National Cyber Security Program of Taiwan (2021 to 2024)

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

February, 2021

Table of Contents

I. Background

In the current digital age, information and communication technology has long been integrated into various aspects of daily life, such as Internet of Things (IoT), Artificial Intelligence (AI), and 5th generation (5G) mobile networks and other technologies. While we enjoy the convenience of technology, there have also been various kinds of cyber security threats, such as Advanced Persistent Threat (APT) attacks, Distributed Denial of Service (DDoS) attacks, and Critical Infrastructure (CI) hacking, and so on. Undoubtedly, cyber security holds a significant impact on national security, public interest, national life, or economic activities. It is indeed necessary to enhance the national security protection capacity and strengthen the security and resilience of basic communication networks.

In addition, in recent years, our country has successively promoted the "5+2 Innovative Industries Plan" and the "Digital Nation and Innovative Economic Development Program (2017-2025)" (DIGI^{+} program) and built “The Six Core Strategic Industries" based on the foundation of 5+2 industrial innovation. Through building Taiwan-based brands, flexible and diverse financial backup systems, a secure industrial development environment, and the gathering and training of digital/bilingual talents, Taiwan has been made a key force in the global economy. However, in the transformation process to an innovative economy, various industries should incorporate cyber security protection thinking to form the basis of the united defense of government agencies and private enterprises, so that the awareness of cyber security will be deeply rooted in our mindset. In this

way, we shape a culture of cyber security, enhance capabilities (soft/hard power) of national cyber security, and build a smart country where the public can trust and rely on.

Since there is a wide application of information and communication services; cyber security plays a key role in our national security and even the aspects of the social-economic application with technology innovation policies, to respond to international trends and emerging types of cyber security attacks and threats, we will continue to develop our cyber security protection capabilities and advantages on the existing basis and aspects of defense. Besides implementing the fifth phase of the National Cyber Security Program of Taiwan (2017-2020), to gradually enhance our cyber security protection capabilities, the National Information & Communication Security Taskforce (hereinafter referred to as the NICST) of Executive Yuan proposed the "National Cyber Security Program of Taiwan (2021-2024)" (hereinafter referred to as NCSP) as the reference guide for promoting our cyber security protection strategy and plan.

II. Global Cyber Security Threats and International Policy Trends

A. Trend of Global Cyber Security Threats

According to the “Global Risk Report” of World Economic Forum (WEF), in the ranking of 2020 global potential risk, either in Global Risks in Terms of Impact or Global Risks in Terms of Likelihood, the ranking of cyber attacks was within the top 10. It is obvious that cyberattacks have become another kind of virtual warfare, with impacts ranging from personal lives to as significant as national security levels.

Cyberattacks have become an important science of cyber security. Through a comprehensive study of global major cyberattacks in 2019, based on the types and numbers of cyber security incidents and further analysis of related global cyber security attacks, we conclude there are six major trends of cyber security threats, including "the intensification of personal data and digital certification leakage attacks”, “the proliferation of ransomware attack risks", "the increase of threats of vulnerabilities of IoT and mobile devices", "APT targeted attacks to steal confidential data", "the hacking of cyber security (information) suppliers destroying supply chain security" and "the multiplication of critical information infrastructure security risks". They are respectively explained as follows:

(A) The intensification of personal data and digital certification leakage attacks

The identity intelligence company 4iQ released the "2019 4iQ Identity Breach Report" in Q1 of 2019. The report stated that there were about 14.9

billion identity data circulated on the Internet in 2018, far higher than the 8.7 billion in 2017. If we analyze the industries where the leaks occurred, online forums accounted for 27.5%, followed by government agencies (12.2%), gaming industries 11.8%, e-commerce websites 11.7%, and education and academia 9.2%. According to the data analysis, only 37% of the personal identification data circulated on the Internet were leaked due to hacker attacks, while the remaining 63% were accidentally exposed. 4iQ speculated that it was caused by many companies transforming their systems to the Cloud, failing to attend to access control, and therefore accidentally caused the leakage of databases and servers.

In Q4 of 2019, the incident that an employee stealing a customer service database from a major domestic technology company showed that the companies were facing a more serious insider threat. On November 5 of the same year, the company confessed on its official blog that it discovered employees had stolen information from the customer service database and sold it to unknown criminal organizations for profit, affecting nearly 120,000 users. Therefore, the source of personal information and credential leakage may not only result from malicious attacks by external hackers but also accidental or malicious internal leakages.

(B) The proliferation of ransomware attack risks

In October 2019, the cyber security service provider Emsisoft announced on its official blog the results of the ransomware survey of the United States in the first three quarters of 2019. This survey was based on statistics of US government agencies, schools, and medical service providers that have been

attacked by ransomware. The results showed that at least 621 organizations have been attacked by ransomware in the past nine months. When a state, city, or county in the United States was attacked by ransomware, it was easy to be reported and become headlines. However, out of the 621 organizations that were attacked, only 68 were government agencies, which meant that more organizations were subject to ransomware attacks but chose to keep them confidential.

According to the observation of Emsisoft, more and more hackers are targeting web hosting service providers or third-party service providers since one successful attack can simultaneously intrude multiple organizations that adopt the same information service. Besides, the redemption required by hackers is getting bigger. If the victim is willing to pay for the first time, then hackers may increase the ransom for the next time. Another trend worth observing is the rise of cyber security insurance. When more organizations purchase cyber security insurance, the organization will be more willing to pay the redemption and become the target of hackers' continuous attacks and increase their motivation.

If we analyze the current attack methods of ransomware, we may conclude that compared with the traditional method of directly attacking the target, hackers first try to attack the third-party service provider with a weaker protection level, and then attack the real target. At the same time, as the victim is exposed to the transfer of insurance risk and chooses to pay the ransom, it further encourages the prevalence of ransomware intrusions.

(C) The increase of threats of vulnerabilities of IoT and mobile devices

In the past 2016 years, hackers used the Mirai botnet virus to hijack 500,000 webcams and launched DDoS to storm the web hosting industry. Subsequently, the research unit of Palo Alto Networks discovered 11 new Mirai variant viruses in early 2019. Different from the previous version, these variant viruses targeted enterprise-level IoT devices, such as wireless projection systems, smart TVs, etc. Hackers seem to have turned their targets to corporate networks to gain greater bandwidth to establish botnets to facilitate DDoS attacks in the future.

The risk of mobile devices is increasing with a wider range of applications and the popularity of mobile devices. In the worldly renowned white hat hacker contest "PWN2OWN" held in Tokyo in November 2019, participating hackers cracked multiple connected devices, such as mobile phones, routers, and smart home devices, and exposed their leaks.

(D) APT targeted attacks to steal confidential data

Hackers usually use the APT attacks to target objects with confidential data or a large amount of personal data, such as financial industry, defense units or social media, etc., especially cloud services that government agencies or enterprises rely on are all targets of attack. After deciding the target, hackers deliberately collect their potential weaknesses and vulnerabilities, including social engineering techniques, vulnerabilities of information and communication systems, supply chain, and other possible intruding methods to achieve the goal of invading the organization successfully.

In 2019, Frankfurt of Germany suffered an Emotet malware targeting attack, which caused several cities and academic networks to shut down.

Emotet boasted a self-propagating advanced modular Trojan program, which was initially used by hackers for banking Trojan malware, but recently widely used as a spreading program for other malware or malicious attacks. Emotet uses a variety of methods and intrusion techniques to continue and maintain the spreading, mainly through phishing spam containing malicious attachments or links. After being infected by the Emotet malware, the internet in Frankfurt shut down in December 2019. Before that, the internet of two universities in Germany and another city north of Frankfurt suffering from Emotet attacks also shut down. From such an example, we may know the attack impact must be handled carefully.

(E) The hacking of cyber security (information) suppliers destroying supply chain security

Cyber security company Proofpoint released a message on its official website in September 2019 that a national hacker group continued to target Utilities Sector suppliers in the United States and launched a Spear Phishing attack on the victim's system. According to the statistics, through planting the LookBack malware on the victim's system, at least 17 vendors have been attacked. Proofpoint further pointed out that the same hacker group launched a new attack in August of the same year. The target for this time was also a U.S. utility service provider. It was disguised as a Global Energy Certification Authority (GEC) in the phishing email, invited the victim to take the certification exam and attached a Word file containing the malicious macro. Proofpoint said that surprisingly the hacker group has not disappeared due to the exposure of the previous attack. Instead, they have continuously improved

their phishing attack strategies, techniques and procedures, clearly exposing thier malicious intentions against U.S. utility service providers.

Since suppliers may neglect the importance of cyber security due to defects in the cyber security protection mechanism or focus on business growth, they are more vulnerable than the real target of hackers' attack. In this regard, hackers can use information and communication equipment suppliers as a springboard to further attack the real targets.

(F) The multiplication of critical information infrastructure security risks

There is a wide range of CI which is inseparable from our lives, including energy, water resources, communications, transportation, finance, emergency rescue, hospitals, government agencies, Hi-Tec industrial parks. The information and communication system required to support CI is the Critical Information Infrastructure (CII), also an important area of protection. Once hacked, it will affect the citizen's lives, even social order, and national security. In recent years, as the CII information architecture has become more open and connected to the Internet, related cyber security risks have also increased.

The National Energy Technology Laboratory of the U.S. released the OE-417 Electric Power Emergency and Interference Report for Q1 of 2019, explaining the outage of the power system caused by cyber attacks. The report showed that the victim of the attack was a Renewable Energy electricity producer in Utah. The attack used known vulnerabilities in the firewall to trigger a Denial of Service (DoS) command, which caused the system to restart, resulting in the disruption of communication among the devicies of the company's control center and other sites.

Another issue that continues to draw great attention from governments and society is the Darknet, which greatly affects social order and security. According to cyber security company Digital Shadows's Photon Research Team, the number of stolen user accounts and passwords circulated on the darknet is near twice the world's population. The vouchers sold and shared by dark web sellers totaled 15 billion sets of leaked vouchers. Among them, one-third of which were unique vouchers. The account information leakage mainly came from online services, such as online banking, social networking sites, and music streaming services. The use of the dark web for transactions in the black market has also increased the number of certificate leakage and caused incessant cyber security incidents.

B. The Development Trends of International Cyber Security Policies

In this section, we comprehensively analyze the critical cyber security policies and regulations of major countries or international organizations, such as the United States, Canada, the European Union, the United Kingdom, Japan, South Korea, Singapore, Australia, and Israel. We also summarize the corresponding countermeasures for the continuously evolving cyber attack patterns as the reference for this program.

(A) The United States

The US agency for cybersecurity is the Department of Homeland Security (DHS). After 2018, the United States passed the Cybersecurity and Infrastructure Security Agency (CISA) Act, which was responsible for the

cybersecurity-related business. In addition, the National Institute of Standard and Technology (NIST) has formulated the national measurement standards. NIST released Cybersecurity Framework (CSF) version 1.0 in February 2014 and the revised version 1.1 in April 2018 for the compliance of various federal government agencies or related units. The key points are summarized in Table 1.

Table 1: NIST CSF in the U.S. (April, 2018/ Version 1.1)

Identify	Protect	Detect	Respond	Recover
1. Asset Management 2. Business Environment 3. Governance 4. Risk Assessment 5. Risk Management Strategy 6. Supply Chain Risk Management	1. Access Control 2. Awareness and Training 3. Data Security 4. Info Proteciton Processes and Procedures 5. Maintenance 6. Protective Technology	1. Anomalies and Events 2. Security Continuous Monitoring 3. Detection Processes	1. Response Planning 2. Communications 3. Analysis 4. Mitigation 5. Improvements	1. Recovery Planning 2. Improvements 3. Communications

Source by：NIST Cybersecurity Framework

The CSF architecture of NIST in the United States is distinguished by five functions: Identify, Protect, Detect, Respond, and Recover (the architecture is shown in Figure 1). Various federal government agencies and critical infrastructure are combined with NIST's CSF framework and cybersecurity-related documents, such as the Special Publication (SP) 800 series, to plan and establish cybersecurity management systems. Since the structure can also be applied to general enterprises, it has gradually become one of the main reference tools for the risk management of cyber security for

enterprises or organizations in other regions or countries.

