and Communication Infrastructure (2005 to 2008)” (abbreviated as Phase 2 mechanism program) in 2004 to implement the following cyber security tasks:

1. In 2003, the classifications of cyber security responsibilities were defined, and in 2006, the classification standards were revised to expand coverage to the educational system. The total management scope increased from 3,713 units to 6,796 units. According to the announcement made by the Directorate-General

of the Personnel Administration, Executive Yuan, all the agencies under the Executive Yuan have been covered, as have up to 80% of local government agencies.

2. The National Security Operation Center (NSOC) was established to improve real-time reporting and responses, which not only provides general monitoring and control but also includes 23 agencies under the scope of protection. Based on agencies' different requirements, various monitoring and control frameworks will be provided to enhance the government agencies' cyber security capabilities.
3. The establishment of a Chief Information Security Officer (CISO) was developed and promoted; such a person would be a part of the duty system within the government agencies and would enhance the classification of cyber security responsibilities and confidential cyber security.

iii. Phase 3 development program (2009-2012)

Enhance the overall cyber security response capabilities and upgrade mechanisms for reporting and responding

With the facilitation of the Phase 1 and 2 mechanism programs, all agencies, as well as the private sector, have become concerned with cyber security. Due to the general environmental factors and increasing cyber security issues, a continuous development program for cyber security was greatly needed. To enhance the implementation of cyber security management, the Executive Yuan issued the "National information and communication security development program (2009 to 2012)" (abbreviated as Phase 3 development program) in January 2009. The Phase 3 development program has four key policies with the objectives of enhancing overall response capabilities, providing reliable information services, optimizing the competitiveness of enterprises, and constructing an environment for the development of the cyber security culture. In 2012, by implementing 30 action plans, the investment of resources in cyber security, the completeness of cyber security regulations, public awareness of cyber security, and the overall capabilities of cyber security protection were improved and enhanced. Furthermore, the frequency of cyber security practices and losses due to cyber security incidents were reduced. Later, these good experiences related to government cyber security applications were shared and expanded to the private sector and companies.

iv. Phase 4 development program (2013-2016)

Enhance the secondary surveillance and control mechanism for cyber security protection and information sharing

In 2013, the Executive Yuan issued the "National information and communication security development program (2013 to 2016)" (abbreviated as Phase 4 development program) as a reference for our national cyber security protection development to integrate government, industrial, and public cyber security protection together using the following techniques:

1. Complete the SOC platform, second surveillance, and cyber security control services.

   Various types of cyber security equipment were installed within the intranet of government agencies to collect cyber security events as the first line of defense, which were then automatically passed to the second line G-SOC to carry out 24/7 cross-agency and cross-department relationship analysis in order to completely control attacks on government agencies' cyber security.
2. Conduct external audits of cyber security and expand the scale of cyber protection practices.

   On an annual basis, no fewer than 20 agencies shall be selected to conduct an external audit of cyber security to better understand the effectiveness and completeness of the cyber security protection measures and management policies of the agencies (units); those audited agencies would then be given suggestions about how to improve. Since 2013, some government agencies and critical infrastructures have selected large-scale cyber security protection practices to better understand whether the agencies and critical infrastructure were familiar with cyber security incidents' standard operational procedures, reporting and response procedures, and integrated preventive mechanisms so that they can minimize their overall cyber security risks.

3. Facilitate the Government Configuration Baseline (GCB) and establish Security Software Development Life Cycle (SSDLC) guidelines.

   Since 2012, all the information and communication end devices (i.e. personal laptops) in the government agencies have been set up with GCB. By 2016, all the Class 3 and Class 4 agencies central and local government agencies should have been following this policy. With regard to software security development, SSDLC guidelines were developed to improve the government agencies' overall cyber security environment.

4. Establish the verification standard and criteria of "De-identification of individual information"

   In 2015, the verification standard and criteria of "De-identification of individual information", CNS 29100 and CNS 29191, were developed, and government agencies took the lead in showing the public how concerned the government was about the potential personal information security risks caused by Big Data and Open Data. On November 30th, 2015, the Financial Information Agency, Ministry of Finance first passed the verification and then obtained the certificate issued by the Electronics Testing Center, Taiwan, thus becoming the first example.

5. Revise the classification of "government agencies (units) cyber security responsibilities"

   In response to cyber security threats and to improve national cyber security protection, the revised "Operational standards of the government agencies (units) cyber security responsibilities" were developed based on information and communication technology, cyber protection practices, and health checks and audits of the government agencies' (units) cyber security.

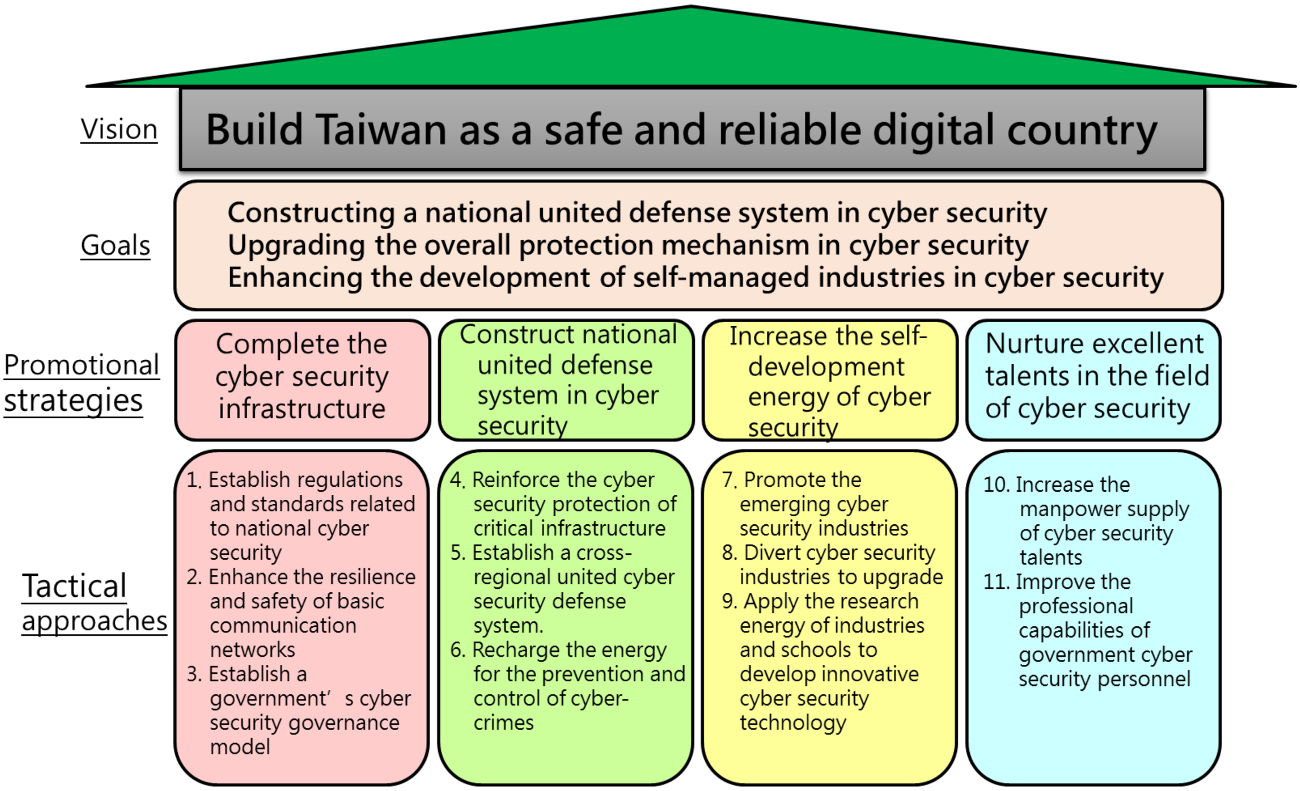
C. Advantage and disadvantage analysis of the cyber security environment

Due to our unique political and economic situations and the trend of global cyber security threats, we continuously facilitate and implement overall national cyber security protection to respond to external challenges with a sense of urgency and necessity. Using SWOT analysis, we properly assessed the advantages and disadvantages of internal cyber security environment with both external opportunities and threats to serve as critical references for program planning.

