법제교류 연구 16-18-⑤
International Legal Collaboration Research 16-18-⑤

Introduction to Korean Cyber Security Law

Park Kwang Dong · Lee Sang Mo ·
Chang Young Jin · Lee Jin Seong ·
Cho Kwang Je · Yoon Soo Jin

한국법제연구원
KOREA LEGISLATION RESEARCH INSTITUTE

법제교류 연구 16-18-⑤
International Legal Collaboration Research 16-18-⑤

Introduction to Korean Cyber Security Law

Park Kwang Dong · Lee Sang Mo ·
Chang Young Jin · Lee Jin Seong ·
Cho Kwang Je · Yoon Soo Jin

한국법제연구원
KOREA LEGISLATION RESEARCH INSTITUTE

Introduction to Korean Cyber Security Law

Researchers : Park, Kwang-Dong (Senior Research Fellow, KLRI)
Lee, Sang-Mo (Research Fellow, KLRI)
Chang, Young-Jin (Professor, Hanlim Graduate Univ.)
Lee, Jin-Seong (Attorney at Law)
Cho, Kwang-Je (Manager, CBKIPA)
Yoon, Soo-Jin (Attorney at Law)

2016. 10. 31

한국법제연구원
KOREA LEGISLATION RESEARCH INSTITUTE

Abstract

Ⅰ. Purpose and Scope of Research

□ Cyber risks especially cyber attacks are new and modern risks which were not intended to occur along with the technology development at all. And under cyber attack cases it is difficult to find out what the exact cause and effect is.

□ Korea has been significantly exposed to cyber attacks due to advanced internet infrastructure, widely spreaded smart-phones and has accumulated experiences in response to cyber attacks from North Korea.

□ Under this situation, cyber security experts and governmental officers from all over the world very interested in Korean cyber security laws and regulations. Nevertheless, the interest was not satisfied because of lacking of the materials introducing our cyber security legislations.

□ Therefore by this research we would like to introduce Korean cyber security legislations. To do this, we shall research related Korean materials which introduce and analysis the legislations, and have a interview many experts in this field.

Ⅱ. Contents

□ Computer networks and information systems have governed daily human lives in this society. But a lot of cyber attacks, this society have been suffered, have made great threats on core functions operated by the networks and systems. This society has also been threaten by a lot of cyber attacks including from North Korea.

□ To respond cyber attacks, a state shall design appropriate legislations and national plans. Korea has also been struggle to make efficient legislations and policies to combat cyber attacks and enhance digital economy based on advanced information and communication technologies.

□ Nationwide responding system against cyber attacks shall be described in National Cyber Security Management Regulation. Following the regulation, Korean government authorities shall develop, establish, and perform the policies and initiatives related with cyber security. The regulation shall describe roles, duties and liabilities of government authorities such as Office of National Security in Blue House and National Cyber Security Center in National Intelligence Service. It also describe information sharing among government authorities.

□ Protecting Critical Information Infrastructure(CII) from cyber attacks is very important in National Security, because it can maintain core functions to operate a state and daily human lives, such as energy, banking, health, water and so on. Korean government has enacted Critical Information Infrastructure Protection Act since 2002. The Act has made national structure to protect CII from cyber attacks and described the provisions on designation on CII, evaluating vulnerabilities and establishing protection plans, responding cyber incidents, and penalties.

□ Protecting nuclear power plants from cyber attacks has been national agenda in Korea after North Korean cyber attacks against Korea Hydro & Nuclear Power Co. Ltd.(KHNP). Korea has enacted Nuclear Protection and Prevention Act to strengthen the protection system of nuclear facilities. Under the Act, the Korea Institute of Nuclear Nonproliferation and Control(KINAC) shall establish KINAC/RS-015 to protect nuclear facilities from cyber attacks.

□ Following the Comprehensive Measures to enhance National Cyber Security, Korean policy makers and legislators heard many voices from individuals, vendors, and governmental institutes agencies that cyber security industry shall be encouraged to support robust cyber security activities with best technologies. Hence, Cyber Security Industry Enhancement Act was newly enacted. According to the Act, Korean central and local government,

and municipals shall establish and perform policies to encourage cyber security industry and prepare measures to allocate budgets to fulfill that policies.