To further enhance active defense and related energy, protect national assets and our privacy, and increase the cost of malicious attacks, the United States announced the National Cyber Strategy in September 2018, scoring 4 major dimensions and 10 goals. The strategy would provide secure networks, information, critical infrastructure, and actively combat cybercrimes and strengthen incident notification and response. Accordingly, it is expected to strengthen cybersecurity management, risk management, supply chain security, and related actions.

Figure1: The Framework of CSF of NIST in the United States

(B) Canada

The Canadian cybersecurity authority is the Department of Public Safety (PS). In order to strengthen the capabilities related to cybersecurity, in 2018, in accordance with the "National Cyber Security Strategy (NCSS)", Canada integrated business units related to cybersecurity and established the Canadian Centre for Cyber Security (CCCS).

The establishment of the Information Communication Security Center is

mainly responsible for the cybersecurity incidents response procedure and cooperation with the Computer Emergency Response Team (CERT) of the country and the Computer Incident Response Team (CIRT) of the government, together with other government agencies, critical infrastructure, enterprises, and international partners. The center also monitors and identifies threats, risks, and vulnerabilities; assists federal government departments in strengthening cybersecurity defense capabilities; and actively cooperates with researchers, critical infrastructure, and academic institutions to solve related cybersecurity issues.

Canada announced the National Cyber Security Action Plan 2019-2024 in May 2019. There were three major goals: (1) Strengthen critical infrastructure protection and enhance cybercrime investigation capabilities, (2) Support forward-looking research and assist innovative enterprises, (3) Initiate domestic provincial and non-governmental cooperation; collaborate with foreign alliances to jointly shape the environment.

In order to strengthen public-private cooperation to jointly combat cybercrime, Canada will expand the Cyber Security Cooperation Program (CSCP), strengthen connections with internal and external stakeholders such as the public and communities and provide necessary resources.

(C) The EU

The competent authority of the EU's cyber and information security is the European Union Agency for Cybersecurity (ENISA). The European Union enacted the Cybersecurity Act in June 2019 to expand ENISA’s rights and obligations. It not only helped ENISA strengthen its governance authority,

increase the allocation of human and financial resources, but also establish a European Cybersecurity Certification Scheme mechanism to assess the safety standard of information and communication products, services and manufacturing processes. The summary of the certification methods, content, and affected objects is as follows:

1. Method: Set product or service category, cybersecurity specifications (such as reference standards or technical specifications), assessment type (such as self-assessment or third-party assessment), expected assurance level (such as basic, substantial, high). Three levels are used on the certificate: basic, substantial, and high to show their cybersecurity risks. Products certified as high-level have passed the highest level of security testing, allowing companies to conduct Cross-border transactions and make it easier for users to understand the safety of products or services. It also enables beneficial competition among suppliers in the EU market, resulting in better products and cost-effectiveness.
2. The value to small and medium-sized enterprises and new enterprises: It helps to reduce the barriers for small and medium-sized enterprises and new enterprises to enter the market because the company only needs to pass product certification once, and its certificate is valid throughout the EU, and at the same time, as security requirements increase SMEs with certified products will enjoy a certain global competitive advantage.
3. Cybersecurity verification or certification mechanism: Suppliers use this mechanism to obtain certificates for their products to ensure that the Information Communication Technology (ICT) products, services, and

processes maintain a sufficient level of cybersecurity and improve the operation of the internal market.

4. Design safety: Encouraging development manufacturers or providers of product, service, or process design to implement this mechanism at the initial stage of design and development, protecting the safety of these products, services, or processes, and minimizing damage from cyberattacks.
5. Beneficiaries: such as citizens and operators. For individuals, commercial buyers, and governments, when purchasing a product or service, they can query the ENISA cybersecurity certification website to obtain information about the product or service. (The information will be more transparent.) The product and service suppliers and providers (including small and medium-sized enterprises and start-ups) can also obtain relevant certificates through this mechanism to enhance their competitiveness.

(D) The UK

The competent authority of the UK government's cyber security is the National Cyber Security Centre (NCSC). In November 2016, it announced the National Cyber Security Strategy 2016-2021, which mainly included Defense, Deterring and Development, three major strategic goals, hoping to achieve the protection of government networks and critical infrastructure, and to curb cybercrime and develop cyber security-related scientific research. The Ministry of Internal Affairs disclosed the implementation of the strategy in May 2019. The effects included improving understanding of cyber security

threats, reducing threats of cyber attacks, and providing integrated resources of advice and support. In addition, through the Active Cyber Programme, it successfully blocked 4.5 million malicious e-mails each month and resisted more than 140,000 malicious phishing websites.

Although the United Kingdom left the European Union officially at the end of January 2020, it is still expected to be consistent with European Union regulations in terms of cyber security or data protection. For example, in 2018, the United Kingdom has amended the Data Protection Act 2018. The definition of personal data was similar to the "General Data Protection Regulation (GDPR)". It adopted the regulation such as the consent of the parties, the right of access, the right to be forgotten, the right to data portability, and the establishment of a data protection commissioner. In addition, the United Kingdom also announced the "Digital Strategy" in March 2017, including building a world-class digital infrastructure, making the United Kingdom the most suitable country for the entrepreneurship and development of digital companies in the world, helping each British company become digital, becoming the safest cyber country in the world, being a world-class leader that provides citizens with the best online services, leveraging the economic power of data, and improving citizens' confidence in data usage. From these relevant measures, it can be seen that the UK hopes not to lose its influence in the era of data economy due to Brexit.

(E) Japan

The competent authorities of cybersecurity in Japan are the Cybersecurity Strategic Headquarters and the National Center of Incident

readiness and Strategy for Cybersecurity (NISC). The Japanese government passed the Cybersecurity Basic Act in 2014. The purpose is to strengthen the coordination between the Japanese government and the private sector in the field of cybersecurity. It was revised in December 2018 with two major additions. One is the establishment of a new "Cyber Security Committee", whose main members include the heads of state administrative agencies, local governments, critical infrastructure operators, and other private professionals, who are responsible for promoting the agreement on cybersecurity-related policies; the second is to expand the business managed by the Cyber Security Strategy Headquarters so that when a cybersecurity incident occurs, they can immediately contact domestic and foreign stakeholders.

The latest cyber security strategies (three-year period) announced in July 2018 boasted three goals: "enhancing economic and social vitality and sustainable development", "realizing a safe and secure society for the citizen" and "ensuring the peace and security of the international community, and the safety of Japan". There were also four strategies: (1) Establishing an information and communication security supply chain; and constructing a safe IoT system, (2) Constructing a university teaching and research environment, (3) Formulating cybercrime countermeasures, and (4) Strengthening cyber defense of government agencies; suppressing cyber attack capabilities; and increasing security response capabilities to large-scale attacks.

In addition, considering the limitation of talents and resource of small and medium-sized enterprises and the local region, that a company cannot be immune to cyber attacks entirely, the Japanese government supports SMEs in

advance by dispatching Registered Information Security Specialist (RISS) to assist enterprises in cyber security management and processing. After the cyber security incident, a cyber security rescue team will be set up to provide relevant assistance to SMEs. As for the local communities, they will cooperate with high-level professional institutions, academia, and the government. That is, they will promote local talent training and launch cooperation platforms to collaborate with cyber security experts and trainees of the Industrial Cyber Security Center.

(F) Korea

The major cyber security competent agency of South Korea is the Office of National Security, while the National Intelligence Service (NIS) is in charge of the cyber security business of the state and public agencies; and the Ministry of Science and ICT responsible for private information and communication infrastructure protection and the business of major information and communication infrastructure.

The overall cyber security policy in South Korea is based on the "National Intelligence Service Act", "Information and Communication Fundamental Protection Act", "Electronic Government Act", "National Informatization Basic Law" and other related laws and regulations. These laws are responsible for the overall national cyber security business plan; the establishment and implementation of amendment plans and security policies; and the management of the cyber security business of the state and public agencies. It also combines with relevant laws and regulations and cooperates with various ministries to promote cyber security business. For example, the

Korea Cyber Security Industry Promotion Law was amended in February 2018 and implemented in May of the same year. The industry promotion law was established as the foundation for the cyber security industry to increase competitiveness. Policy goals were set for the needs of the revitalization of cyber security industry, improving the safety of the information and communication environment and the national economy. In Article 3 of the law, it further required the national and local governments to implement the necessary policies and establish a financial assurance plan in order to revitalize the information security industry. In addition, in accordance with Article 14 of the law, the Minister of Ministry of Science and ICT can promote the development and investment in cyber security technology of related businesses.

There were 6 goals in the latest national cyber security strategy announced in April 2019, including strengthening the security of the country's core infrastructure, improving the ability to respond to cyber attacks, establishing a trusted and managed network governance, laying a foundation for the infrastructure of cyber security industry, cultivating a culture of cyber security, and leading international cyber security cooperation.

Taking the aforementioned second goal as an example, in order to enhance South Korea’s ability to respond to cyber attacks, to ensure the prevention of cyber attacks, and to increase the readiness to defend large-scale cyber attacks, comprehensive and effective countermeasures were formulated to strengthen the response capabilities to cybercrime. Relevant measures were established, such as: concentrating the energy of the state (ministries) to fight

against national-level cyber attacks; extensively researching threats or weaknesses information, and conducting analysis to enhance the response capabilities, etc.

(G) Singapore

The competent authority for cyber security in Singapore is the Cyber Security Agency (CSA). For the overall cyber security policy, Singapore announced the "Cyber Security Strategy" in 2016. The main contents include (1) Strengthening the resilience of critical information infrastructure; (2) Creating safer cyberspace for companies and communities to face cyber threats, combat cybercrimes, and protect personal data; (3) Developing a Cyber Security Ecosystem, including skilled labor, advanced technologies and strong research capabilities of companies; (4) Strengthening international cooperation due to cross-border cyber attacks.

At present, the latest 5-year advancement plan of cyber security is “Infocomm Security Masterplan (ISMP)”. On the basis of the previous two phases of the plan, Singapore’s cyber security is strengthend through Critical Infocomm Infrastructure, the government, and the efforts of enterprises and individuals, including 3 key points: (1) Strengthening of safety and recovery capabilities of critical cyber communication infrastructure to cope with highly developed cyber attacks. (2) Enhancement of the adoption of security measures for cyber communication by enterprises and individuals. (3) Development of Pool of Infocomm Security Experts.

In addition, in order to develop the digital economy, Singapore has especially strengthened its security protection work in the

telecommunications sector to respond to threats to security at home and abroad. Since 2018, the Infocom media development authority (IMDA) has prepared and established the Telecom Cybersecurity Strategic Committee (TCSC) to improve the country's ability to respond to cyber security threats and to enhance Singapore's ability to deal with critical information and communications infrastructure issues. After the establishment of the Telecom Security Strategy Committee, it will mainly establish partnerships with the telecom industry (including global cybersecurity experts and major telecom operators) to strengthen the protection of telecom infrastructure and establish the network security capabilities of Singapore telecom operators.

(H) Australia

The Australian Cyber Security Authority is the Australian Signals Directorate (ASD) under the Ministry of Defense. In the field of cyber communication and security, Australia places more emphasis on the link between information sharing and crime prevention and assists related businesses through military organizations. The bureau mainly assists in maintaining the security of cyber communication in Australia through three major projects: (1) Informing: obtaining undisclosed international information through related mechanisms and performing notification or information sharing. (2) Protecting: through the grasp of possible threats, proactively provide suggestions or assistance to improve the risk management of the government, enterprises, or communities facing cyber threats. (3) Disrupting: through the application of technology or active defense technology, destroying possible attacks, combating terrorism, cyber espionage,

and serious cyber crimes.