Strengths: S	**Weaknesses: W**
1. Completed four phases of the National Cyber Security development program, and the completeness of the national cyber security was improved. 2. government has elevated the cyber security leadership level and created the Department of Cyber Security, Executive Yuan, cyber security office of National Security Council, and National Communication Commission to serve as a strong foundation for the government's cyber security and the construction of a national cyber security protection mechanism. 3. NICST established the "Critical information infrastructure security management team" and "Industrial development team" to expand the scope of cyber security protection. 4. Aggressively actively promote the regulations of the "Cyber Security Administration Act" to serve as the legal positioning of national cyber security tasks and expand the Act to include related items and rules. It could then become a good foundation for constructing a digital country.	1. e have no specific national critical information infrastructure protection (CIIP) policies, protection baseline and management standards, or a continuous monitoring and controlling mechanism of CI cyber security incidents, so cyber security alarms and incidents management were difficult to implement effectively. 2. The cyber security talents of government agencies, industries, and academic territories have been too few to facilitate critical technological research and the development of local cyber security industries. 3. Both the scale and productivity of cyber security industries were too small to compete with international companies so the cyber security talent cultivation and research resources have been limited.
Opportunities: O	**Threats: T**
1. The government introduced the DiGi+ Plan to implement the 5+2 Industrial Innovations and elevate the demand for and growth of cyber security to the next level. 2. The government has established the cyber security troops and focused on cultivating talents to meet the increasing demands.	1. APT attacks and organization-based hackers are still trying to steal official government and commercial business secrets. 2. Both the frequency and scale of DDoS attacks are increasing and expanding. 3. Critical information infrastructure

3. Our national cyber security situation is unique, and dark attacks have been diverse, so we can attract other countries to initiate collaboration with us.	connections to the Internet are common so the risk of hacking is increasing, which will threaten social economics and can badly hurt national security. 4. Innovative IoT information technologies are rapidly growing, and the threats to cyber security are keeping pace.

IV. Blueprint



Vision

Build Taiwan as a safe and reliable digital country

Goals

Constructing a national united defense system in cyber security
Upgrading the overall protection mechanism in cyber security
Enhancing the development of self-managed industries in cyber security

Promotional strategies

Complete the cyber security infrastructure	Construct national united defense system in cyber security	Increase the self-development energy of cyber security	Nurture excellent talents in the field of cyber security

Tactical approaches

1. Establish regulations and standards related to national cyber security 2. Enhance the resilience and safety of basic communication networks 3. Establish a government' s cyber security governance model	4. Reinforce the cyber security protection of critical infrastructure 5. Establish a cross-regional united cyber security defense system. 6. Recharge the energy for the prevention and control of cyber-crimes	7. Promote the emerging cyber security industries 8. Divert cyber security industries to upgrade 9. Apply the research energy of industries and schools to develop innovative cyber security technology	10. Increase the manpower supply of cyber security talents 11. Improve the professional capabilities of government cyber security personnel

Figure 3 Project development blueprint

A. Vision

Our promotional activities for our national cyber security policies have passed through four phases of systematic development and have gradually achieved the periodical objectives of “Developing a safe cyber security environment, completing cyber security protection management, sharing diverse cyber security data, expanding cyber security talent cultivation, and enhancing international cyber security experience exchanges”. Therefore, the completeness of our national cyber security was effectively elevated.

Hacker attacks are becoming more diverse as information technology develops and evolves to be oriented more toward organizations. To facilitate the development of the digital economy, all kinds of basic constructions will gradually become digitalized. If cyber security incidents continue to occur frequently, economic stability, social security, and national security will not only be inconvenienced but also seriously threatened. Therefore, from the perspective of risk management, how to facilitate overall national cyber security defensive capabilities is extremely important. Furthermore, in order to coincide with the government's "5 plus 2" industry innovations and DiGi+ plan, two very important policies, we need to establish an alternative and solid security infrastructure approach to facilitate the economics of our digital country as a critical success factor. The program was based on the vision of "**Build Taiwan as a safe and reliable digital country"** to gradually improve the nation's overall cyber security defensive capabilities' energy through prospective policies and nationally integrated resource investments.

B. Objectives

According to the "Cyber security is national security" strategy, our country has improved its cyber security level to the level of national security. We have shown that we are determined to aggressively defend our digital homeland. Furthermore, to construct a complete national cyber security development strategy and prevent hacker attacks, the National Security Council (NSC) collaborated with the DCS and related units to hold the "cyber security is national security" strategic meeting in August 2016. Said meeting focused on how to establish an integrated national-level cyber security protection team and determined that the critical infrastructure for creating the Information Sharing and Analysis Center (ISAC) and Computer Emergency Response Team (CERT) cyber security management mechanism had to be shared, and then all the related responsible agencies were invited to implement said mechanism accordingly.

From this foundation, the vision of "Build Taiwan as a safe and reliable digital country" could be achieved. NCSP was based on the objectives of **"Constructing a national defense system in cyber security, upgrading the overall protection mechanism in cyber security, and enhancing the development of self-managed**

industries in cyber security”. Critical information infrastructure territories shall be taken as the basis for developing the national defense system, and we are dedicated to improving the overall cyber security protection energy in order to reduce the frequency and impact of cyber security incidents. Furthermore, the mechanism for emergency resources and the resilience following such events would be enhanced to reinforce the protection of our digital homeland’s cyber security.

While the national cyber security protection mechanism has facilitated government agencies, it has not yet been expanded to other territories of critical infrastructure, primarily because the other non-government critical infrastructures are operated by private companies. Therefore, a request that all critical infrastructure providers enhance their cyber security defensive mechanisms or set up cyber security protection related standards has no legal support. With NCSP, the Cyber Security Administration Act shall be leveraged to facilitate the completeness of national cyber security regulatory foundations and ensure that the agencies and providers responsible for critical infrastructure implement cyber security protection measures. Furthermore, this team will actively facilitate cyber security related standards and criteria, the management system of the government’s cyber security, and the improvement of the overall cyber security protection mechanism.

Critical information infrastructure security is critical to national social economics and country security; therefore, local cyber security self-managed industries and cyber security talents are essential for preparing sufficient energy to protect cyber security and the digital country’s security. The national cyber security self-managed companies are usually small- or medium-sized enterprises so they do not have the resources or talents to develop a complete solution for cyber security issues, nor can they afford the significant costs of international marketing and local services to enter the international market.

C. Promotional strategies

To construct a national united defense system, improve the overall cyber security protection mechanism, enhance the development of cyber security self-managed industries, and ensure the digital homeland’s security, NCSP included the four facilitating strategies of “Complete the cyber security infrastructure”, “Construct a national united defense system in cyber security”, “Increase the self-development energy of cyber security”, and “Nurture excellent talents in the field of cyber security” in order to gradually facilitate the advanced protection of national cyber security and an integrated protection system to create a safe and reliable digital country.

i. Complete the cyber security infrastructure

In response to rapidly growing information technology and cloud services, as well as quickly evolving cyber security attacks in this digital era, the governments of Europe, the U.S., and the Asia-Pacific area have developed many regulations and policies related to cyber security to control expected and unknown cyber security risks to respond to internal and external cyber security challenges.

Due to our unique political and economic situations, we face very serious cyber security threats and attacks. We need to have a very high standard to handle cyber security and develop cyber security into a national security framework. The NCSP started from a basic cyber security environment by way of the regulations, standards, and cyber security management to create a safe basic cyber security environment that would become the foundation of the national united defense system, cyber security industries’ self-managed energy, and cyber security talent cultivation.