□ Electronic financial transaction is the convenient and quick ways to transact in the area of finance, so that it enables the financial companies or an electronic financial business entities to provide the user with new service and to enhance their profit. Notwithstanding this merits, the electronic financial transaction might cause big problems and turmoil if the hacking incidents on the IT network system occurs. Therefore it becomes more important to ensure the confidence of user by keeping the safety of information network system - its authenticity, confidentiality, integrity, availability and legitimate use should be provided without errors. To make secure and reliable electronic financial transactions, the “Electronic Financial Transactions Act” has been enacted.

□ After suffering several significant personal information disclosed cases, National Assembly members proposed a bill to independently and wholly focusing on personal information protection. The bill enacted to be an Act at March 29, 2011. and has been effected since 2011. 9. 30. To protect the personal information, the Act describes that a personal information manager shall establish an internal administration plan, keep access records, and take technical, administrative and physical measures necessary

for securing safety. He/she shall also have to establish and disclose of Personal Information Management Policies, and to designate Personal Information Protection Managers. Ministry of Interior certificate personal information protection measures in accordance with the Act. When a personal information manager becomes aware that personal information has leaked out, he/she shall notify the relevant holder of the information.

Ⅲ. Expected Effects

□ By understanding Korea's national structure to responding cyber attacks, law and policies related to critical information infrastructure including nuclear power plants, enhancing information security industry, securing electronic financial transactions, and protecting personal information, the other countries could establish robust cyber security laws and policies to responding cyber attacks.

□ By supporting the other countries to establish the laws and policies, Korea is also able to expand its role to the emerging markets, especially Asian countries, and strength cooperation on relevant industry with increasing demands for products and services related to cyber security. Therefore, it is likely to encourage sustainable cooperation on cyber security sector among Asian countries and the other countries in the world, after this research introducing Korean cyber security legislations.

□ Besides, the research is likely to assist materializing the value of creative economy and accompanied growth through the cyber security.

Key Words : Cyber Security, Critical Information Infrastructure, Personal Information Protection, Cyber Security Industry, Electronic Financial Transaction, Cyber crime, Cyber Attack

Table of Contents

Ⅰ. Introduction

A. Purpose of Research

Cyber risks such as cyber attacks and cyber crimes are new and modern risks which were not intended to occur along with the technology development at all. Thus in the most of cases it is difficult to find out what the exact cause and effect is.

In the last six years damage caused by cyber attacks rose 20 percent every year in the U.S. and it is estimated that economic losses caused world-widely by cyber attacks is 4,450 billion dollars(4.52 trillion won) annually. In addition, cyber crimes cause reportedly the social cost about 0.8 percent of the world GDP.

Because those cyber risks cannot be solely addressed by either individual or certain agencies, national level response system needs to be built and operated with the body coordinating and integrating the perils based on the technological superiority.

On January 14, 2016, multi-level targeted cyber attack occurred against government and non-governmental organizations (NGO) in the Asian countries. It showed that Asian nations are also not free from cyber attacks. Meanwhile, in order to deal with cyber attacks or crimes Asian nations also prepare the national level response system and improve and legislate laws related.

At ARF(the Asean Regional Forum), the only Asian-Pacific region intergovernmental, multilateral security association, the member nations have been discussed cyber security legislation concerning each country and the region.

Cyber security experts from Asian countries sought a legal and policy development for the region and their countries. When Asian countries and many other countries establish and maintain cyber security legislations, they refer to Korean legislations and have a great interest in understanding the legislation. The reason that they have interest in our legislation is Korea has been significantly exposed to cyber attacks due to advanced internet infrastructure, widely spreaded smart-phones and has accumulated experiences in response to cyber attacks from North Korea.