The Australian Department of Justice has provided a Protective Security Policy Framework (PSPF) since 2010, including 5 principles, 4 security aspects (Outcomes), and 16 Core Requirements; among them, the security aspects are mainly Governance, Information, Personnel, and Physical environment recommendations, combined with corresponding core requirements and standardized methods to facilitate implementation.

At present, the latest 4-year plan for the Australian cyber security policy is the “Cyber Security Strategy in 2020”, announced in August 2020 and was expected to invest 1.67 billion Australian dollars in 10 years. The investments are as follows: (1) The government will take action to strengthen the protection of Australian people, businesses, and critical infrastructures from multiple threats. (2) The company will take action to protect its products, services, and customers from intrusions through known network vulnerabilities. (3) Actions taken by the community to raise the public's safety awareness of online transactions to ensure consumers can shop with peace of mind. Cyber communication security will be promoted through the joint efforts of the government, the private sector, and the community.

(I) Israel

From July 1, 2018, the Israeli government’s cyber security authority will be the National Cyber Directorate (INCD) officially. The country mainly builds cyber security protection through the cooperation of the military, government, and the public. Usually, through INCD, cyber security is implemented to assist the public and private sectors; when a cyber security

incident occurs, the National Information Security Incident Preparation Team (CERT-IL) under the committee will assist in the implementation of information sharing and loophole repairs, etc.; when a national-level incident occurs, the competent authority and intelligence units will carry out the intrusion source tracing and incident response, and also cooperate with domestic and foreign intelligence agencies, such as trying to target the attacker, in order to respond to the possible influence or threat.

Israel's cyber security or information and communication security is divided by ministries and committees and included in the annual administrative work of its affiliated agencies. In addition to INCD, the Ministry of Public Security is also responsible for cybercrime. In 2016, the Ministry included combating cybercrime and preventing social media bullying as targets for the year; it also strengthened the investigation of emerging criminal modes of child pornography, data theft and viruses. In the 2019 annual report (Ministry Overview-2019), it continued to attend to cybercrimes, cyber security threats, and terrorist attacks; cooperated with INCD and other agencies to protect CI or other information and communication systems from external threats or attacks.

In 2018, Israel has drafted the "Cybersecurity Laws and Regulations". The specifications include expanding the capabilities of INCD; in addition to directly reporting to the prime minister, assisting in the assessment of national cyber risks, planning for national reorganization and recovery capabilities, etc., to identify, prevent and mitigate hostile behavior and other considerations, the bill authorizes the committee to directly, or under the authorization of the

court, access private sector documents and computer data and obtain equipment for inspection. However, due to excessive disputes in some projects, relevant procedures have not yet been completed.

In addition, it is worth noting that the Israeli government strongly encourages the development of the cyber security industry. For example, the Israel Innovation Authority (IIA) has either established incubators or platforms to facilitate domestic companies to develop a global market, or encouraged domestic manufacturers to participate in international forums, assisted in seeking partners or promoting matchmaking, and subsidized investment plans for companies with the potential of development.

III. The Current State of Promotion of Cyber Security in Taiwan

A. Organizational Structure

National Information & Communication Security Taskforce (NICST) was established in January 2001 and is responsible for the national cyber security policy, notification response mechanism, consultation and review of major plans, and coordination and supervision of cross-sector cyber security affairs. In order to implement the strategy, "Cyber Security is National Security", an important strategy to improve the leading level of cyber security, the Executive Yuan established a special unit dedicated to cyber security affairs on August 1, 2016, the Department of Cyber Security (hereinafter referred to as the DCS) to replace the original task force, the Cyber Security Office. In addition to serving as the staff unit of NICST, it also develops fundamental national cyber security guidelines, policies, and major plans, and formulates related laws and regulations.

There are currently two systems under NICST including cyber protection and cyber crime investigation. Based on the "Guidelines for the Establishment of the National Information & Communication Security Taskforce" revised on December 25, the organizational chart of NICST is shown in Figure 2

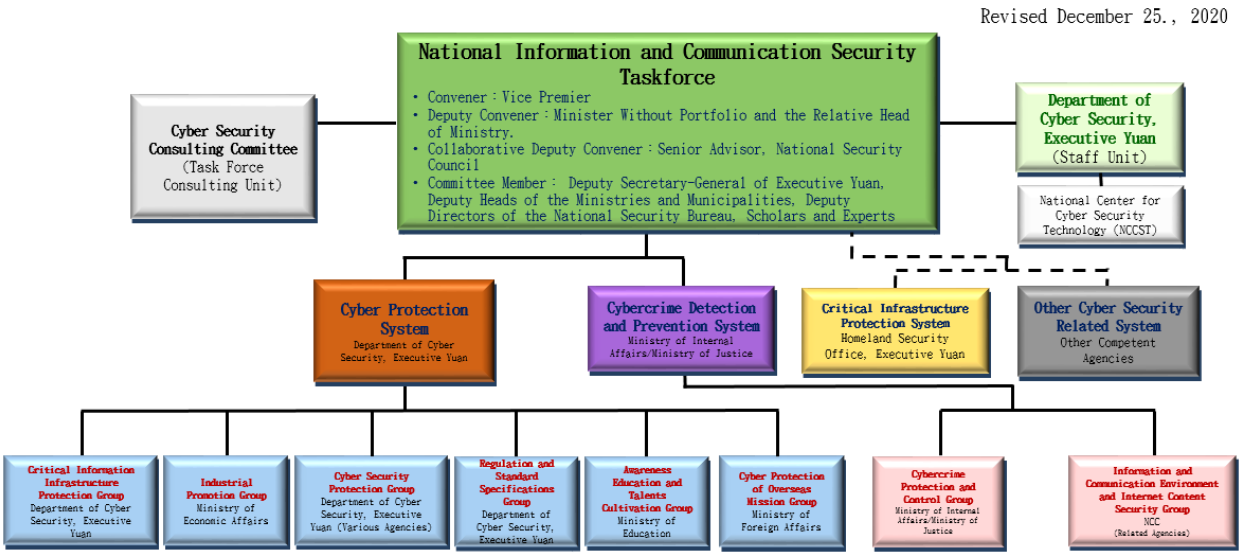

Figure2: NICST Organizational Chart

(A) Cyber Protection System: sponsored by the DCS of Executive Yuan, the system is responsible for integrating cyber security protection resources and promoting cyber security-related policies. The competent authorities (units) and tasks are as follows:

1. Critical Information Infrastructure Protection Group: sponsored by the DCS of the Executive Yuan, responsible for planning and promoting the security management mechanism of critical information infrastructure; supervising the implementation of security protection in various fields; and conducting audits, drills, and related operations.
2. Industrial Promotion Group: structured by the Ministry of Economic Affairs, responsible for promoting the development of the cyber security industry, integrating production, government, academic, and research resources, and developing related innovative applications.
3. Cyber Security Protection Group: structured by the DCS of the Executive Yuan, the team is responsible for planning and promoting the security

mechanism of various information and communication application services of the government, providing cyber security technical services, supervising government agencies in implementing cyber security protection and reporting responses, handling cyber security audits and cyber attack and defense drills, and assisting various agencies to strengthen the integrity and effectiveness of cyber security protection.

4. Regulation and Standard Specifications Group: structured by the DCS of the Executive Yuan, is responsible for the research and formulation (revision) of cyber security-related laws and regulations; the development of cyber security-related national standards; and the formulation and maintenance of government agencies' cyber security practices and reference guides.
5. Awareness Education and Talents Cultivation Group: structured by the Ministry of Education, responsible for promoting fundamental cyber security education, strengthening the cyber security of the education system, improving the quality of cyber security of the whole people, providing cyber security information services, building a fully functional integrated platform, handling international-level cyber security competition, promoting industry-university exchanges, and reinforcing the cultivation of cyber security talents.
6. Cyber Protection of Overseas Mission Group: Sponsored by the Ministry of Foreign Affairs, it is responsible for integrating the information and cyber management of the foregn agencies and representative offices to enhance their cyber security protection capabilities and reduce the risk of

hacking and cyber security incidents.

(B) Cybercrime Detection and Prevention System: co-sponsored by the Ministry of the Interior and the Ministry of Legal Affairs, is responsible for preventing cybercrime, maintaining public privacy, promoting the information and communication environment and cyber content security, etc., and establishing the following groups. Their sponsoring agencies and tasks are as follows:

1. Cybercrime Protection and Control Group: co-sponsored by the Ministry of the Interior and the Ministry of Justice, responsible for cybercrime investigation, computer crime prevention, digital forensics, and review of laws and regulations related to cybercrime prevention.
2. Information and Communication Environment and Internet Content Security Group: sponsored by the National Communications Commission, responsible for promoting the information and communication environment and cyber content security and assisting in the prevention and control of cybercrimes.

The National Center for Cyber Security Technology (NCCST) was established in March 2001. It serves as a think tank and staff unit of the government's cyber security technology, assisting the NICST to gradually establish a cyber security protection mechanism; provides before incident security protections, during incident early warning and responses, and post incident recoveries and forensics and related cyber security technological services for various government agencies. Through these methods, it assists the

government agencies and core industries to strengthen cyber security protection capabilities and reinforce cyber security information sharing and united defense to reduce the risks of cyber security.

In addition to the promotion of private cyber security, the "Taiwan Network Information Center (TWNIC)" under the jurisdiction of the National Communications Commission is responsible for the maintenance and operation of the "Taiwan Computer Emergency Response Team/Coordination Center, TWCERT/CC". The team led to promote the notification of private cyber security incidents, the provision of cyber security teaching resources, the organization of cyber security advocacy activities, and assisted private units to establish an internal CERT/CSIRT mechanism in the industry to implement cyber security incident notification, and strengthen the coordination and cooperation of domestic information reinforcing the collaboration of domestic cyber security response organizations to shorten the timeliness of processing cyber security incidents.

B. Phases of Promotion

Since 2001, NCCST has successively promoted 5 phases of major cyber security plans or programs, each with a 4-year period, which has effectively improved the completeness of our country's cyber security. The key points of each phase of the plans or programs are shown in Figure 3.