1. Establish regulations and standards related to national cyber security

1.1 Complete the “Cyber Security Administration Act” and other related regulations

(1) Complete specific national cyber security acts—”Cyber Security Administration Act” to gradually implement the acts in official government agencies, critical infrastructure providers, public businesses, and government-sponsored private sectors or institutes.

(2) Complete the amendments or revisions of the related items and rules.

(3) Complete the Cyber Security Administration Act and related

regulations, standards, inspections, amendments, and revisions.

1.2 Respond to new technological developments and establish cyber security standards and criteria

(1) Continue to focus on newly developed technology and collect standards and criteria related to international cyber security in order to establish national standards that are in line with those of countries around the world.

(2) Regularly review and amend or revise cyber security operational criteria, national standards, reference guidelines, etc. in order to respond to the development trends of new technology and meet the requirements of cyber security in a digital country.

2. Enhance the resilience and safety of basic communication networks

2.1 Enhance the cyber security protection and responsive energy of the communication network

(1) Enhance the cyber security protection and response measures of the communication network to improve the toughness and security of the national basic network.

(2) Realize real-time operational statuses of critical communication networks and explore the potential cyber security threats to activate the response mechanisms and reduce cyber security risks.

2.2 Enhance IoT security and facilitate the security verification certificate

(1) Collect and analyze IoT equipment-related international cyber security criteria and standards and use them as a basis for developing national technological criteria and verification standards.

(2) Build an IoT equipment-related cyber security inspection environment and facilitate the IoT equipment security verification certificate to encourage industries to perform cyber security inspections.

2.3 Facilitate the centralized integration of government agencies' data centers and optimize the government's intranet protection framework

(1) Establish a government agency-centered data center to centralize security protection energy.

(2) Align with adjustments in the government's intranet and improve cyber security protection strategies and framework.

3. Establish the government's cyber security governance model

3.1 Develop a national-level cyber security risk management mechanism

Establish the framework and methodology for identification, assessment, processing, and monitoring cyber security risks at the national level in order to benefit national property owners and critical infrastructure providers with regard to the implementation of the cyber security management mechanism and improving the overall cyber security resilience and safety.

3.2 Help government agencies adopt the cyber security governance mechanism

(1) Develop a training and cultivating mechanism for seed teachers and evaluators in the Cyber Security Governance Maturity model.

(2) Help government agencies adopt the Cyber Security Governance and apply the Cyber Security Governance Maturity model to self-evaluations and audits in order to allocate national cyber security resources accordingly.

ii. Construct a national united defense system in cyber security

NICST has recently formed the "Critical information infrastructure security management team" in response to the increasing threats to national cyber security and to strengthen the new security triangle of the National Security Council, DCS, and the NCC. This security triangle is linked to eight critical infrastructure domains that are managed by seven government agencies. Such a connection has expanded the national united defense mechanism in cyber security and led to the establishment of the Information Sharing and Analysis Center (ISAC), the

Computer Emergency Response Team (CERT), and the Security Operation Center (SOC) at eight critical information infrastructure and national levels. A national cyber security united defense and collaboration network will be formed by information exchange from the national level, CI authorities, and providers, and it can ensure integrated cyber security protection, information sharing, and connections to the international community.

To complete that last mile to enhance local governments' cyber security protection, NCSP has facilitated local governments to create a regional integrated cyber security protection system, using six municipalities as regional leaders to connect with other cities and counties to develop local integrated cyber security protection networks. They can then connect to the national cyber security integrated protection system to strengthen the cyber security protections of both central and local governments' critical information infrastructure. The abilities of the inspection and investigation for cross-nation cyber crimes is also one of the NCSP's key aspects for enhancement.

4. Reinforce the cyber security protection of critical infrastructure

4.1 Establish policies and risk control and management principles for the critical information infrastructure's cyber security protection

(1) Establish cyber security policies, risk management mechanisms, and protection suggestions for the critical information infrastructure, and periodically review and revise them.

(2) Establish ISAC, CERT, and SOC guidelines related to critical infrastructure domains.

4.2 Instruct all critical information infrastructures to implement cyber security protection standards

(1) Develop cyber security protection strategies and protection standards related to all the critical infrastructure domains.

(2) Inventory all the information assets, systems, and networks related to critical infrastructure to establish a databank of the assets.

(3) Develop a risk assessment and management mechanism related to

all the critical infrastructure domains in order to implement risk control.

(4) Establish ISAC, CERT, and SOC related to all the critical infrastructure domains to realize cyber security information sharing, early alarms, emergency responses, and continuous monitoring and control to achieve thorough cyber security risk control.

(5) Facilitate all authorities responsible for critical infrastructure domains to study and implement cyber security protection plans to comply with cyber security protection standards.

(6) Regularly conduct reporting and response practices related to critical infrastructure domains.

5. Establish a cross-regional united cyber security defense system

5.1 Establish a national cyber security information integration and alarm center

(1) Establish N-ISAC, NCERT, and N-SOC at the national level to achieve cross-regional information sharing, emergency responses, and cyber security monitoring and control. Enhance vertical reporting and the transversal notification mechanism to control overall national cyber security risks.

(2) Analyze real-time cyber security incident patterns and measures to prepare active defensive mechanisms and establish a cross-regional cyber security integrated protection mechanism.

(3) Regularly conduct practices related to cross-regional critical infrastructures.

5.2 Combine the energies of local industries and the private sector to establish a mechanism for a domestic and international protection alliance

(1) Continue to participate in important international meetings and activities to exchange and share cyber security threats to develop international collaborations with other countries.

(2) Assist industries to build up the CERT/CSIRT mechanism and implement cyber security event reporting in order to collaborate with domestic cyber security response organizations and enhance their capabilities for handling cyber security incidents.

(3) Leverage the resources of the private sector and social media to spread messages related to cyber security and technical documents to improve the public's awareness of cyber security.

5.3 Construct a regional integrated protection system for local governments' cyber security

(1) Connect six leader municipalities with the neighboring cities or counties to facilitate their regional cyber security integrated protection. Develop united local cyber security protection networks and facilitate the government to collaborate with nearby academic institutes to jointly cultivate cyber security talents that meet both of their needs.

(2) Facilitate the introduction of the Government Configuration Baseline (GCB) and replace information hardware/software at high risk in first-line government agencies to complete enhanced vertical protection.

6. Recharge the energy for the prevention and control of cyber-crimes

6.1 Enhance the detection energy to prevent innovative cyber technological crimes

(1) Expand the cyber security information collection network and analyze new types of cyber crimes. Create an active criminal detective network to explore, test, report, and share data related to cross-agency cyber security.

(2) Study and analyze data related to cyber crimes and integrate related digital information technology to store evidence of cyber threats in order to analyze the motivations and intentions of hacker attacks to improve the detection efficiency for new cyber crime patterns.

(3) Enhance cyber hacker attack detection technologies and improve the collection of information and forensic energies related to technological cyber crimes.

6.2 Improve cyber criminal evidence collection and forensic energies

(1) Upgrade assistant tools to enhance the on-site evidence collection capabilities of first-line staff and simplify operational procedures so that digital evidence can be kept more completely to improve forensic efficiency.

(2) Integrate cross-area forensic resources and organize the relationship between various data to handle critical digital evidence in a timely manner.

6.3 Construct a cyber environment for implementing cross-border detection

(1) To respond to cross-border and undercover cyber crimes, we need to construct domestic and international relay checkpoints as a control, monitoring, and chasing mechanism so that hacked computers can be immediately discovered and the required survey can be conducted to stop cyber theft.