Nevertheless, the interest was not satisfied because of lacking of the materials introducing our cyber securitylegislations. Thus Korean legislation needs to be introduced to countries around the world once the legislation is organized with knowledge and experiences accumulated through informatization and economic development. The legislation will be used as an important reference for those countries to set up national level countermeasures and make relevant laws to prepare cyber attacks and crimes.

B. Scope and Methods of Research

The literature of national strategies, policies and legislation concerned the cyber security are collected and analyzed. Papers and technical reports issued by government ministries, professional research institutes and academies as well as materials of workshops and seminars are also analyzed.

Based on those analyses, the history and features of cyber securitylegislation evolved and developed through the process of informatization and economic development are analyzed.

It reinforces the awareness of cyber securitylegislation and encourages a practical legislative exchange support, exchanging and cooperation with relevant foreign experts such as Cherian Samuel, associate fellow at Institute for Defence Studies and Analyses, India, Dr. Cuihong Cai, associate professor at Fudan University, Liam Nevill, analyst, International Cyber Policy Centre at Australian Strategic Policy, Uchenna Jerome Orji, lawyers in Nigeria, Jana Robinson, director at the Prague Security Studies Institute (PSSI), and Dr. Yuan and Dr. Hwang, professors of National Defense University of Republic of China.

With such a literature analysis and expertises' collaboration, we seek to a substantive understanding and cooperation on the cyber security legislation. We, authors, have also shared expert opinions with each other and designated each one's role and written this paper distributed as follows.

Researcher	Charged parts
Park, Kwang-Dong	Ⅲ. A. Overview B. National Cyber Security Management Regulation Ⅴ. Conclusion
Lee, Sang-Mo	Ⅰ. Introduction
Chang, Young-Jin	Ⅲ. C. Critical Information Infrastructure Protection Act D. Act on Measures for Protection of Nuclear Facilities, etc and Prevention of Radiation Disasters
Lee, Jin-Seong	Ⅳ. A. Cyber Security Industry Enhancement Act
Cho, Kwang-Je	Ⅱ. Current Status of Cyber Security Initiatives
Yoon, Soo-Jin	Ⅳ. B. Electronic Finance Transaction Act Ⅳ. C. Personal Information Protection Act

Ⅱ. Cyber Security Initiatives and Legislations

A. Overview of Recent Cyber Attacks

1. Recent Cyber Attacks

Korea has suffered so many cyber attacks, although it has developed cyber security policies and legislation. The Ministry of Science, ICT and Future Planning in Korea, indicated that about 296 cyber attacks happened per day in 2012.[1)]

In 2001, Korea suffered the first nationwide cyber crisis which shut down networks and made malfunctions to access internet services. After this crisis, people understood the importance of cyber security for the first time. In June 2004, hacking arising from China made malfunctions against networks of government and public agencies happened. In July 2009, DDoS cyber attacks happened targeting Blue House, Ministry of National Defense, Korea Exchange Bank, Shinhan Bank. In March 2012, another DDoS cyber attacks made great damages the networks of 24 government authorities including Blue House and major ISPs and Banks. NH Banking systems were malfunctioned by cyber attacks in April 2011, and JoongAng Daily's homepage was changed and some data were deleted by cyber attacks.[2)]

In March 2013, three South Korean television stations and a bank suffered from frozen computer terminals.[3)] The South Korean government

1) http://english.yonhapnews.co.kr/northkorea/2013/10/04/62/0401000000AEN20131004007400320F.html(Last visited October 12, 2016)

2) National Assembly Library, Cyber Terror, Fact Book Vol. 39(2013. 9), p.19.

authority raised alert level on cyber attacks to three on a scale of five, and North Korea has been blamed for similar attacks in 2009 and 2011 and was suspected of launching this attack as well.[4] In June 2013, web-sites of government authorities were changed and servers of major medias companies were destroyed by cyber attacks, and Comprehensive Governmental Information Center were under DDoS attacks.