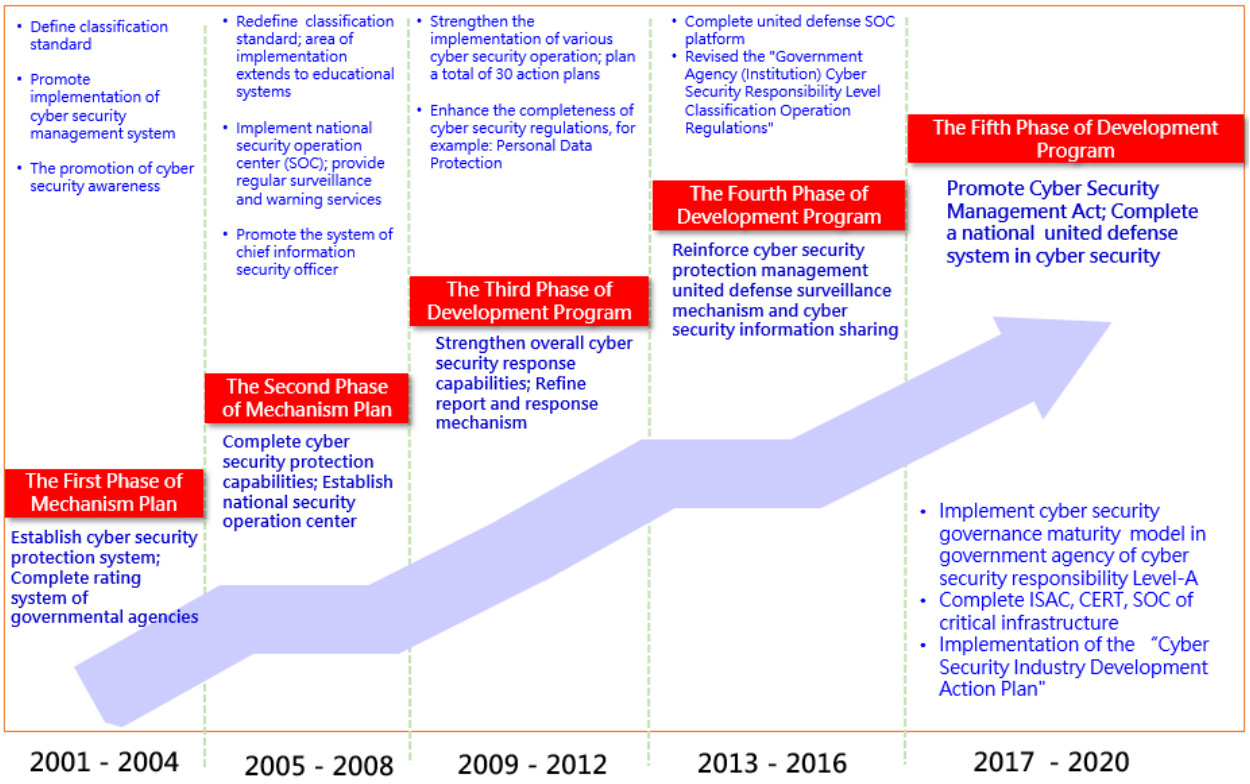

Figure 3: The promotional phases of cyber security in our country

(A)The First Phase of Mechanism Plan (2001-2004)

Establish a Cyber Security Protection System; Complete Rating Mechanism for Government Agencies

The Executive Yuan promulgated the "Mechanism Program of Security in Establishing National Information and Communication Infrastructure" (abbreviated as the Phase 1 mechanism program) on January 17, 2001, with the vision of "ensuring a national safe and reliable information and communication environment". The main achievement of this phase lies in the construction of a cyber security protection system. The achievements include:

1. Establish the NICST, together with NCCST, a technical staff unit, as the competent authority of national cyber security construction and policies.
2. Promote the cyber security management system for important government agencies involved in the livelihood and economy of the country; provide

corresponding cyber security support and work requirements for agencies with different responsibility levels through the establishment of cyber security crisis notification and early warning mechanisms for the agencies and responsibility level classification standards; conduct external cyber security audits against designated agencies.

3. Promote cyber security training for information personnel; strengthen cyber security manpower training and concept promotion; enhance public awareness of cyber security, etc.
4. Review and revise relevant laws and regulations on cyber security; formulate technical standards and specifications for cyber communication security; establish product inspection and guarantee mechanism.
5. For the important operating system of CI, plan and promote the establishment of Information Security Management System (ISMS), as well as cyber security control programs such as the early warning, notification mechanism, and personnel training of the security operation center.

(B) The Second Phase of Mechanism Plan (2005-2008)

Improve the Capabilities of Cyber Security Protection; Establish a National Security Operation Center

Based on the first phase of the mechanism plan, the Executive Yuan approved the “Mechanism Program of Security in Establishing National Information and Communication Infrastructure (2005 to 2008)" (abbreviated as Phase 2 mechanism program) in 2004; continued to strengthen national protection basis for cyber security overall. The important results include:

1. Establish a National Security Operation Center (N-SOC) to provide monitoring and early warning services for important core government agencies and provide 24-hour protection.
2. Establish the Chief Information Security Officer (CISO) mechanism for government agencies and designate the deputy head of the ministries in charge of cyber security operation as the CISO concurrently; promote the implementation of cyber security-related plans in the implementation unit.
3. Expand the scope of implementation of grading operations of cyber security responsibility levels of the government agencies; greatly increase the number of cyber security systems include in important government agencies and extend the scope of implementation to the education system.
4. Promote the introduction of ISMS into the education system, and guide county (city) education network centers to establish ISMS.
5. Enhance the effectiveness of operations through audits. Various agencies have introduced internal audit systems to implement cyber security-related promotion work and continue to conduct external cyber security audits for public and private organizations and provide auditing recommendations.
6. Extend the field of protection of the cyber security plan; strengthen the formulation of cyber security plans that promote online transaction security and protect people's personal data.

(C)The Third Phase of Development Plan (2009-2012)

Strengthen the Overall Response Capability of Cyber Security; Improve the Report and Response Mechanism

The Executive Yuan issued the "National information and

communication security development program (2009 to 2012)" (abbreviated as Phase 3 development program) in January 2009. With the vision of building "a safe and reliable smart nation; a secure and qualified digital life", we conduct the experience of cyber security promotion to the private sector and gradually strengthen their cyber security defense mechanism. The main results are as follows:

1. Establish response procedures for cyber security incident detection, identification, analysis, and response, improve notification timeliness, and continue to strengthen emergency notification, response, and recovery capabilities.
2. Promote the introduction of cyber security governance and performance evaluation in government A-level and B-level agencies, require agencies to allocate specific information security responsibilities and concurrent manpower according to their needs, and establish classification and classification of information systems and corresponding basic information security protection needs.
3. Adopt the "plan-do-check-act" (PDCA) planning model to improve the information security management level of government agencies, reduce related operational risks, and facilitate domestic government agencies and private enterprises to pass international security standards verification (such as ISO 27001).
4. Intensify the reliability and security of e-commerce, strengthen the identity authentication mechanism for online transactions, and promote the use of Public Key Infrastructure (PKI) certificate services.

5. Promote the use of third-party appraisal by business institutions, strengthen the cyber security inspection of business of various purposes in accordance with the authorization of laws and regulations, urge the industry to strengthen personal data protection, establish a cyber security management system, conduct internal audits and entrust a third party to conduct external cyber security audits.
6. Strengthen the research energy of cyber security research, encourage higher education systems to offer cyber security courses, cultivate cyber security professional research talents, develop key cyber security technologies, and transfer to provide value-added applications in the industry.
7. Advocate and strengthen the concept of cyber security, promote cyber security awareness activities for schools at all levels, inspect the security of cyber assets, conduct public security inspections and competitions and other activities, and enhance national cyber security awareness.

(D)The Fourth Phase of Development Plan (2013-2016)

Strengthen the United Defense Monitoring Mechanism for Cyber Security Protection Management; Intensify Cyber Security Intelligence Sharing

The Executive Yuan approved the “National information and communication security development program (2013 to 2016)” (abbreviated as Phase 4 development program) in 2013, with the vision: "building a safe cyber security environment; stepping towards a high-quality cyber society", to strengthen the counterreaction capabilities of the central government against cyber attacks. The four major goals are as follows:

1. National policies and environmental construction: continue to increase and revise information security policies, norms, guidelines, standards, and manuals, take stock of my country's information security laws and regulations, discuss and formulate information security laws; promote reasonable manpower and budget mechanisms for information security in various government agencies, Handle the evaluation of information security service vendors every year; handle the preparation and operation of the "National Center for Cyber Security Technology", promote administrative legalization; promote the security verification of information and communication equipment, actively communicate with international certification and certification organizations, and regularly review and review the establishment project
2. Cyber security protection and information sharing: promote the establishment of a governmental cyber security governance structure, assessing the maturity of cyber security governance of government agencies of A, B, C level; establish an iWIN network content protection agency to strengthen the mechanism of network content security management; implement cyber security offensive and defensive drills, and develop situational drills and actual drills of cyber security; promote governmental cyber security management systems, and improve operations of governmental cyber security management; develop the security settings of cyber security infrastructure, and continuously construct Government Configuration Baseline (GCB) for different systems; increase the capabilities of collection of intelligence of cyber security threats, and

strengthen information analysis and sharing mechanism.

3. Industrial development and technological upgrade: construct the research capacity of cyber security protection technology and strengthen the competitive advantage of emerging cyber security independent technologies; intensify the cooperation of cyber security technology research and development between enterprises and academic institutions, and carry out the application of emerging technological practices of cyber security; strengthen the applications of crime investigation, improve digital evidence preservation, and promote digital forensic laboratories to grasp the tendencies of cybercrime in real time; base on current key technologies, such as mobile devices, mobile applications, wireless networks, and Secure Software Development Lifecycle (SSDLC), etc., to build a corresponding security detection mechanism.
4. Talent cultivation and international exchanges: promote cyber security professional training and certification mechanism, and plan to establish the registration and certification mechanism of cyber security professionals; establish the evaluation system for cyber security functional capabilities and encourage various categories of personnel to complete cyber security function training regularly and pass courses evaluation.

(E)The Fifth Phase of Development Plan (2017-2020)

Promote the Cyber Security Management Act; Complete National Cyber Security United Defense System

The Executive Yuan approved the “National Cyber Security Program of Taiwan (2017-2020)" (abbreviated as Phase 5 program) in 2017. In order to

respond to the threats and challenges of information and communication security as the government promotes the development of a digital nation and innovative economies, we upgrade cyber security to the level of national security protection under the policy direction of "Cyber Security is National Security". Meanwhile, we continue to promote the improvement and implementation of various cyber security protection measures, facing complex and changing cyber security threats.

The vision of the fifth phase is "building a safe and reliable digital country". There are three major goals: "Building a National Cyber Security United Defense System", "Improving the Overall Cyber Security Protection Mechanism", and "Strengthening the Development of Independent Cyber Security Industries". There are also four major promotional strategies, including "Completing Cyber Security Infrastructure", "Building a National Cyber Security United Defense System", "Promoting the Independence of the Cyber Security Industry" and "Nurturing High-Quality Cyber Security Talents"; 11 specific measures have been formulated to gradually promote national cyber security defense-in-depth and united defense system, to stabilize the security defense line of national digital territory. The current priorities of implementation and results of promotion are as follows:

1. Complete cyber security infrastructure

(1) On May 11, 2018, the Legislative Yuan passed the third reading of the Cyber Security Management Act. The Presidential Decree was issued on June 6; and the enforcement decree was issued on December 5, establishing the basis for the legalization of cyber security in our country.

The Act was officially implemented on January 1st, 2019 with the six sub-regulations also implemented simultaneously to implement various cyber security operations.

(2) In order to establish the cyber security protection standards of information and communication products in our country, the Ministry of Economic Affairs and the National Communications Commission jointly promote security testing, certification, and verification for information and communication products, including the establishment of products testing standards, testing laboratory certification, cyber security testing service, cyber security verification of the product, and issuance and announcement of certification marks, etc.; and prioritize products with market scale and greater impact on livelihoods as the targets of promotion. At present, IoT cyber security standards such as video surveillance (IP CAM, NVR, DVR), smart buses (vehicles and smart stop signs), and smart streetlights (light controllers and lighting gateways) have been formulated, of which the cyber security industrial standard of IP CAM has become a national standard (CNS 16120).

2. **Construct national cyber security united defense system**

(1) The cyber security united defense system of our country is based on the core of eight major CI sectors. Coordinated by the Executive Yuan, it combined with the central competent authority in charge of business purpose, to connects to CI providers to provide cyber security protection; and connect with the national level to conduct horizontal cross-domain united defense, forming a "Three-layered Cyber Security United

Defense Architecture" to mitigate the impact of CI operation disconnection due to cyber security attacks, thereby strengthening overall national security. Currently, we have promoted the establishment of Security Operation Center (SOC) of domestic-level and various CI-sector-level, Computer Emergency Response Team (CERT), Information Sharing and Analysis Center (ISAC) and other united defense mechanisms. By these systematic and institutionalized deployments, we conduct cyber security information collection and sharing; incident report and response; integration, sharing and application of intelligence, and establish a complete defense line.