(2) Develop an integrated protection channel for public and private sectors to control cross-border cyber crime trails and evidence for the immediate reporting, defending, and source chasing to improve the efficiency of criminal detection and prevention.

iii. Increase the self-development energy of cyber security

Both governments and private enterprises have considerable demands for total cyber security solutions provided by relevant suppliers to equip them with sufficient cyber security protection energy. However, our local cyber security companies and their self-research and development capabilities are all small- or medium-sized enterprises so they cannot afford to quickly develop the cyber security solutions that the market requires. As a result, they rely on foreign companies for related support, making the domestic cyber security self-protection energy low and the related progress of local cyber security development slow.

NICST has created the “Industrial promotion group” to break through the bottleneck of national cyber security industrial development and also established the “National defensive requirements division” to facilitate the key “Cyber security is nation security” strategy that promotes the development of national defensive cyber security industries. Furthermore, Taiwanese cyber security industries would be able to take advantage of excellent technologies in the global cyber security market.

7. Promote the emerging cyber security industries

7.1 Connect national self-defense needs and develop a domestic cyber security industrial ecosystem

(1) Align with newly developed applications of cyber security technologies and provide the proper places for technological verification to increase independent research and development proportions of our local cyber security industries and ultimately reduce dependence on foreign products.

(2) Create opportunities for collaborations for local cyber security products and the critical environment to improve the visibility of domestic cyber security products and boost the development energy of cyber security industries.

(3) Establish a good environment for developing cyber security industries and instructing innovative startup companies or teams with development potential to facilitate the development of a growing cyber security industrial ecosystem.

8. Encourage cyber security industries to upgrade

8.1 Facilitate the cyber security products of our domestic companies to be included in common supply contracts

(1) Inventory domestic self-developed cyber security technology and critical industrial needs every year to establish the relevant cyber security industrial standards as references for related product

procurement. Through common supply contracts, we can encourage government agencies to purchase domestic cyber security products and thus increase the usage of domestically produced cyber security products.

(2) Continue to revise the cyber security industrial standards and improve products' safety in common supply contracts. Enhance the procurement of cyber security products with high quality and security in government agencies.

8.2 Develop cyber security industrial standards and establish inspection, certification, and verification mechanisms

(1) Collect, study, and analyze the technological standards of international cyber security industries as references so that we can amend and revise our national standards for information and communication products and product certification and verification mechanisms.

(2) Promote national cyber security inspection, certification, and verification mechanisms to aid domestic cyber security inspection laboratories in establishing qualified inspection service powers and instruct companies to perform product security tests and cyber security make-up consultations to elevate the competitiveness of our local cyber security products on the international market.

9. Apply the research energy of industries and schools to develop innovative cyber security technology

9.1 Encourage core and self-development orientation technology

(1) Target prospective technologies and industrial demands to facilitate the mapping of industries and academies to disseminate research results among industries and improve the domestic research energy of critical cyber security technologies.

(2) Review the unmet technological needs of cyber security industries to connect the research energies of industries and academies in order

to develop critical core cyber security technologies. Then, introduce those technologies to the critical environment for further tests to develop an international class of cyber security products, integrated technologies, and projects with constantly increasing applications.

(3) Leverage the cyber security technology research process and results to cultivate high-end cyber security professional talents and facilitate the cultivation of industrial and academic cyber security talents.

iv. Nurture excellent talents in the field of cyber security

The self-development of national cyber security industries will require stronger and more cyber security manpower for support. Since the government urgently needs to improve the quality and quantity of national cyber security talents, actively cultivating high-end cyber security talents is crucial.

10. Increase the talent supply for the cyber security market

10.1 Invest in cyber security talent cultivation in colleges and universities

(1) Survey and estimate potential gaps between the supply and demand of industries' cyber security technology and talent to provide results that can aid in academic cyber security talent cultivation planning and implementation.

(2) Propose practical approaches for guiding the integration of resources among industries, academies, and research institutes to foster cooperative educational resources, a nurturing environment and model, etc. so that a systematic and well-organized cyber security talent cultivation model can be introduced into the regular educational system to maximize talent cultivation productivity.

(3) Encourage enterprises to collaborate with schools and develop cyber security talent cultivating courses and classes that are required by relevant industries.

10.2 Select industrial professionals to help cultivate the cyber security talents required by the industries

(1) Based on cyber security task requirements, cultivate capabilities through practices and trainings to enhance the quality and quantity of cyber security talent cultivation.

(2) Develop a learning and practice platform to enhance trainees' experiences and capabilities with regard to cyber security protection arrangements.

(3) Actively facilitate collaboration with international cyber security training institutes to further encourage experience sharing among cyber security talents.

11. Improve the professional capabilities of government cyber security personnel

11.1 Develop professional skills of government cyber security personnel and a functional blueprint with related training programs

Create a functional capability blueprint for government agencies' cyber security personnel to develop their professional capabilities and plan relevant training courses to meet the manpower demands for government agencies' cyber security.

11.2 Establish the certification system of cyber security training centers

Establish a certification system for government agencies (units) cyber security training centers so that certified centers can offer cyber security-related courses, train cyber security personnel, and expand the scope of cyber security talent cultivation.

11.3 Cultivate government officials with basic cyber security knowledge

(1) Professional training courses for middle and high-level managers and certified government officials should include the subject of cyber security awareness.

(2) Enhance the facilitation of all agencies to provide cyber security awareness training for cyber security personnel and general

personnel differently based on cyber security classifications.

11.4 Facilitate government agencies to allocate the required manpower dedicated to cyber security

(1) Actively study facilitating mechanisms for cyber security manpower allocation in government agencies.

(2) Actively coordinate all agencies to appoint the required cyber security manpower step by step based on related regulations, policy priorities, and business dynamics.

D. Teamwork of government agencies

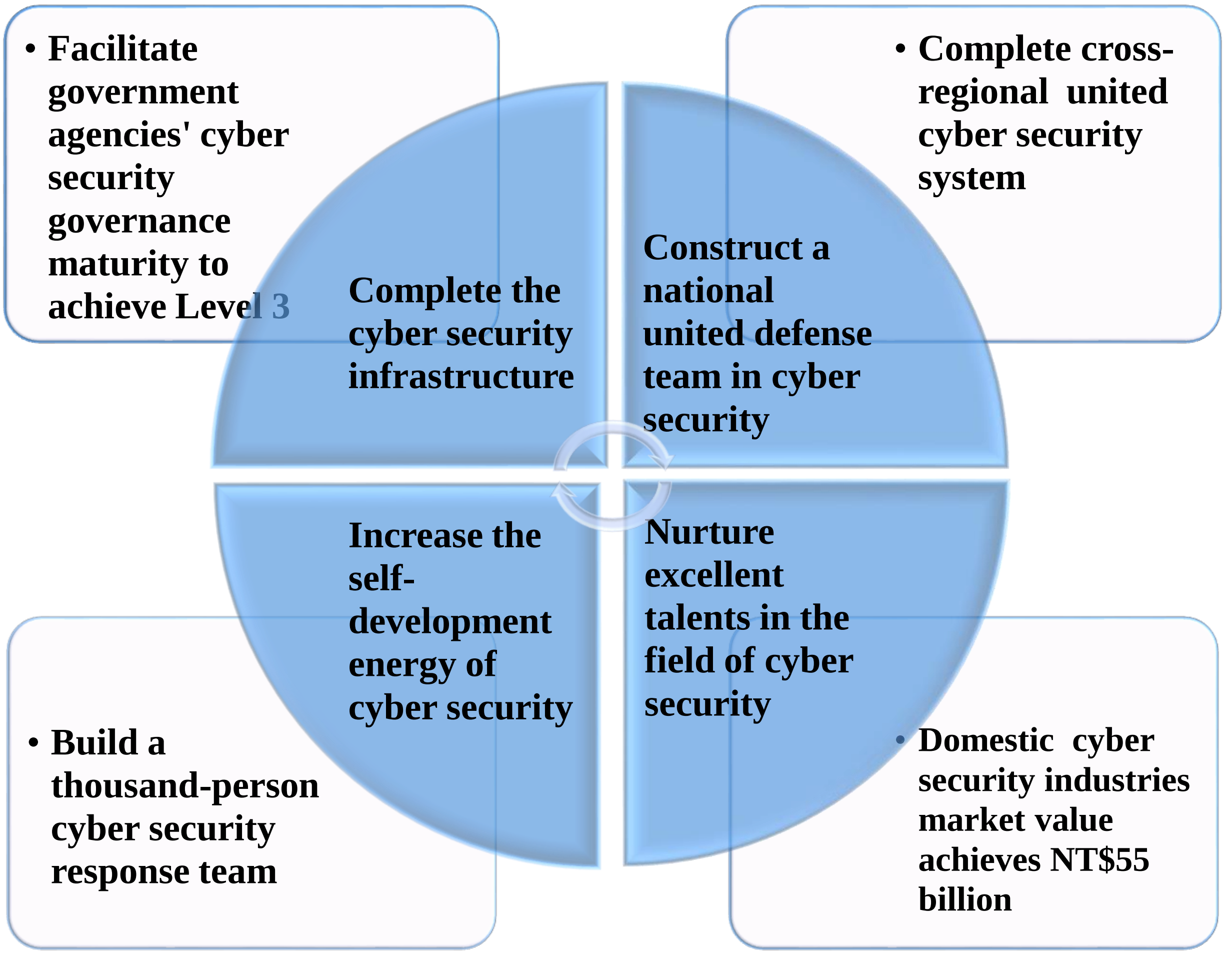
Table 1. List of teamwork tasks of government agencies