From December 2014 to June 2015, Computers in the state-owned operator Korea Hydro & Nuclear Power Co. Ltd.(Herein after "KHNP") were hacked, leading to leaks of internal data that include blueprints of reactors and radiation-exposure estimates.[5] The cyber attacks were made between Dec. 9 and 12 by sending 5,986 phishing emails containing malicious codes to 3,571 employees of the nuclear plant operator.[6] South Korean prosecutors assert that North Korean hackers were responsible for repeated disclosures of information, including blueprints of South Korean nuclear reactors gleaned from cyber attacks, as well as threats to extort money and destroy the nuclear facilities.[7] Because the malicious codes used for the nuclear operator hacking were the same in composition and working methods as the so-called ‘kimsuky’ that North Korean hackers use.[8]

---

3) Tania Branigan, “South Korea on alert for cyber-attacks after major network goes down: Computer systems of banks and broadcasters are interrupted, with fingers immediately pointed at North Korea”, The Guardian, 20 March 2013.

4) https://en.wikipedia.org/wiki/2013_South_Korea_cyberattack(Last visited October 12, 2016)

5) http://www.wsj.com/articles/south-korea-nuclear-plant-operator-hacked-1419237333 (Last visited October 12, 2016)

6) http://www.reuters.com/article/us-nuclear-southkorea-northkorea-idUSKBN0MD0GR20150317 (Last visited October 12, 2016)

7) http://www.heritage.org/research/reports/2015/03/the-us-needs-to-respond-to-north-koreas-latest-cyber-attack(Last visited October 12, 2016)

8) http://www.independent.co.uk/news/world/asia/north-korea-blamed-for-cyberattacks-on-south-korean-nuclear-power-plant-operator-10113860.html(Last visited October 12, 2016)

However Korean society has been under great shock and realized cyber attacks would be made great damages by malfunctioning nuclear power plants, which could lead to make harm against ordinary lives.

2. North Korean Cyber Capabilities

Kim Jung-Eun reshuffled power elites and adopted 'Economy-Nuclear Parallel Policy' by strengthening economic construction and national defense capability, in order to build up his own dictatorship.[9] North Korea uses cyber attacks as a major asymmetric strategy with nuclear power[10], to catch up on its military inferiority and recover recession-bound economy.[11]

Suffering a shrinking economic situation, North Korean government have been starving to encourage cyber attacks because it have been cost-benefit asymmetric measures causing confusions in international societies including South Korea and U.S.[12] Furthermore even the cyber attacks turn out arising from North Korea, it would deny it and argued it is needed to be supported by clear and convincing evidences.[13]

North Korean cyber attacks shall be leaded by Reconnaissance General Bureau(RGB). It is associated with cyber attacks as well as with terrorist,

9) Korea Institute for National Unification(KINU): North Korea Domestic and Foreign Policy Evaluation and Outlook after Kim Jong-un seizing the Power: 11th KINU Unification Forum(2015), pp.1-5.

10) Tobias Feakin, Playing Blind-Man's Buff: Estimating North Korea's Cyber Capabilities: International Journal of Korean Unification Studies, vol. 22, no. 2(2013), pp.67－69.

11) Jeong Yoon Yang, So Jeong Kim, Il Seok Oh, Analysis on South Korean cyber securityReadiness regarding North Korean Cyber Capabilities, WISA(2016).

12) Il Seok, Oh, South Korean Legal Initiatives to combat Cybercrime and Enhance Digital Economy, SECURING CYBERSPACE, PENTAGON PRESS(2016), p.307.

13) Id.

clandestine, and illicit activities and this shows that North Korea would use cyber activities for more provocative purposes.[14] Another important organization operating cyber attacks is Unit 121 which has been consisted with intelligence parts and attacking[15] parts by about 3,000 experts in cyber attacks.[16]

Above recent cyber attacks in Korea have been traced to be related with North Korea. However it is very difficult to make counter attacks against North Korea, because cyber conflicts may lead to real conflicts with kynetic arms. Therefore Korean government shall establish and develop cyber security policies and legislations to detect, control, investigate and respond cyber attacks from North Korea.

B. Cyber Security Policies

1. Cyber Security and Risk Allocation

A cyber risk such as cyber attacks or electronic infringement is a modern risk that was not expected by the technological advances. The features of modern risks, unpredictability and dissemination, threaten the individual life and affect the welfare of society as well as the existence of a nation.