(2) Regarding the local government: by strengthening the cyber security protection of the local government and its affiliated local offices, we assist them in constructing a safe information and communication operating environment and establishing a reliable cyber security environment. Also, from the six special municipalities, we combine neighboring counties to promote cyber security regional united defense; establish a local united cyber security protection network; and drive the local government to cooperate with nearby academic research institutions to jointly cultivate future cyber security talents for the government and academia. At present, 6 regional ISACs have been established and become members of the National Information Sharing and Analysis Center (N-ISAC), so that information can be quickly shared with local governments. SOCs of 6 regions have also been completed to collect the information of cyber security of neighboring

counties and cities and conduct a comprehensive analysis to grasp suspicious malicious behavior.

3. Boost the independence of the cyber security industry

(1) In order to promote the independent development of the national cyber security industry, and to increase the domestic autonomy rate, the Executive Yuan promulgated the "Procuring Principles for Information and Communication Security Independent Products" on November 28, 2019, encouraging central and local agencies (institutions), public schools, government-owned enterprises, and administrative legal persons to adopt independent products of cyber security. in accordance with the Public Procurement Laws and Regulations, thereby driving the development of cyber security industry and strengthening security protection capacity for national cyber security. In addition, to assist cyber security vendors to enhance their mid-to-long-term competitiveness, the Ministry of Economic Affairs has established an integrated cyber security service platform (SecPaaS) and promoted the matching services of domestic cyber security products and services. The suppliers are the manufacturers that can provide cyber security services, such as security software development tool vendors, penetration testing service providers, and emerging cyber security product providers. Their products and services will hit the store shelves after they have passed the examination. The demand side is the field representative or product integrators, such as a system integration service provider and a solution provider. Through assisting the demand side of introducing cyber

security product trials and demonstrations, we hope to build and promote cyber security solutions in the vertically integrated field.

(2) In order to accelerate the development of cyber security industry, the government has invested resources to create favorable conditions and development environment for the cyber security industry players in Taiwan, so that the participants can quickly accumulate various capabilities and have room for growth in the early stages of development. We will also combine with the cyber security startup community; organize technical gatherings and workshops; establish an environment for cyber security trends and technology exchanges among the industry, academia, and research circles; concatenating domestic cyber security R&D power so that cyber security technology will take root; and at the same time support startups to a total of 25 companies, such as the industrialization of the white hat hacker community, or driving the investment by large enterprises.

4. Cultivating high-quality cyber security talents

(1) In 2018, the Ministry of Education added an electronic-information discipline cluster, setting up an “Information and Communication Security Discipline", to the original public-funded studying abroad examinations to provide admitted students with the opportunity to study abroad. In addition, since 2019, it promoted the establishment of 5 cyber security master programs in 4 colleges and universities, and gradually established a systematic cyber security talent cultivation system. In addition, we have implemented a diversified practice training model.

Since 2016, we have promoted the training course of "Taiwan Cool Hacker". With the goal of cultivating talents with cyber security technical and practical skills, we invited teachers from the academy and industry and promote the Mentor system, instructing cyber security practices and technology and the experience of cyber security competition through apprenticeship. In addition, students with outstanding performance in cyber security skills are given opportunities for more specialized and advanced studies. In 2017, we launched a new type of cyber security summer school program (Advanced Information Security Summer School, AIS3). With the goal of cultivating high-level cyber security talents, we also hosted Final CTF or special contest of cyber security practical application. Through the diversified practical training model, in recent years, the cyber security students of our country have been ranked among the best, while attending contests abroad like the DEF CON CTF and other international cyber security competitions.

(2) Aiming at the cultivation of talents in the cyber security industry, the Ministry of Economic Affairs has started the cyber security industry talent development class since 2017, subsidizing 400 hours of full-time cyber security training for each trainee while the training unit will provide employment matching services after the completion of the course. There was 100% matchmaking within 3 months after the 2017 training; the matchmaking for 2018 was also up to 80%, and 20% of the successfully paired went directly into cyber security industry. Regarding

the development of cyber security talents, we use various cyber security training models in the market to set up on-the-job classes for short-term cyber security training in different industrial fields. The Industrial Bureau provides subsidies to the enterprise-appointed trainees, immediately strengthen the level of cyber security in the industry. In 2010, there were a total of 11 short-term cyber security classes, training 220 people; a total of 6 CI cyber security classes, training 133 people; a total of 3 long-term cyber security classes, training 69 people. Aiming at the development of high-level cyber security talents, the TWISC Center Alliance has set up 7 TWISC Cyber Security Specialty Centers, cultivating a total of 792 master and doctoral students of cyber security program. By the third quarter of 2010, 289 journals and seminar papers have been published; 96 pieces of industry-university cooperation have been implemented, and 15 cyber security technologies have been transferred.

C. Cyber Security Development Issues Analysis and Response Strategies

In response to Taiwan's special political and economic situation and global cyber security threats, it is urgent and necessary to continuously promote and implement the overall national cyber security protection to respond to external challenges. Based on the results of the fifth phase of the development plan and the aforementioned global cyber security threats and international policy trends, we conduct an in-depth SWOT (Strength Weakness Opportunity Threat) analysis of the advantages and disadvantages of our internal environment and the opportunities and threats from the external environment, as shown in Figure 4 below, as a key reference for this program.

Advantages	Disadvantages
1. Cyber security is among our focused policies and has been promoted proactively. 2. The execution of Cyber Security Management Act and the sub-laws; the formulation of industry standards and testing specifications; the complete legal foundations and related coordinating systems. 3. The advantage of Taiwan's ICT industry supply chain; the exported advantage of industrial computer products. 4. There are bountiful high-quality information-related talents and high-level hackers in Taiwan.	1. The regulations of cyber security are not comprehensive enough; the cyber security awareness of both enterprises and citizens still needs to be improved. 2. The overall national cyber security united defense mechanism is not comprehensive. 3. The domestic cyber security industry is relatively small in scale, with insufficient output value. 4. Lack of cyber security talents with the experience of prospective research, actual practice, and critical infrastructure.
Opportunities	**Threats**
1. Taiwan boasts the most crucial cyber security strategic position in the world. 2. There has been energy for cybercrime investigation and cyber security protection	1. Taiwan's special-political economic status, facing national-level organizational hacker's attacks. 2. Innovations of emerging cyber security;

mechanisms in Taiwan, enhancing the resolution of international cooperation. 3. Gradual centralization of the government information and communication environment, beneficial for cyber security protection reinforcement. 4. Increasing demand for cyber security protection of 5G, IoT, AI, and other industrial innovation.	lack of proactive defense mechanisms. 3. Increasing cyber security threats of critical infrastructure and supply chains; lack of public-private partnership collaboration mechanism. 4. Our cyber security vendors face tremendous pressure of competition from worldly known manufacturers.

Figure 4: Current Cyber Security Development- SWOT Analysis

Afterward, we adapt TOWS matrix to conduct strategic analysis on the aforementioned SWOT, using strengths, weaknesses, and opportunities to formulate offensive strategies and transition strategies; then based on strengths, weaknesses, and threats to formulate avoidance strategies and hedging strategies, as shown in Figure 5 below. Furthermore, based on the four promotional strategies of the fifth phase of the development plan: (1) completion of the cyber security basic environment; (2) the construction of a national security united defense system; (3) the promotion of the independent energy of the cyber security industry; and (4) the cultivation of high-quality cyber security elite talents, we may analyze that in the aspects of cultivation of elite talents, and the united defense of national cyber security, we should expand higher education cyber security instructors and invest in cyber security science research, as well as strengthen proactive defense energy and detection technology and other measures. In terms of governance of the basic environment and industrial protection energy, it is necessary to strengthen the public-private partnership collaborative governance mechanism and the supply chain security, and guide enterprises to intensify the cyber security protection energy during digital

transformation. Finally, the various analysis results are summarized. After research and analysis, we present the solutions of this development blueprint.

SO MAXI-MAXI Strategies	WO MINI-MAXI Strategies
1. Build a safe environment for a smart country (S1+S2+S3+O4) 2. Enhance scientific and technological detection capability to prevent new types of cybercrime (S1+S4+O2) 3. Take the initiative to block the attack on the border (S1+O2+O3)	1. Continue to promote centralized sharing of governmental information (security) (W2+O3) 2. Expand international engagement and deepen international intelligence sharing (W2+O2) 3. Expand the quota of cyber security educators and teaching resources in higher education (W4+O1+O4) 4. Shift resources to high-level cyber security scientific research (W4+O1+O2+O4)
ST MAXI-MINI Strategies	**WT MINI-MINI Strategies**
1. Strengthen supply chain security management (S2+S3+S4+T3) 2. Establish public-private partnership collaborative governance operation mechanism in every CI sector (S2+S4+T3) 3. Deepen public-private partnership cooperation; information intelligence sharing and response practices in normal times (S2+S4+T2+T3)	1. Guide enterprises to intensify cyber security protection power during digital transformation(W1+W2+T1) 2. Cultivate top practical and cross-regional cyber security talents (W4+T1+T2) 3. Strengthen the critical infrastructure personnel's cyber security awareness and construction ability (W1+T2+T3)

Figure 5: TOWS Analysis Matrix

IV Development Blueprint

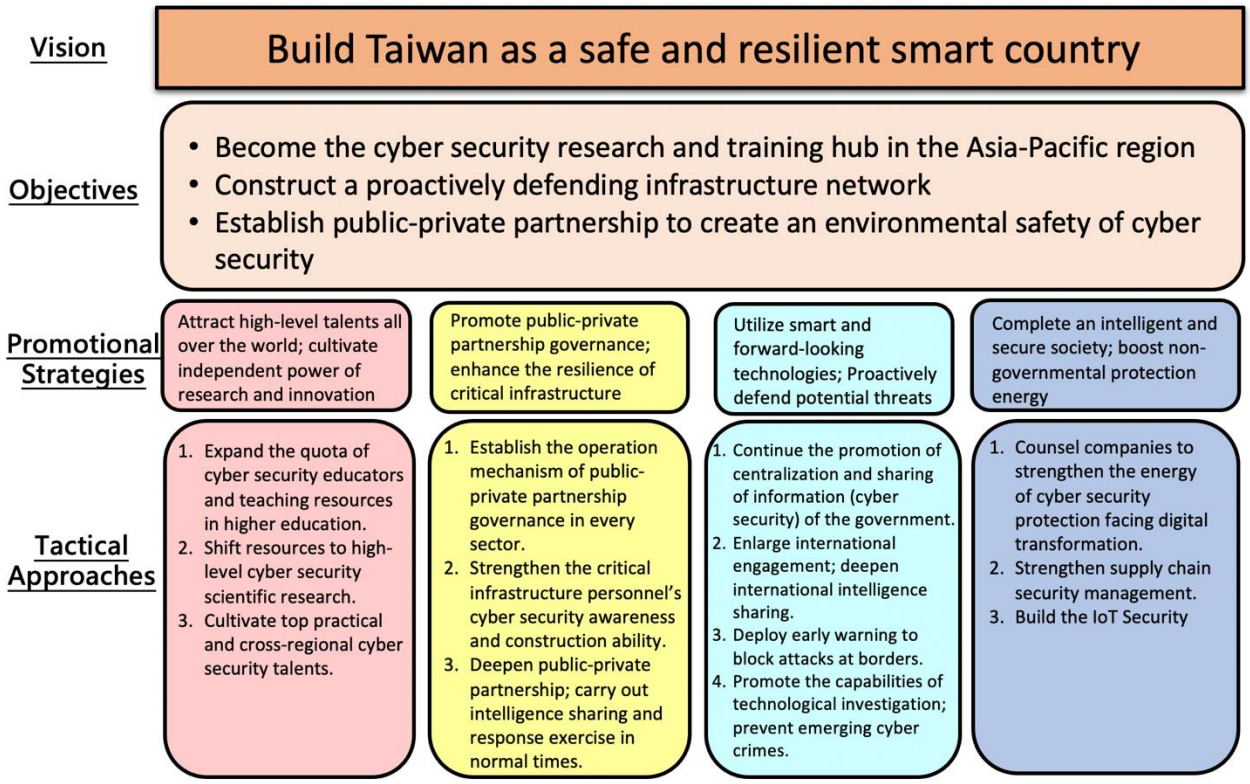

Figure 6: The sixth phase of the national cyber security program

A. Vision

Our national cyber security policy has undergone systematic development in the first five stages, and gradually achieved the scheduled milestones to effectively reinforce the readiness of national cyber security. The objectives are as follows: "the establishment of a safe environment of cyber security; the completion of cyber security protection management; sharing of multiple cyber security information; the expansion of the cultivation of cyber security talents; and the reinforcement of international cyber security exchanges."