Practical approaches/Task items	Responsible agencies
1. Establish regulations and standards related to national cyber security	
1.1 Complete the "Cyber Security Administration Act" and other related regulations	DCS, Executive Yuan and related government agencies
1.2 Respond to new technological developments and establish cyber security standards and criteria	DCS, Executive Yuan and related government agencies
2. Enhance the resilience and safety of basic communication networks	
2.1 Enhance the cyber security protection and responsive energy of the communication network	NCC
2.2 Enhance IoT security and facilitate the security verification certificate	IoT targeted government administration
2.3 Facilitate the centralized integration of government agencies' data centers and optimize the government's intranet protection framework	National Development Council and all government agencies
3. Establish a government's cyber security governance model	
3.1 Develop a national-level cyber security risk management mechanism	DCS, Executive Yuan
3.2 Help government agencies adopt the cyber security governance mechanism	DCS, Executive Yuan and all government agencies

Practical approaches/Task items	Responsible agencies
4. **Reinforce the cyber security protection of critical infrastructure**	
4.1 Establish policies and risk control and management principles for the critical information infrastructure's cyber security protection	DCS, Executive Yuan
4.2 Instruct all the critical information infrastructures to implement cyber security protection standards	Authorities of CI
5. **Establish a cross-regional united cyber security defense system**	
5.1 Establish a national cyber security information integration and alarm center	DCS, Executive Yuan
5.2 Combine the energies of local industries and the private sector to establish a mechanism for a domestic and international protection alliance	DCS, Executive Yuan and Ministry of National Defense
5.3 Construct a regional integrated protection system for local governments' cyber security	All local governments
6. **Recharge the energy for the prevention and control of cyber-crimes**	
6.1 Enhance the detection energy to prevent innovative cyber technological crimes	Ministry of the Interior and Ministry of Justice
6.2 Improve cyber criminal evidence collection and forensic energies	Ministry of the Interior and Ministry of Justice
6.3 Construct a cyber environment for implementing cross-border detection	Ministry of the Interior and Ministry of Justice
7. **Promote the emerging cyber security industries**	
7.1 Connect the national self-defense needs and develop a domestic cyber security industrial ecosystem	Ministry of Economic Affairs
8. **Encourage cyber security industries to upgrade**	
8.1 Facilitate the cyber security products of our domestic companies to be included in common supply contracts	Ministry of Economic Affairs
8.2 Develop cyber security industrial standards and establish inspection, certification, and verification mechanisms	Ministry of Economic Affairs

Practical approaches/Task items	Responsible agencies
9. **Apply the research energy of industries and schools to develop innovative cyber security technology**	
9.1 Encourage core and self-development orientation technology	Ministry of Science and Technology and Ministry of Economic Affairs
10. **Increase the talent supply for the cyber security market**	
10.1 Invest in cyber security talent cultivation in colleges and universities	Ministry of Education
10.2 Select industrial professionals to help cultivate the cyber security talents required by the industries	Ministry of Economic Affairs
11. **Improve the professional capabilities of government cyber security personnel**	
11.1 Develop professional skills of government cyber security personnel and a functional blueprint with related training programs	DCS, Executive Yuan
11.2 Establish the certification system of cyber security training centers	DCS, Executive Yuan
11.3 Cultivate government officials with basic cyber security knowledge	National Development Council
11.4 Facilitate government agencies to allocate the required manpower dedicated to cyber security	DCS and Directorate-General of Personnel Administration, Executive Yuan

E. Key performance indicators



Facilitate government agencies' cyber security governance maturity to achieve Level 3
Complete cross-regional united cyber security system
Complete the cyber security infrastructure
Construct a national united defense team in cyber security
Increase the self-development energy of cyber security
Nurture excellent talents in the field of cyber security
Build a thousand-person cyber security response team
Domestic cyber security industries market value achieves NT$55 billion

Figure 4 Key performance indicators

The NCSP is based on visions, objectives, and strategies to facilitate the establishment of four key performance indicators (as shown in Figure 4)

i. Facilitate government agencies' cyber security governance maturity to achieve Level 3

According to the 2016 evaluation of the cyber security report published by Trend Micro, cyber threats have reached a new high and cost global enterprises nearly 1 billion US dollars (equivalent to NT$30 billion) due to ransomware in 2016. The quantity of those ransomware grew by seven times compared with 2015. Taiwan was ranked among the top 20% of total attacks worldwide, making it a country with high information security risk.

To effectively reduce and control government agencies' cyber security risks, cyber security governance needs to be implemented. We started instructing government agencies on how to introduce the cyber security governance maturity assessment model in 2014 in order to evaluate the effectiveness of the cyber security governance in the organizations. As of the end of 2016, 10 government agencies have held trial runs of the model. In the future, we will not only actively facilitate all government agencies to adopt the cyber security governance maturity model and regularly conduct self-evaluation, but we also aim to establish evaluation mechanisms by third parties for government agencies. Through a fair judgement of third parties, all agencies will be guided to enhance their cyber security governance to move toward established, predictable, and even innovating organizations. Class A and Class B government agencies will be supported to upgrade their cyber security governance maturity to achieve at least Level 3. The essences of government agencies' cyber security will be completed.

Regarding matters that need to be addressed, the "Cyber Security Administration Act" is the first step to facilitating regulation of cyber security governance. In response to the cyber security threats that are increasingly tougher every day and to complete regulations for the digital era, the DCS has actively worked to create the "Cyber Security Administration Act" and completed the rules and related items under the Act. With specific cyber security regulations, all agencies were authorized to sustain cyber security. Agencies responsible for critical infrastructure domains could perform inventories and amendments or revisions of the responsible regulations or standards as the basis for facilitating national cyber security tasks and elevating the protection energies of national cyber security.

ii. Complete cross-regional united cyber security system

When the WannaCry ransomware attack penetrated systems around the world in May 2017, our government agencies only suffered slightly thanks to their long-term cyber security protection preparations. Nevertheless, some administrative computers of such critical infrastructures as hospitals and power plants were infected but were managed to be kept under control with normal operations. Therefore, with regard to cyber security, facilitating critical information infrastructure protection (CIIP) is a key task of the NCSP.