As information age has been longer, has the risk been increased. Therefore it becomes a critical task to protect citizens from cyber risks and it is a national core issue to realize, maintain, and manage the task.

---

14) Jenny Jun, Scott LaFoy, Ethan Sohn: North Korea's Cyber Operations - Strategy and Response: Center for Strategic & International Studies(2016), p.35.

15) http://news.khan.co.kr/kh_news/khan_art_view.html?artid=201304102221195&code=940202 (Last visited October 12, 2016).

16) http://news.mk.co.kr/newsRead.php?year=2013&no=274000(Last visited October 12, 2016).

Since cyber securityactivity is one of the national security priorities, it should be implemented systematically at national level.

Regarding this, President Obama stated as information infrastructure such as computer, communication networks on which the U.S. citizens depend is a national strategic assets, it should be protected as a national security priority. The U.S. Congress also recognize cyber threat and attacks as a serious national security issue. Despite cyber risks are connected to the life of citizens as well as military operations, laws and policies related to cyber did not catch up rapidly changing technologies. So the U.S government and high ranking generals and officials recognize cyber risks as the most concerned national security challenges. Meanwhile, the U.S. Cyberspace Policy Review required the federal government to strengthen a long-term investment to develop the source of cryptography and information assurance technologies as well as infrastructure protection. “Strehgthening”, here, means the federal government have to possess capability to take priority on cyber securitysector. To do this, the government let the Congress invest into cryptography and cyber security sector.

2. Korean Cyber Security Policies and Initiatives

Cyber risks should be properly distributed to cyberspace users since there are risks as long as cyberspace exists. It is, however, impossible to distribute the risks to all cyberspace users as it is difficult to define whether the risks occurs, what the cause is and the range of damages because of lacking of the rational functions on the cause and effect of cyber risks. Therefore nation should make the cyber risks to be distributed primarily to the public sector in order to stabilize daily life of cyberspace

users and to set up a national and collective security system. The government should provide policies and legal basis to enforce the distribution of cyber risks.

Cyber security has been one of the important part in Korean National Security. Korean government emphasized cyber security as follows in National Security.

In addition to provocation from NK, threats and challenges against national security can manifest themselves in various forms : transnational threats such as terrorism, cyber attacks, climate change, epidemics, natural disasters and accidents, and as yet unknown future threats. In the Information Age, in which the world is connected through various networks, the possibility of cyber attacks is also a serious security issue. Being used in an increasing number of fields including the business, academic, military, and cultural areas, cyberspace offers a great number of benefits to humankind. The anonymity and trans-nationality of cyberspace, however, have brought various threats in such forms as cyber crimes and cyber attacks. Such cyber threats underline the need for the establishment of not only a domestic response system but also bilateral and multilateral cooperation mechanisms, some of which include fostering confidence-building measures between countries and establishing international norms.[17)]

Korean government developed National Cyber Security Comprehensive Measures of 2013 to realize a robust cyber security, after above 3.20, 6.25. cyber attacks from North Korea. The measures consisted with 4 major agenda such as Prompt, Cooperative, Robust and Creative. To reach “Prompt” Korean government designated Office of National Security as a control tower of governmental cyber security activities, and National

17) The National Security Strategy 2014 of Korea.

Intelligence Service as a working coordinator of the activities. This should be “prompt” responding system against cyber attacks with dispersing promptly the information and decisions related to the cyber attacks. To realize “Cooperative”, the government should established information sharing systems including public and private areas. to make “Robust” Korean government were increased to designate Critical Information Infrastructures from 209 to 400 to make robust responding and resilience of critical functions from cyber attacks and crimes. To reach “Creative” the government established a plan to educate and train about 5,000 persons as cyber security experts by 2017.

Recently, Korean government has established national response policy to address growing cyber attacks, in particular, from North Korea. After, especially, the NH Bank hacking and DDos attacks in 2013, “comprehensive national cyber security measures” are prepared by the joint ministries with NIS(National Intelligence Services) so as to systematically cope with cyber risks threatening national security.