To accelerate Taiwan’s industrial transformation and upgrade, the government has created a new economic model that pursues sustainable development with "innovation, output value, employment" as the core values, while stimulating industrial innovation through the three strategies of "connecting the future, connecting the world, and connecting local". In order to achieve the above goals, the "5+2 Innovative Industries Plan " was promoted in 2016 as the core to drive the growth of Taiwan’s industries of next generation, while the "Digital Nation and Innovative Economic Development Program (2017-2025)" (DIGI^{+} program) has been promoted since 2017. With the vision of "developing an active Internet society; promoting a high-value innovative economy; and expanding a prosperous digital land" as policy blueprints to achieve digital development and innovation, we aim to accelerate the integration of AI, IoT, Big Data and other smart technologies into our industries and daily life.

In order to develop an active network society, promote a high-value innovative economy, and build a rich digital country, this program will serve as a solid cornerstone of the aforementioned two major digital economic plans at this stage; and will be combined with the promotional strategies formulated by the prominent cyber security industry development plan, one of the six core strategic industries; and greatly strengthen the pulse of the various digital economy in stable information and communication security environment. With the vision of "build Taiwan as a safe and resilient smart country", we hope to create a safe and reliable society with smart life.

B. Objectives

With the development of emerging technologies and the popularization of IoT devices, as well as the advent of the 5G era, the threat of information and communication is increasing. Our government is also facing more severe challenges due to its special political and economic situation. In order to maintain our energy and advantages of cyber security protection, and to actively cultivate sufficient cyber security talents as the primary goal, the first objective of this program is to “become the cyber security research and training hub in the Asia-Pacific region”. We will establish Cyber Security Center of Excellence. Starting from the five aspects of cyber security: that is, forward-looking cyber security research, the development of top practical talents, the establishment of internship fields, international cooperation, and technology transfer, innovation and incubation, to introduce sufficient teaching and research resources to cultivate top talents of cyber security practical training and forward-looking cyber security research energy.

The second objective of this program is "construct a proactively defending infrastructure network". It alters the passive defense after a cyber security incident occurs; turning passive into active defense; adjusting the protection mechanism and improving contingency measures; introducing source tracing, detection, early warnings and countermeasures into the protection strategies to respond to multiple and complex malicious attacks. In recent years, countries around the world have successively adopted this approach. Through the use of national mission-oriented research related application technologies, this

program improves the cyber security protection of Government Service Network (GSN), analyzes the information and converts it into effective intelligence, and then further enhances the power of scientific and technological investigations to prevent emerging cybercrimes.

The last objective is “establish public-private partnership to create an environmental safety of cyber security”, a continuation of the combination of resources and energies from sectors of industry, government, academia, and research institutes to extend the energy of cyber security protection to private units; in addition, there have been many cyber security incidents in recent years due to malicious attackers hacking information service providers. They further intruded governmental agencies through remote connections and other methods, turning the supply chain vendors contracting government tenders into cyber security breaches. These events demonstrate the increasing importance of the implementation of outsourcing security management of government information operations. In addition, 5G networks and IoT devices are closely related to the lives of our citizens. This program not only promotes chip security to improve the core security of equipment, but also improves the network security of the new generation of mobile communication technology and promotes IoT compliance verification and field demonstration, so that our citizens experience the convenience brought by new technology, and at the same time enjoying security, and jointly maintaining a smart network security environment.

C. Promotional Strategies

In order to cultivate outstanding cyber security talents in our country, improve CI protection, use forward-looking technology to proactively prevent threats and block them at the source, extend cyber security awareness and capacity to private enterprises through public-private partnership collaboration, and build a safe and intelligent networking environment. This program proposes four promotional strategies, namely "absorbing global high-level talents, cultivating independent innovation and research energy, promoting public-private partnership collaborative governance, enhancing the resilience of critical infrastructure, making good use of smart and forward-looking technologies, proactively resisting potential threats, constructing safe and smart IoT, and increasing non-governmental protection energy." We will continue to promote the cyber security industry in conjunction with the "cyber security excellence industry" plan of the six core strategic industries, to build a safe, resilient and smart country.

(A) Attract high-level talents all over the world; cultivate independent power of research and innovation

In response to the demand for cyber security manpower during national development, in the fifth phase of the development plan, various competent authorities (units) have promoted relevant plans to inject resources to build cyber security cultivation environment, emphasizing innovation and cultivation models with a practice and industry-university connection orientation. The models also combined with the cyber security teaching

energy of international and domestic universities and colleges; established a demand-oriented cyber security personnel training system as the goal; nurtured high-quality cyber security talents and provided them to various industries in Taiwan.

Currently, Taiwan is now promoting the DIGI+ program and the 5+2 industrial innovation plan and using them as the foundation to build six core strategic industries to drive their digital upgrade. Cyber security has indeed become the most important foundation; it is urgent to cultivate sufficient cyber security talents and forward-looking research. For the future demand of cyber security in terms of technology and talent to take roots, this strategy plans to establish The Excellent Center of Cyber Security, with the goal of becoming an iconic high-level talent and technological innovation base in the Asian region.

1. Expand the quota of cyber security educators and teaching resources in higher education

1.1 The project increases the quota of teachers

Invite first-rate cyber security competition teams, teachers in the practical fields, researchers and well-known celebrities in the communities at home and broad; and provide excellent salaries to recruit top high-level researchers as cyber security instructors; encourage colleges and universities to compete with domestic and foreign industries and academic research institutions for the recruitment of excellent cyber security talents to facilitate the cultivation of cyber security professionals and the quality of teaching.

1.2 Open academic area network centers, government networks and other fields for internships and actual drills

(1) Through the university area network center and university cyber security laboratory, provide the three aspects of "themes of teaching experiment", "modes of internship field (physical/virtual)" and " teaching and research courses combined with the cyber security departments in the universities". Integrate the network or simulation situation in the laboratory into teaching practices; conduct research and analysis or offensive and defensive drills to cultivate cyber security practical talents.

(2) Plan the GSN backbone network as an open data field; expand the field of cyber security teaching practice; and improve the facility and environment of cyber security teaching.

2. Shift resources to high-level cyber security scientific research

2.1 Develop a national mission-oriented and key (core) cyber security prospective research

In response to emerging threats and development trends in cyber security, the Excellence Center for Cyber Security has recruited international talents to be responsible for the short-to-mid-term applied technology research required by government agencies, as well as the long-term basic research on our key cores, in order to cultivate and strengthen the autonomy of cyber security prospective research in our country.

2.2 Deeply cultivate academic cyber security research

Intensive research and development of software and hardware-related cyber security technologies to meet the cyber security technology needs of the state and private industries, enhance the research and development capabilities of industry, government and academia, and activate the cyber security research ecosystem.

2.3 Transnational talent exchange and research cooperation

(1) Participate in the formulation of international cyber security standards and regulations; ensure that the technology of development is in line with international standards; and carry out international cooperation through the results of prospective research on cyber security to enhance the international visibility of Taiwan.

(2) The goal is to cultivate high-level talents with international vision and R&D technology; actively promote diplomacy of science and technology; and operate interntaitonal partnerships for the cultivation of multinational talents.

3. Cultivate top practical and cross-regional cyber security talents

3.1 Cultivation of cyber security talents in schools, on the jobs and governmental agencies

(1) Cyber security talents in schools: Constructing demand-oriented design course content and modules; optimizing cyber security practice teaching resources; cultivating cross-regional cyber security and strengthening cyber security awareness education; and nurturing talents of cyber security practices.

(2) On-the-job cyber security talents: promoting industrial cyber security teaching and practical courses for the axis industries; developing

cyber security professional training and practical application talents; and accelerating the industry to enhance the energy of cyber security talents.

(3) Cyber security talents in governmental agencies: Promoting the cyber security function training blueprint, divided into three aspects of strategy, management and technology; planing 6 aspects of cyber security function training; improving the cyber security management and technical capabilities of the government agencies, and training the full-time manpower for government agencies.

3.2 Cultivation of top cyber security talents with practical experience

The initial training targets focus on the elites with cyber security potential in our country. We select the best talents from industry, academia, government and military for training, implementing training programs. And for different types of cyber security talents, we plan different evaluation mechanisms (such as obtaining relevant licenses or passing exams, etc.). The top talents who have completed the training can get better job opportunities and can assist the cyber security protection of government and critical information infrastructure (CII) as the backing of the country's urgent need of manpower deployment, while the long-term recruitment targets will be expanded to the Asia-Pacific region, and the goal is to become a top talent training base of cyber security for the Asia-Pacific region.

(B) The Promotion of public-private partnership collaborative governance; Enhancement of the resilience of critical infrastructure

The fifth phase of the development plan has established 8 major CI sectors and a national-level information sharing and analysis center (ISAC), computer emergency response team (CERT) and security operation center (SOC), which will assist the government to manage and transmit across-regional national cyber security information to assist domestic emergency handling capabilities in response to cyber security incidents, and fully grasp cyber security united defense monitoring conditions all time.

In order to improve CI's cyber security protection energy and response capabilities to enhance its protection resilience, this strategy will continue to promote and implement cyber security protection standards in various sectors, supplemented by offensive and defensive drills and audits to review its implementation effectiveness; at the same time, constructing a blueprint for cyber security functions in this field to improve the cyber security quality of the CI frontline personnel.

1. Build Public-private partnership Calloborative Governance Operational Mechanism in various fields

1.1 Continue to promote the implementation of the cyber security management law, and review it in due course to respond to the trend of international cyber security protection

In response to practical implementation and promotional needs, we will adjust relevant laws and regulations, and continue to improve and expand the assessment of the maturity of cyber security governance to accelerate the construction of our national cyber security environment.

1.2 Promote the implementation of cyber security protection baseline of critical infrastructure

Establish and rollingly revise the cyber security protection standards in the CI sector and introduce CI providers with cyber security responsibility above B or higher level. And through the cyber security audit to understand the implementation of the compliance items of the CI provider's cyber security law (such as maintenance plans, to-do lists and cyber security protection standards), and strengthen the integrity and effectiveness of the cyber security protection work.

1.3 Establish the maturity of cyber security governance in the industrial control field

Industrial control systems provide management and control for various industrial processes and are widely used in CI sectors such as petroleum, water resources, natural gas, and power grids. In order to effectively measure the degree of cyber security protection of industrial control systems, we will establish cyber security governance evaluation model in the field of industrial control to grasp the cyber security implementation status of CI providers and improve the readiness of cyber security protection.

1.4 Promote national-level cyber security risk assessment

Identify the core information and communication systems and their cyber security threats in various CI sectors, and effectively control the threats of overall cyber security in our country.

2. The enhancement of personnel' cyber security awareness and

reinforcement of cyber security capacity construction

2.1 Set up Chief Information Security Officer (CISO) and strengthen personnel's cyber security professional capabilities

(1) Promote CI providers to set up high-level cyber security chiefs to coordinate the cyber security policies and resource scheduling; and drive CI organizational culture that highlights cyber security.

(2) Establish a database of cyber security experts in various CI sectors (such as retirees or vendors) to handle external cyber security audits or drills of CI providers.

(3) Develop learning maps for cyber security functions in various sectors of CI, develop relevant courses year by year, and train a certain number of employees.

2.2 Establish a simulated field as a practical response capability; incorporate cyber security situation into teaching and training

Establish a national CI simulation field; provide an empirical field of cyber security protection solutions required in the domestic CI field; and support education and training, large-scale offensive and defensive drills, and international cyber security offensive and defense competitions.