The implementation of CIIP can be divided into the following three layers: the Executive Yuan, the authorities of CII domains, and the CII providers. CII would establish such platforms as SOC (pre-monitoring and controlling ahead of incidents), CERT (incidents reporting and responding), and ISAC (information sharing after an incident occurs) to implement risk management, information sharing, collaboration, report and respond mechanisms, etc. Furthermore, for integrated central and local government protection, the NCSP has created six municipality-based regional integrated protection networks to improve the energy connection of cyber security protection between local governments and central governments. As a result, the response actions of local governments to any kind of cyber security related threats should be made quicker through such resource integration and application. Then, the regional academic research institutes would be able to improve the outcome of talent cultivation along with such progress.

The NCSP plans to complete the national construction of a cross-regional cyber security integrated protection system by 2020. This vertical protection system will be constructed to link the first line of agencies and central government; from CI providers to the national level, cross-regional cyber security integrated protection would be enhanced to effectively defend against external threats and challenges related to cyber security.

iii. Domestic cyber security industries market value achieves NT$55 billion

According to the Worldwide Security and Vulnerability Management forecast issued by the International Data Corporation (IDC) in October 2016, the market size of cyber security-related hardware, software, and services will have an 8.3% compound annual growth rate from US$73.7 billion (NT$2.34 trillion) in 2016 to US$101.6 billion (NT$3.22 trillion) by 2020.

However, the market value of national cyber security industries was roughly NT$34.4 billion in 2016, which did not represent a considerable share of the market since many of the players were system integration companies with annual sales exceeding NT$0.5 billion. This situation reflects the need to upgrade local innovation and research energies. In order to upgrade the self-development energies of national cyber security, the NCSP starts from government needs and aims to help include domestic cyber security products certified by security standards in common supply contracts, encourage government agencies to adopt domestic cyber security products first, and elevate the market value of domestic cyber security industries. Government agencies can also serve as a trial area for domestic cyber security products and provide feedback to improve critical cyber security technology products and their research quality.

The NCSP plans to drive domestic cyber security industries to achieve a NT$55 billion market value by 2020. By preparing the cyber security industries' environment, establishing a security inspection mechanism, and increasing the international exposure of domestic companies, we can enhance the energy of domestic cyber security industrial development and penetrate the international cyber security market to develop a good foundation for significant growth of domestic cyber security industries in the future.

iv. Develop a thousand-person cyber security response team

Excellent cyber security talents are the key to properly constructing a national protection system. According to a survey performed by the DCS, a cyber security manpower shortage is a common concern among Class A, B, and C+ government agencies. This situation reflects the difficulties encountered in pursuing vertical protection systems in the government. To satisfy the manpower demands for national cyber security, the NCSP plans to actively cultivate professional cyber security talents through diverse, systematic channels and industrial-academic collaborations. By the end of 2020, government agencies should have their own thousand-person cyber security response teams ready. This thousand-person cyber security manpower team will carry out assigned cyber security protection tasks before cyber threat incidents occur. They should also be able to create a cross-agency emergency response taskforce when an incident does occur to immediately handle cyber security incidents. Once a case is closed, they will assist with resilience and management.

In the short term, the cyber security talents of government agencies need to be quickly cultivated. Meanwhile, the cyber security protection network of the government system needs to be more delicate and flexible in order to respond to threats. Therefore, having a cyber security service team ready is urgent, and the relevant personnel should be properly trained in a qualified training center. In the long term, the aforementioned cyber security response team will be responsible for properly training additional cyber security talents. They can link their practical experiences with training materials to further improve the quality and quantity of national cyber security talents to protect the security of our digital country.

Table 2. Yearly milestones

KPI	2017	2018	2019	2020
Facilitate government agencies' cyber security governance maturity to achieve Level 3	• Completed legislation of the Cyber Security Administration Act • Facilitate Class A and B government agencies to complete self-assessment of cyber security governance maturity	• Develop a 3rd party evaluation mechanism for cyber security governance maturity	• Facilitate 30 Class A government agencies to implement the 3rd party evaluation of the cyber security governance maturity to achieve Level 2 and above	• Facilitate all Class A government agencies to implement the 3rd party evaluation of cyber security governance maturity to achieve Level 3 and above
Complete cross-regional united cyber security system	• Construct the integrated ISAC (including government agencies, critical infrastructure domains, educational system, and the private sector)	• Develop an integrated reporting and response system and create a NCERT	• Develop an integrated monitoring and control mechanism for cyber security protection; Establish the national cyber security information integration and alarm center	• Establish national cyber security threat risk signs; Complete the cross-regional united cyber security system

KPI	2017	2018	2019	2020
Domestic cyber security industries market value achieves NT$55 billion	• Inventory domestic self-developed cyber security technologies; Build a security trial field on empirical evidence	• Instruct cyber security companies to have international exposure	• Facilitate the creation of a cyber security test environment and instruct companies to seek verification there	• Lead newly developed cyber security teams and instruct 30 companies with revenues under NT$100 million to improve the market value of domestic cyber security industries to reach NT$55 billion
Develop a thousand-person cyber security response team	• Establish a cyber security service team; Instruct agencies to implement cyber security protection and governance	• Expand the scope of the cyber security service team and cascade down to all authorities of CI	• No less than four units should pass certification to become qualified cyber security training institution	• Government agencies' (units) exclusive cyber security manpower should achieve the target of a thousand people

V. Expected effectiveness and benefits

A. Complete the foundation of regulations for the digital era and construct a safe and reliable Internet ecosystem.

B. Complete critical information infrastructures and an integrated protection system of six municipalities to improve the national defensive energy.

C. Improve the self-development cyber security energies of domestic industries to help the domestic cyber security industries achieve a market value of NT$55 billion.

D. Develop a thousand-person cyber security response team among all of the government agencies. Prepare the national cyber security manpower to protect the security of our digital country.

VI. Promotional organizations, resource requirements, and project management

A. Promotional organizations

Based on the “Key Points of the National Information and Communication Security Taskforce (NICST)”, the DCS, Executive Yuan, is responsible for policies that integrate and facilitate cyber security. This unit is responsible for all programs related to planning and facilitating.

B. Plan execution

Program-related task items and key performance indicators shall be proposed and planned by the responsible agencies and their subordinate units. Plan details will then flow to related agencies and be incorporated into their annual plans for further implementation based on the government’s administrative standards.

C. Source of budget for execution

All budgets for annual plans proposed by relevant agencies will be managed and allocated by said aforementioned agencies. Otherwise, the responsible agencies will have to independently raise funds based on related administrative procedures. These annual plans should be discussed and reviewed on an annual basis and then revised to agree with the updated budget review and pass the comprehensive evaluation.

D. Management and review of related action plans

According to the monitoring mechanism currently available, the program’s task items and key performance indicators should be managed and reviewed by the DCS, Executive Yuan, to ensure that every action is properly implemented.

E. Program review and revision

The program and its revised versions have been reviewed and approved to be implemented by the Executive Yuan. The program should be thoroughly reviewed and revised for the next four years of the development plans before the previous four years of the implementation period are completed. The development programs and related promotional plans should be reviewed with continuous updates every year.