After the attack on the KHNP(Korea Hydro & Nuclear Power Co. Ltd) in 2014, the government has arranged ‘comprehensive measures to enhance a cyber security alert’. According to the measures the government must: ① strengthen cyber security capabilities, ② carry forward a development of cyber securitykey technology and foster elite personnel, ③ supplement cyber response operation organization and skilled professionals and promote relevant industry, ④ expand international cooperation, ⑤ improve statue consolidation related to a cyber security.

Korean government has also acknowledged the importance of responding cyber attacks and crimes, and it designated Special Secretary of Cyber Security in Blue House in Janary 2015. After 3 month, Secretary of Cyber

Security in Blue House was appointed and he controlled cyber security policies and initiatives performed by Korean governmental authorities. In addition, as the National Assembly recognize cyber attacks as a national security issue, it submitted the bill of 'the Anti-cyber terrorism Act' and the bill of 'National cyber security Management Act' based on Presidential instruction 「National Cyber Security Management Regulation」 to integrate and manage the national cyber security response system.

C. Development of Cyber Security Laws and Regulations

The discussion of modifying laws related to cyber securities began in earnest when the adverse effects of the informatization on the national level which has been progressed since 1980 became the social problem.

In 1986, the initial informatization law, 「Expansion and Promotion of Utilization of Communications Network Act」, was enacted and regulated national policy and institution related to information. In accordance with the law the importance of data protection in the private sector was emerged. As a result, 「The framework act on informationalization promotion 」 including fundamental rules about data protection was also enacted in 1996. In the same year, the criminal law was amended to insert provisions about the offense forgery and falsification of electronic record and the invasion of privacy on electronic record.

In addition to that, various maintenance activities with data protection has been begun. For example, 「Digital signature act」 was enacted in 1999 along with the growing users of internet and e-commerce and 「Promotion of utilization of information and communication network act」 was completely

revised. Entering the communicopia in 21st century, the rate of reliance and importance on national and social communication systems has grown. Thus the need of maintenance of cyber security law has been increased. So 「Communication Infrastructure Protection Act」 was enacted in 2001 and a fraud misusing of computer was newly inserted into criminal law. Moreover, 「Promotion of utilization of information and communication network act」 was renamed as 「Promotion of utilization of information and communication network and data protection act」 adding the data protection provisions.

In 2005, 「the National Cyber Safety Management Regulation」 was enacted by presidential instruction to protect national communication networks. As implement of knowledge and information society has become a direction of national informatization policy, 「Promoting digitalization on administrative works to realize electronic government Act」 was completely revised to 「Electronic Government Act」 in 2007. 「Critical Information Infrastructure Protection Act」 also revised to improve the verification system of implement of protection on the major communication infrastructure.

According to the revision of 「the Government Organization Act」 in 2008, the works of Ministry of Information and Communication were transferred to relevant ministries such as Korea communication commission, the Ministry of Government Administration and Home Affairs and the Ministry of Knowledge Economy, etc.. The name of government department was also changed as a way of transformation in promoting system on informatization and data protection.

To systematize cyber security in defence sector 「Act on Establishment of Infrastructure for Informatization of National Defense and Management of Informational Resources for National Defense」 was enacted in 2010

and 「Electronic Government Act」 was also fully revised. As shown, government has continuously made efforts to reflect a developing and changing information society to the legislation in real. In 2011, 「The Privacy Act」 was enacted and September, 30, 2011 was enforced.

To ensure safety and reliability in electronic financial transactions by clarifying the relationship of electronic financial transactions laws, to provide convenience as creating a foundation for sound development of electronic financial business and to encourage to develop national economy, 「Electronic financial transaction Act」 was made in 2006 and has been enforced since 2007. According to the law, financial company or electronic financial business operators should take responsibility for damages when a user suffers a loss caused by certain accidents.

In 2015, 「Act on the promotion of the industry on data protection」 was legislated in order to achieve technological superiority on cyber security and to stimulate cyber security industry. Under the act the criteria for ‘the payment of appropriate data protecting service’ was set up and public-private joint monitoring system was conducted to recommend standard contract form and reform unreasonable order practices.