3. Public-private partnership cooperation to deepen the exchange of information and implementation of response drills in normal times

3.1 Improve the cyber security united defense mechanism (information sharing, response notification, cyber security monitoring) of the critical infrastructure

(1) Continue to improve the integrity and effectiveness of cyber security

monitoring of government agencies.

(2) Establish a notification exchange format that meets the latest international standards; quickly transform, share and apply information of cyber security events, and shorten the timeliness of the process of notification response and intelligence integration.

(3) The competent authorities in various CI sectors continue to improve the operation of cyber security united defense and enhance its qualitative and quantitative benefits.

3.2 Regularly conduct public-private united offensive and defense drills

The competent authorities in the CI sector regularly implement offensive and defensive drills to improve personnel's familiarity and alertness to events of cyber security attacks, shorten the incident response time and reduce losses.

3.3 Handle cross-regional (or transnational) offensive and defensive drills for critical infrastructure

Regularly conduct cross-CI sector or transnational offensive and defensive drills to verify the effectiveness of cyber security protection and strengthen the resilience of CI information cyber protection.

(C) Utilization of smart and forward-looking technology; Proactive defense against potential threats

In view of the increasingly sophisticated attack methods, traditional defenses are no longer sufficient. The focus of future promotion lies in the conversion of intelligence and information from effective intelligence; the preparation of prediction of attack methods; and even tracing the source of the

attack for blocking, etc. This strategy is based on the 7 attack stages proposed by the Cyber Kill Chain: reconnaissance, arming, delivery, attack, installation, command and control, taking action to formulate defense actions at each stage.

In the investigation stage, we reduce cyber security risk through the establishment of a mechanism for proactive discovery of the vulnerabilities of the information and communication system in advance, notification and repair mechanism, and the promotion of the government's great intranet, centralization of the government's cyber security protection to reduce cyber security risks; in the armed stage, improve threat search and active detection Measure energy and cooperate with international companies to increase the breadth of intelligence search, predict attack patterns to be deployed in advance; in the stages of delivery, attack, installation, ordering and control, develop active defense technologies to establish a zero-trust architecture cyber security protection verification environment , To improve the depth of cyber defense; at the final stage of action, the deterrence effect is achieved by strengthening cybercrime detection and prevention capabilities, enhancing traceability and tracking capabilities, and strengthening cross-border cybercrime detection.

1. Continue to promote centralized sharing of government information (cyber) security

1.1 Connect with the independent needs of national defense and develop the ecosystem of the domestic cyber security industry

(1) Provide internal-to-internal, internal-to-external, and cross-organization network diversion operations to strengthen GSN internal

information and communication security.

(2) Complied with the upward concentration of information resources and promote the concentration and export of network of the government agency to higher-level agencies.

(3) Strengthen the proactive defense energy of the government's intranet and block malicious attacks in time.

1.2 Establish the mechanism to actively discover, report and repair the vulnerabilities of the information and communication system

Through an automated notification mechanism, shorten the window period between the release and repair of the agency’s cyber security vulnerabilities and reduce the risk of the system being hacked.

2. Expand international participation and deepen cross-border intelligence and capital sharing

2.1 Development of forward-looking research and technology application of active defense

Research and develop automated smart collaboration and response cyber security modules; combined with AI technology to improve the ability to quickly detect and respond to cyber attacks; and build a cyber security R&D ecosystem.

2.2 Integrate domestic and foreign sources of information, and deepen international cooperation

Develop N-ISAC to become the main domestic intelligence and information integration platform; integrate domestic and foreign intelligence and information sources; enhance threat collection and active

detection capabilities; and promote standard intelligence and information exchange formats to interface with the world.

3. Defend in Advance to Block the Attack at Borders

3.1 Apply emerging technologies to quench effective intelligence and develop proactive defense technologies

With proactive defensive thinking, strengthen the research and development and application of related technologies to enhance the cyber security protection capabilities of government agencies, through the key aspects of research and analysis, defense-in-depth, active prevention, source tracing and blocking, etc.

3.2 Improve the comprehensiveness of the defense-in-depth of the government service network

(1) Evaluate and introduce the Zero Trust Network and gradually try to verify its feasibility.

(2) Improve the power of GSN cyber security threat analysis and grasp the proactive defense information and overall profile of threat attack.

(3) Strengthen malicious intrusion detection of the external network and regional united defense; enhance the defense resistance of domain name system (DNS) against attacks to ensure the "confidentiality" and "integrity" of DNS data and the continuous “availability" of DNS.

4. Enhancing the power of technological investigations to prevent emerging cybercrimes

4.1 Strengthen the detection capabilities of emerging cybercrimes

Analyze the attack patterns and defense mechanisms of hacker

attacks on the IoT and relay stations; strengthen the practical training of criminal investigation skills; and build a simulation platform for the investigation of cyber security incidents to strengthen the overall investigation and actual combat power.

4.2 Improve the source tracing and tracking capabilities of cyber security events

Continue to expand the power of cyber security forensics; autonomously develop on-site evidence collection tools; strengthen information sharing and technical exchanges; and analyze and compare the sources of countermeasures and hacker organizations for the purpose of traceability.

4.3 Strengthen the investigation mechanism of cross-border cybercrime

(1) Actively participate in various judicial and international cyber security seminars; establish a window for accessing relevant criminal information with foreign companies; enhance cross-border cybercrime investigation channels and technologies; and promote international information exchange.

(2) Make good use of information technology to develop independent application systems to discover domestic hidden malicious threat endpoints in advance.

(D) Building a secure and smart IoT; enhancement of non-governmental protection energy

Recently, it has been discovered that malicious attackers have changed

to a circuitous attack mode, first intruding outsourced information service providers of government agencies, and then indirectly hacking government agencies. Therefore, in addition to continuing to strengthen the cyber security protection capabilities of government agencies in our country, outsourced information service providers are also the key links. Therefore, we will strengthen the supply chain risk management of outsourcing as a key task for promotion.

Facing the 5G network era, the security of various information and communication-related equipment is becoming more and more important. In addition to assisting telecom industry vendors in our country to focus on 5G cyber security risk issues and propose corresponding solutions, it is also necessary to pay attention to various aspects of the IoT equipment and services related to the network development of a new generation, and formulate relevant compliance verification and field demonstrations, to accelerate the implementation and commercialization of IoT cyber security solutions and refer to international standards to promote internationally competitive cyber security solutions, with the hope of exporting to the international market.

1. Counseling companies to strengthen cyber security protection capabilities during digital transformation

1.1 Integrate private resources to establish a public-private partnership collaboration mechanism to assist companies in enhancing their cyber security protection capabilities

(1) Optimize TWCERT/CC cyber security information system and services; deepen cyber security incident consulting and co-operation

services for the domestic enterprises, expand cyber security promotion, and enhance the energy and awareness of cyber security protection of private sectors.

(2) Improve the cyber security knowledge and protection capabilities of online retailers, and reduce the risk of personal information leakage.

1.2 Raise citizen's awareness of cyber security

The government should work with the private sector to raise the citizens' cyber security awareness, integrating cyber security awareness into the citizens' life, and internalize it into the basic needs of service use, to facilitate the development of advanced cyber security technology, software and hardware, and professional talents.

2. Strengthening the Supply Chain Security Management

2.1 Strengthen the supply chain risk management of outsourcing

We assist and counsel various agencies to handle outsourcing operations, including the establishment, maintenance or information and communication services to strengthen the cyber security management of the outsourcing manufacturers.

2.2 Focus on the security of telecommunications chip products

(1) Research and develop chip circuit cyber security testing tools to solve the hidden cyber security risks of chips.

(2) Establish an internationally recognized chip cyber security testing laboratory to supplement the gaps of domestic chip testing technology and the ecosystem of the testing environments and reduce the cyber security compliance barriers for exporting domestic products.

3. Build the IoT Security

3.1 Build a safe and smart mobile technological network of new generation

(1) Continue to complete 5G cyber security supervision regulations and actions and establish 5G cyber security testing laboratories to verify the feasibility of the regulations and assist the industry to complete cyber security protection of the 5G network.

(2) Establish a national-level communication and information security laboratory and develop a reference framework and guidance documents for information and communication security protection to improve the security of the 5G network in our country.

(3) Build a 5G vertical application development environment, promote integration and coordination to facilitate cooperation among all parties, and adjust laws and regulations to promote the development of 5G vertical applications.

3.2 Formulate IoT cyber security compliance certification and field demonstration

(1) Formulate IoT cyber security testing and verification framework, and formulate priority strategies and checklist items for IoT cyber security testing.

(2) Establish a product refining field; promote a supply-demand matching mechanism; and strengthen the value integration of the cyber security service chain.

(3) Assist domestic legal persons and information and communication

manufacturers to participate in the formulation of cyber security-related international standards, and conduct information exchanges with international standards-related organizations to promote the integration of cyber security technology with international standards in our country.

(4) Promote cyber security testing of IoT devices; enhance manufacturers' and users' awareness of cyber security protection; and promote the development of digital innovative applications.

D. Duty Division by Agencies

Table 2: Duty Divisions by Agencies

Work Item	Unit of Organization/ Competent Agency
Strategy 1: Attract high-level talents all over the world; cultivate independent power of research and innovation	
1. Expand the quota of cyber security educators and teaching resources in higher education	
1-1 The project increases the quota of teachers	Ministry of Education
1-2 Open academic area network centers, government networks and other fields for internships and actual drills	Ministry of Education; Department of Cyber Security, Executive Yuan; (National Development Council)
2. Shift resources to high-level cyber security scientific research	
2-1 Develop a national mission-oriented and key (core) cyber security prospective research	Department of Cyber Security, Executive Yuan; Board of Science and Technology, Executive Yuan
2-2 Deeply cultivate academic cyber security research	Ministry of Science and Technology
2-3 Transnational talent exchange and research cooperation	Department of Cyber Security, Executive Yuan; Board of Science and Technology, Executive Yuan; Ministry of Science and Technology
3. Cultivate top practical and cross-regional cyber security talents	

Work Item	Unit of Organization/ Competent Agency
3-1 Cultivation of cyber security talents in schools, on the jobs and governmental agencies	Ministry of Education; Ministry of Economic Affairs; Department of Cyber Security, Executive Yuan
3-2 Cultivation of top cyber security talents with practical experience	Department of Cyber Security, Executive Yuan; Board of Science and Technology, Executive Yuan
Strategy 2: The Promotion of public-private partnership collaborative governance; Enhancement of the resilience of critical infrastructure	
1. Build Public-private partnership Collaborative Governance Operational Mechanism in various fields	
1-1 Continue to promote the implementation of the cyber security management law, and review it in due course to respond to the trend of international cyber security protection	Department of Cyber Security, Executive Yuan; (Various Agencies)
1-2 Promote the implementation of cyber security protection baseline of critical infrastructure	Various CI Competent Agencies
1-3 Establish the maturity of cyber security governance in the industrial control field	Department of Cyber Security, Executive Yuan; (Various CI competent agencies)
1-4 Promote national-level cyber security risk assessment	Department of Cyber Security, Executive Yuan; (Various CI competent agencies)
2. The enhancement of personnel' cyber security awareness and reinforcement of cyber security capacity construction	
2-1 Set up Chief Information Security Officer (CISO) and strengthen personnel's cyber security professional capabilities	Various CI competent authorities
2-2 Establish a simulated field as a practical response capability; incorporate cyber security situation into teaching and training	Department of Cyber Security, Executive Yuan; Board of Science and Technology, Executive Yuan; (Various CI Competent Authorities)
3. Public-private partnership cooperation to deepen the exchange of information and implementation of response drills in normal times	
3-1 Improve the cyber security united defense mechanism (information sharing, response notification, cyber security monitoring) of the cirtical infrastructure	Department of Cyber Security, Executive Yuan; Various CI Competent Authorities
3-2 Regularly conduct public-private united offensive and defense drills	Various CI Competent Authorities