VII. Attachments

Attachment 1. Yearly Key Milestones

Task item	Key milestones by year	Responsible (assistant) agencies
1. Establish regulations and standards related to national cyber security		
1.1 Complete the "Cyber Security Administration Act" and other related regulations	1. Before the end of 2017, completed legislation of the Cyber Security Administration Act and the related items and rules. 2. For 18 months after the regulations were approved, the Cyber Security Administration Act was implemented in three stages; the scope of the applied regulations should be reviewed two years after regulation approval.	DCS, Executive Yuan and related government agencies
1.2 Respond to new technological developments and establish cyber security standards and criteria	Complete two reviews and amendments or revisions of the cyber security related operational criteria, national standards, guidelines, etc. every year.	DCS, Executive Yuan and related government agencies

Task item	Key milestones by year	Responsible (assistant) agencies
2. Enhance the resilience and safety of basic communication networks		
2.1 Enhance the cyber security protection and responsive energy of the communication network	1. By the end of 2018, complete the establishment of the Network Operation Monitoring Center (NOMC) 2. From 2017 to 2020, complete 30 domestic critical IASP companies' referrals and connections and immediately exchange data about cyber security threats	NCC
2.2 Enhance IoT security and facilitate the security verification certificate	1. By the end of 2017, complete the inventory of the cyber security verification standards of critical IoT items, use research and analysis results to amend or revise IoT-related cyber security verification standards every year 2. By the end of 2018, develop a cyber security inspection and test environment for IoT equipment	IoT targeted government administrations

Task item	Key milestones by year	Responsible (assistant) agencies
	and instruct companies to implement cyber security inspections and the testing of IoT equipment and products.	
2.3 Facilitate the centralized integration of government agencies' data centers and optimize the government's intranet protection framework	1. By the end of 2019, the malicious IP and DNS blocking services within backbone network gateway should be expanded, including agencies' internal access circuits within the cyber security protection services 2. By the end of 2020, complete the circuit back-up mechanism of computer facilities for northern, central, and southern GSN plants	National Development Council and all government agencies
3. Establish a government's cyber security governance model		
3.1 Develop a national-level cyber security risk management mechanism	1. By the end of 2017, complete the national cyber security risk frameworks and methodology 2. From 2018 to 2020, facilitate the critical	DCS, Executive Yuan

Task item	Key milestones by year	Responsible (assistant) agencies
	infrastructures to implement the cyber security risk assessment and management	
3.2 Help government agencies adopt the cyber security governance mechanism	1. By the end of 2017, promote Class A and B government agencies' complete self-assessment of cybersecurity governance maturity. 2. By the end of 2018, establish the 3rd party evaluation mechanism of cyber security governance maturity. 3. By the end of 2019, facilitate 30 Class A government agencies to implement the 3rd party evaluation of cyber security governance maturity. 4. By the end of 2020, facilitate all Class A government agencies to implement the 3rd party evaluation of the cyber security governance maturity.	DCS, Executive Yuan and all government agencies

Task item	Key milestones by year	Responsible (assistant) agencies
4. Reinforce the cyber security protection of critical infrastructure		
4.1 Establish policies and risk control and management principles for the critical information infrastructure's cyber security protection	1. By the end of 2017, the policies and suggestions of critical information infrastructure cyber security protection have been completed. 2. By the end of 2017, the guidelines of ISAC, CERT, and SOC for CI have been completed.	DCS, Executive Yuan
4.2 Instruct all the critical information infrastructures to implement cyber security protection standards	1. By the end of 2017, Information Sharing and Analysis Centers (ISAC) for all critical infrastructures had been established; by the end of 2018, expand the scope of ISACs. 2. By the end of 2019, complete the following tasks: (1) Create computer emergency response teams (CERT) for all critical infrastructures. (2) Instruct all critical infrastructures in developing and implementing their cyber	Authorities of CI

Task item	Key milestones by year	Responsible (assistant) agencies
	security protection strategies and standards. (3) Thoroughly inventory the information assets and complete risk assessment for critical infrastructures. 3. By the end of 2020, complete the security operation center (SOC) for all critical infrastructures.	
5. Establish a cross-regional united cyber security defense system		
5.1 Establish a national cyber security information integration and alarm center.	1. By the end of 2017, create a national information sharing and analysis center (N-ISAC). 2. By the end of 2018, establish a national computer emergency response team (N-CERT). 3. By the end of 2019, establish a national security operation center (N-SOC). 4. Implement practices related to cross-regional	DCS, Executive Yuan

Task item	Key milestones by year	Responsible (assistant) agencies
	critical infrastructure every year.	
5.2 Combine the energies of local industries and the private sector to establish a mechanism for a domestic and international protection alliance	1. Participate in key domestic and international events and meetings related to cyber security integrated protection and seek both domestic and international cyber security integrated protection collaborations to create a mechanism with mutual benefits. 2. Establish connections with domestic and international cyber security organizations to facilitate the exchange of cyber security information and related collaborations.	DCS, Executive Yuan and Ministry of National Defense
5.3 Construct a regional integrated protection system for local governments' cyber security	1. 95% of first-line agencies introduced government configuration standards (GCB). 2. Information equipment with high risks in agencies shall be gradually replaced. By the end of 2020, 95% of such equipment should be replaced.	All local governments

Task item	Key milestones by year	Responsible (assistant) agencies
	3. By the end of 2020, the regional integrated protection system of six municipalities will be completed.	
6. Recharge the energy for the prevention and control of cyber-crimes		
6.1 Enhance the detection energy to prevent innovative cyber technological crimes	By the end of 2018, develop collection and research mechanisms for new types of cyber threats and attacks, as well as a reporting defensive mechanism. Furthermore, improve the practical training of criminal detective skills to enhance the new types of detection and prevention for cyber crimes.	Ministry of the Interior and Ministry of Justice
6.2 Improve cyber-criminal evidence collection and forensic energies	By the end of 2019, gradually consolidate the nation's resources related to cyber crime evidence collection and forensic services to continuously upgrade digital forensic knowledge and immediately control critical digital evidence to enhance forensic efficiency.	Ministry of the Interior and Ministry of Justice

Task item	Key milestones by year	Responsible (assistant) agencies
6.3 Construct a cyber environment for implementing cross-border detection	By the end of 2020, gradually complete the cross-border pursuit of cyber crimes and the related preventive mechanism, develop a public and private joint integrated protection channel to continuously construct mechanisms for pursuing potential security threats and criminal targets.	Ministry of the Interior and Ministry of Justice
7. Promote the emerging cyber security industries		
7.1 Connect the national self-defense needs and develop a domestic cyber security industrial ecosystem	1. By the end of 2017, complete the inventory of cyber security industries' demands and situations. 2. By the end of 2020, assist in establishing at least 30 cyber security startups and facilitate the mapping of startups and venture funds. 3. Instruct companies of newly developed cyber security application technology to implement the verification of critical infrastructure technology	Ministry of Economic Affairs

Task item	Key milestones by year	Responsible (assistant) agencies
	twice a year.	
8. Encourage cyber security industries to upgrade		
8.1 Facilitate the cyber security products of our domestic companies to be included in common supply contracts	Based on the key demands of industries, establish related cyber security industrial standards as a reference for related product procurement. Aligned with common supply contract criteria, facilitate government agencies to purchase domestic cyber security products.	Ministry of Economic Affairs
8.2 Develop cyber security industrial standards and establish inspection, certification, and verification mechanisms	1. Amend or revise at least three national standards related to cyber security per year. 2. By the end of 2020, develop a self-operational system of cyber security industrial standards certification and verification; instruct companies to pass cyber security inspection, test, certification, and verification.	Ministry of Economic Affairs
9. Apply the research energy of industries and schools to develop innovative cyber security technology		

Task item	Key milestones by year	Responsible (assistant) agencies
9.1 Encourage core and self-development orientation technology	1. By the end of 2017, complete cyber security critical technology POC and initial environmental simulation; introduce on-site verification to the critical environment in 2018. 2. By the end of 2020, develop new application and technologies related to integrated cyber security; promote related applications and products.	Ministry of Science and Technology and Ministry of Economic Affairs
10. Increase the industrial cyber security talent supply		
10.1 Invest in cyber security talent cultivation in colleges and universities	1. By the end of 2018, establish a seed teachers selection mechanism for cyber security for overseas study. 2. By the end of 2020, establish a systematic cultivation mechanism in universities and colleges to develop cyber security talents.	Ministry of Education
10.2 Select industrial professionals to help cultivate the	1. Regularly hold international cyber security	Ministry of Economic