Work Item	Unit of Organization/ Competent Agency
3-3 Handle cross-regional (or transnational) offensive and defensive drills for critical infrastructure	Department of Cyber Security, Executive Yuan; (Various CI Competent Authorities)
Strategy 3: Utilization of smart and forward-looking technology; Proactive defense against potential threats	
1. Continue to promote centralized sharing of government information (cyber) security	
1-1 Connect with the independent needs of national defense and develop the ecosystem of the domestic cyber security industry	National Development Council; Department of Cyber Security of Executive Yuan; (Various agencies)
1-2 Establish the mechanism to actively discover, report and repair the vulnerabilities of the information and communication system	Department of Cyber Security, Executive Yuan; (Various agencies)
2. Expand international participation and deepen cross-border intelligence and capital sharing	
2-1 Development of forward-looking research and technology application of active defense	Ministry of Economic Affairs
2-2 Integrate domestic and foreign sources of information, and deepen international cooperation	Department of Cyber Security, Executive Yuan;v (Various CI Competent Authorities)
3. Defend in Advance to Block the Attack at Borders	
3-1 Apply emerging technologies to quench effective intelligence and develop proactive defense technologies	Department of Cyber Security, Executive Yuan
3-2 Improve the comprehensiveness of the defense-in-depth of the government service network	Department of Cyber Security, Executive Yuan; National Development Council
4. Enhancing the power of technological investigations to prevent emerging cybercrimes	
4-1 Strengthen the detection capabilities of emerging cybercrimes	Ministry of Internal Affairs; Ministry of Justice
4-2 Improve the source tracing and tracking capabilities of cyber security events	Ministry of Internal Affairs; Ministry of Justice; Department of Cyber Security, Executive Yuan
4-3 Strengthen the investigation mechanism of cross-border cybercrime	Ministry of Internal Affairs; Ministry of Justice
Strategy 4: Building a secure and smart IoT; enhancement of non-governmental protection energy	
1. Counseling companies to strengthen cyber security protection capabilities during digital transformation	

Work Item	Unit of Organization/ Competent Agency
1-1 Integrate private resources to establish a public-private partnership collaboration mechanism to assist companies in enhancing their cyber security protection capabilities	National Communications Commission; (Ministry of Economic Affairs)
1-2 Raise citizen's awareness of cyber security	National Communications Commission
2. Strengthening the Supply Chain Security Management	
2-1 Strengthen the supply chain risk management of outsourcing	Department of Cyber Security, Executive Yuan
2-2 Focus on the security of telecommunications chip products	Ministry of Economic Affairs
3. Build the IoT Security	
3-1 Build a safe and smart mobile technological network of new generation	National Communications Commission
3-2 Formulate IoT cyber security testing and field demonstration	Department of Cyber Security, Executive Yuan; Ministry of Economic Affairs; (National Communications Commission)

NOTE: The CI competent authorities refer to the Ministry of Economic Affairs, National Communications Commission, Financial Supervisory Commission , Ministry of Health and Welfare, Ministry of Transportation and Communications, and Ministry of Science and Technology

E. Key Performance Indicators

According to the vision, goals and promotional strategy, this program sets 3 important performance indicators, which are described as follows:

(A)The Cultivation of 350 Cyber Security Practical Experience Talents

In response to the demand for cyber security manpower for national development, the Cyber Security Office of the Executive Yuan has worked with the Ministry of Education, the Ministry of Science and Technology, the Ministry of Economic Affairs and other agencies (units) to jointly promote the cultivation of cyber security professionals, inject resources to build an

environment for cyber security cultivation, combining with the cyber security teaching energy of domestic universities and colleges to establish a demand-oriented cyber security personnel training system. At present, the campus side has already promoted the master program of cyber security; for the industry side, the Ministry of Economic Affairs has formed mid- to long-term development classes for the unemployed; in the country level, the academic and research institutions in our country have completed many academic studies on the forward-looking cyber security research and are gradually building a systematic cyber security talent cultivation and forward-looking research system.

This program will continue to increase the quota of domestic high-level cyber security talents and establish a national forward-looking research center for the future needs of cyber security in terms of technology and talents to take roots. The goal is to become a representative high-level talents and technological innovation base in Asia. At least 350 domestic and international practical combat talents will be trained by renowned trainers from foreign cyber security academia, industry and community; providing sufficient teaching and research resources to nurture the training of top practical talents and the cyber security forward-looking research energy in our country.

(B)Promote the governance maturity of cyber security of the government agencies (including objective indicators) to level 3

In order to measure the defensive capabilities and governance effectiveness of the government agencies in our country, we have proactively promoted the governance maturity of government agencies in the fifth phase

of the development plan. And addressed in the management aspect of the "Information and Communication Security Responsibility Level Rating Method" that public agencies that have been clearly defined as cyber security responsibility level A and level B shall conduct cyber security governance maturity assessment once a year.

The current cyber security governance maturity assessment method is based on the three aspects of cyber security governance: the "strategic", "management" and "technical" aspects of the three design-corresponding inspection projects, including policy and organizational management effectiveness, performance and achievement supervision implementability, cyber security incident management, and emergency response effectiveness and other indicators. The capabilities are divided into 6 levels from low to high after evaluation, which are "Level 0 Incomplete Process", "Level 1 Performed Process", "Level 2 Managed Process", "Level 3 Established Process", "Level 4 Predictable Process", "Level 5 Optimizing Process". According to the statistics by the end of 2020, the average maturity level of A-level institutions was 2.56.

In order to improve the maturity of cyber security governance in the existing Information Technology field, objective indicators will be added, such as collecting monitoring data, offensive and defensive exercise effectiveness, and analyzing the authenticity of its protection level; in addition, OT cyber security governance maturity assessment and related standard documents will be set simultaneously and imported to CI providers. With the above-mentioned cyber security governance maturity measurement

mechanism, in 2024, all A-level government agencies will reach above level 3 or higher (including objective indicators). It is expected that cyber security defense in our country will be achieved in advance, traced and tracked with early warnings.

(C) Formulate 12 cyber security testing technological guideline or industry standard

With the vigorous development of 4G and 5G communications, the application of IoT devices has also become more widespread. In order to enhance the cyber security protection capabilities of our national information and communication products, the Ministry of Economic Affairs and the NCC have mutually cooperated to formulate IoT device cyber security testing standards. From 2017 on, we have successively initiated cyber security standards, technical guidelines or drafts regarding video surveillance (IP CAM, NVR, DVR), smart buses (vehicles and smart stops), smart streetlights (light controllers and lighting gateways), wireless Access Points (AP), wireless routers, MOD (Multimedia on Demand) set-top boxes, cable TV set-top boxes, smart speakers, etc. In addition, various types of product cyber security testing laboratories have been established by joint efforts and the results have been witnessed. In particular, the video surveillance cyber security industry standard has become our national standard (CNS 16120) in 2019.

In view of the diversified development of IoT devices, at this stage, the method of gradually formulating cyber security testing standards for a single item may not keep up with the speed of product innovation. Therefore, an

overall strategy and promotional plan are needed; for this, this program will refer to the product certification framework from the US NIST and the EU ENISA to develop the IoT cyber security testing framework of our country. It is expected that a total of 12 IoT cyber security testing technical guidelines or industrial standards will be formulated in 4 years, and it is expected that the IoT device cyber security testing ecological chain can be maintained continuously. A safe and reliable digital infrastructure will be provided for our citizens.

Table 3: Milestones by Year

Key Performance Indicator	2021	2022	2023	2024
Cultivation of 350 Cyber Security Practices Talents	Cultivate 50 Cyber Security Practices Talents	Cultivate 50 Cyber Security Practices Talents	Cultivate 125 Cyber Security Practices Talents	Cultivate 125 Cyber Security Practices Talents
Promote Cyber Security Governance Maturity of Governmental Agencies to Level 3 (Including Objective Indicators)	Establish Cyber Security Governance Maturity Objective Indicators	Promote 3 A-Level Governmental Agencies to Implement Cyber Security Governance Maturity until Above Level 2 (Including Objective Indicator)	Promote 30 A-Level Governmental Agencies to Implement Cyber Security Governance Maturity (Including Objective Indicator) till Above Level 2	Promote All A-Level Governmental Agencies to Implement Cyber Security Governance Maturity (Including Objective Indicators) Until Level 3

Key Performance Indicator	2021	2022	2023	2024
Formulate 12 Cyber Security Testing Technological Guideline or Industry Standard	Complete 3 Cyber Security Testing Technolocial Guideline or Industry Standards	Complete 3 Cyber Security Testing Technological Guildeines or Industry Standards	Complete 3 Cyber Security Testing Technological Guidelines or Industry Standards	Complete 3 Cyber Security Testing Technical Guidelines or Industry Standards

V. Expected Benefits

A. In order to develop the digital application of cyber security ecosystem, complete DIGI+ and 5+2 industrial innovation solutions and cyber security capabilities, with the vision of "becoming the high-level cyber security talents and technological innovation base for the Aisa-Pacific region", we will let the future demand of cyber security in terms of technology and talent take roots, and provide sufficient teaching and research resources to bolster top practical talents and forward-looking research energy of cyber security in our country.

B. Facing the environment of increasingly severe cyber security threats, we will build a proactive defense mechanism. Through strengthening cyber assets placement management before attacks, and the bottom-up integration of cyber security protection, the risks of cyber security will be successfully reduced, achieving the effectiveness of early deployment. When an attack occurs, by developing proactive defense technology and deepening the domestic intelligence and information integration platform, it is hoped to prevent attacks on the border and achieve the effect of early blocking; finally, after the attack, the power of technological investigation of the judicial unit to prevent emerging types of cybercrime will be continuously increased to achieve the effect of traceability. Then, the cyber security governance maturity measurement mechanism (including objective indicators) will be used to present the government agencies' proactive defense energy by quantitative indicators; and follow up by the measurement results as a reference for formulating improvement strategies to assist agencies in improving the basic environment

of cyber security.

C. In recent years, smart cities/smart countries have been actively promoted at home and abroad, and the infrastructure for building a smart life is intertwined with multiple IoT devices and agile networks. Therefore, safe IoT devices are extremely critical. The future IoT cyber security testing technical guidelines or industry standards not only follow and synchronize with international standards, but also enable equipment manufactured by private enterprises to gain competitiveness, and ultimately consumers can obtain safe products to become the biggest beneficiaries, and to develop a sustainable IoT ecosystem.

VI. The Promoting Organization, Demand of Resources and Planning Management

A. The Promoting Organization

According to the "Key Points for the Establishment of the National Information and Communication Security Taskforce of the Executive Yuan", the DCS of Executive Yuan is the organizing and unit for the overall planning and promotion of cyber security-related policies and will be responsible for the overall planning and promotion of this program.

B. Implementation

The organizing agency (unit) of the work item of this program shall convene relevant ministries and meetings to propose action plans and performance indicators. The detailed implementation plan shall be formulated by each organizing agency (unit) in accordance with the relevant work regulations of the government's policy plan.

C. Source of Budget and Execution

The sources of the budgets of the annual plan proposed by the organizing agencies (units) are allocated by the agencies themselves or raised in accordance with relevant administrative procedures. The implementation of the annual plan shall be reviewed annually, and necessary amendments shall be made in accordance with the results of the budget review and comprehensive evaluation.

D. Management and Examination of Related Action Plans

The work items and performance indicators of this program will be

implemented by the DCS of Executive Yuan using the existing supervision mechanism.

E. Approval and Revision of this program

This program will be implemented after being approved by the Executive Yuan, and it will be the same when amended. This program should be reviewed and revised as a whole before the expiration date of the 4-year implementation period, and the development plan and related promotion plans should be rollingly reviewed on an annual basis as needed.