Task item	Key milestones by year	Responsible (assistant) agencies
cyber security talents required by the industries	competitions; cultivate individuals to participate in cyber security competitions. 2. By the end of 2018, introduce advanced cyber security programs from other countries to the necessary industries and have them put through test runs. 3. By the end of 2019, localize advanced cyber security programs and provide such programs to the industries. 4. By the end of 2020, cultivate 2,000 talents to work in the field of industrial cyber security.	Affairs
11. Improve the professional capabilities of government cyber security personnel		
11.1 Develop professional skills of government cyber security personnel and a functional blueprint with related training programs	1. By the end of 2017, complete government cyber security personnel and functional blueprint with related training programs.	DCS, Executive Yuan

Task item	Key milestones by year	Responsible (assistant) agencies
	2. Promote the training of government cyber security personnel annually.	
11.2 Establish a certification system for information security training units	1. By the end of 2017, complete development of the certification system planning for cyber security training institutions. 2. From 2018 to 2019, instruct two training institutes to assess certification.	DCS, Executive Yuan
11.3 Cultivate government officials with basic cyber security knowledge	1. By the end of 2017, incorporate cyber security programs into training courses for relevant middle and senior managers and personnel that have passed the national examinations. 2. By the end of 2020, align the cyber security related central and local agencies to facilitate basic cyber security courses and digital classes to improve information personnel and general government	National Development Council

Task item	Key milestones by year	Responsible (assistant) agencies
	officials' basic cyber security knowledge.	
11.4 Facilitate government agencies to allocate the required manpower dedicated to cyber security	Assist the responsible agencies in gathering information (security) manpower and continuously facilitate the four information (security) tasks available. Furthermore, according to the "Basic Law for Central Government Agency Manpower Allocation", review the manpower allocation to save the manpower necessary for supporting cyber security.	DCS and Directorate-General of Personnel Administration, Executive Yuan

Attachment 2. National Information and Communication Security Taskforce (NICST) setting specifications

Established and announced by the Executive Yuan. Document No. T90E069579-1 (台 90 經字第 069579-1 號函)

Reviewed and revised by the Executive Yuan on March 17th, 2003.

Revised and announced by the Executive Yuan on April 18th, 2005; Document No. YTT94008356(院台科字第 94008356 號函)

Revised and announced by the Executive Yuan on September 14th, 2006. Document No. YTE0950091248（院台經字第 0950091248 號函）

Revised and announced by the Executive Yuan on July 29th, 2008. Document No. YTE0970088180（院台經字第 0970088180 號函）

Revised and announced by the Executive Yuan on December 31st, 2009. Document No. YTE0980099344（院台經字第 0980099344 號函）

Revised and announced by the Executive Yuan on March 7th, 2011. Document No. YTE1000093156（院臺經字第 1000093156 號函）

Revised and announced by the Executive Yuan on January 4th, 2013. Document No. YTPD1010155308（院臺護揆字第 1010155308 號函）and effective on January 1st, 2013.

Revised and announced by the Executive Yuan on March 24th, 2014. Document No. YTP1030128738（院臺護字第 1030128738 號函） and effective on 3rd March, 2014.

Revised and announced by the Executive Yuan on December 29th, 2014. Document No. YTP1030157519（院臺護字第 1030157519 號函） and effective on 29th December, 2014.

Revised and announced by the Executive Yuan on March 13th, 2015. Document No. YTP1040126086（院臺護字第 1040126086 號函） and effective on March 13th, 2015.

Revised and announced by the Executive Yuan on January 19th, 2016. Document No. YTP1050150599（院臺護字第 1050150599 號函） and effective on January 20th, 2016.

Revised and announced by the Executive Yuan on August 24th, 2016. Document No. YTP1050173756（院臺護字第 1050173756 號函） and effective on September 1st, 2016.

A. The Executive Yuan aims to establish National Information and Communication Security policies, speed up the construction of the National Information and Communication Security environment, and improve national competitiveness and has thus developed the National Information and Communication Security Taskforce (NICST).

B. The tasks of NICST are listed as follows:

i. Consultation and review of National Information and Communication Security policies.

ii. Consultation and review of National Information and Communication Security report and response mechanisms.

iii. Consultation and review of major National Information and Communication Security plans.

iv. Coordination and instruction of cross-agency information and communication security affairs.

v. Other business items assigned by the Executive Yuan related to National Information and Communication Security.

C. The NICST shall have one chairman, the Vice Premier of the Executive Yuan, who shall serve concurrently; two vice chairman, the Minister without portfolio assigned by the Premier of the Executive Yuan and Minister of related ministries will serve concurrently; one co-vice chairman of the Advisory Committee of the National Security Council serves concurrently; and 18 to 35 committee members. In addition to chairman, vice chairman, and co-vice chairman, other committee members are related to cyber security and selected from vice ministers of ministries or municipalities, scholars and experts by the premier of the Executive Yuan. Any committee member who is not a representative of the government agency can be replaced when the chairman resigns.

D. Department of Cyber Security, Executive Yuan is the staff unit of NICST.

E. NICST has two direct reporting units, the Cyber Protection System and the Cyber-crime Detection and Prevention System. Their host agency and assignments are as follows:

i. Cyber Protection System: Under DCS, Executive Yuan, responsible for integrating cyber security protection resources and drawing up cyber security policies. Its divisions and assignments are as follows:

1. Critical Information Infrastructure Protection (CIIP) Group: Under DCS, Executive Yuan, responsible for planning and promoting CIIP mechanisms, supervising the implementation of security protection, audit and exercise, among other tasks.

2. Industrial Promotion Group: Under the Ministry of Economic Affairs, responsible for facilitating the development of cyber security industries and integrating the research resources of industries, government, and academics to develop innovative applications.

3. Information and Communication Security Protection Group: Under DCS, Executive Yuan, responsible for planning and facilitating security mechanisms of governmental information and communication application services with technical support. It also supervises government agencies implementing cyber security protection, reporting and responding to any cyber security incident. Security audits, cyber attack exercises, and helping government agencies to improve the completeness and effectiveness of their cyber protection are its core tasks too.

4. Standards and Specification Group: Under DCS, Executive Yuan, responsible for making and revising cyber security-related

ordinances or regulations and developing national standards. Furthermore, it also established and maintains the cyber security operational standards and guidelines of government agencies.

5. Awareness Education and Personnel Training Group: Under the Ministry of Education, responsible for promoting basic cyber security education, enhancing the cyber security of the educational system, raising public literacy of cyber security, providing cyber security services, constructing an integrated platform with universal functions, holding international cyber security competitions, facilitating industrial and academic communications, and reinforcing cyber security talent cultivation.

ii. Cyber-crime Detection and Prevention System: Under both the Ministry of Interior and the Ministry of Justice, responsible for preventing cyber-crimes, protecting citizens' privacy, facilitating the information and communication environment, and enhancing Internet content security. Its divisions and assignments are as follows:

1. Personal Information Protection and Legislation Promotion Group: Under the Ministry of Justice, responsible for promoting personal information protection, making amendments to citizens' privacy protection, and revising regulations and standards related to cyber-crimes.
2. Cyber-crime Prevention and Control Group: Under both the Ministry of Interior and the Ministry of Justice, responsible for investigating cyber-crimes, preventing computer crimes, carrying out digital forensics, etc.

To actively propose national cyber security policies and facilitate strategies, we will enhance the cyber security experience sharing and exchange between cyber security industries, government agencies, and academic institutions, as well as fulfill the energy required for cyber security. Thus, NICST will set up a Cyber Security Consulting Committee accordingly.

F. Each aforementioned group shall appoint one chairman who is selected from the committee of the host agency and is responsible for determining the operational criteria required by each group.

The Cyber Security Consulting Committee shall have 17 to 21 committees. The NICST chairman will appoint talents, scholars, and experts in the field of cyber security as committee members with terms of two years of service, which may be extended.

G. In principle, NICST and the Cyber Security Consulting Committee should hold a joint meeting every six months or extraordinary meetings as required, and all such meetings should be chaired by the NICST chairman.

H. The committee members and each group chairman of NICST and Cyber Security Consulting Committee are all non-paid positions.