Additionally, the government has pushed ahead several plans such as establishment of ‘the promoting plan of data protection industry’, data protection technology development, fostering expert workforce, creating assimilation new market, supporting overseas expansion etc. so as to create foundation to stimulate systematic data protection industry.

Ⅲ. Legislations related with Establishing National Cyber Security Structure and Protecting Critical Infrastructure

A. Overview

With developed ICT technologies and infrastructures, Korea has established the advanced society using ICT in every parts of daily lives. However this society has been also suffered a lot of cyber attacks using this advanced ICT technologies and infrastructures, including attacks form North Korea.

After suffering the cyber attacks Korean government developed and established policies and initiatives enhancing cyber security. The policies and initiatives have been codified with Koran legislations as Acts or Regulations.

Nationwide responding system against cyber attacks shall be described in National Cyber Security Management Regulation. Following the regulation, Korean government authorities shall develop, establish, and perform the policies and initiatives related with cyber security. The regulation shall describe roles, duties and liabilities of government authorities such as Office of National Security in Blue House and National Cyber Security Center in National Intelligence Service. It also describe information sharing among government authorities. However the regulation shall not govern private areas, because an Act, passing by National Assembly, shall be needed to apply the provisions of the regulation on private sectors. Therefore a bill, making the regulation to an Act, has been proposed to

National Assembly but it can not even be replied to the related standing committee.

Protecting Critical Information Infrastructure(CII) from cyber attacks is very important in National Security, because it can maintain core functions to operate a state and daily human lives, such as energy, banking, health, water and so on. Korean government has enacted Critical Information Infrastructure Protection Act since 2002. The Act has made national structure to protect CII from cyber attacks and described the provisions on designation on CII, evaluating vulnerabilities and establishing protection plans, responding cyber incidents, and penalties.

Protecting nuclear power plants from cyber attacks has been national agenda in Korea after North Korean cyber attacks against KHNP. Korea has enacted Nuclear Protection and Prevention Act to strengthen the protection system of nuclear facilities. Under the Act, the Korea Institute of Nuclear Nonproliferation and Control(KINAC) shall establish KINAC/RS-015 to protect nuclear facilities from cyber attacks.

B. National Cyber Security Management Regulation

1. Duties, Policies and Management of Cyber Security

a. Duties of ensuring cyber security[18)]

The head of central administrative agency is responsible for ensuring security on its information and communication networks. To do this, he should take all necessary measures including hiring experts taking full charge of cyber securityworks.

18) Article 4. of the Cyber Security Management Regulation.

The head of relevant central administrative agency shall make the head of public agency and local government concerned take necessary action such as securing experts.

b. Policies and management[19)]

The director of the National Intelligence Service (hereinafter referred to as a "Director of NIS") shall control and coordinate policies and management relating to national cyber securityafter consultation with the head of central administrative agency.

The Director of NIS shall establish and implement a national cyber securitybasic plan conferring with the head of central administrative agency to effectively and systematically carry out cyber security related tasks. The Director of NIS shall also ask relevant organizations for coordination to smoothly improve the national cyber securitybasic plan.

2. Strategy Council and Counterplan Council

a. Strategy council[20)]

The council of national cyber securitystrategy (hereinafter referred to as the "Strategy council") shall be established under the Director of NIS so as to deliberate on important matters relating to national cyber security.

The Director of NIS shall be the chairman of the strategy council. The member of the Strategy Council shall be the vice-minister of Strategy and Finance, the vice-minister of Science, ICT and Futrue Planning, the vice-minister of Education, the vice-minister of Foreign Affairs, the vice-minister of Unification, the vice-minister of Justice, the vice-minister

19) Article 5. of the Cyber Security Management Regulation.
20) Article 6. of the Cyber Security Management Regulation.

of National Defence, the vice-minister of Government Administration and Home Affairs, the vice-minister of Trade, Industry and Energy, the vice-minister of Health & Welfare, the vice-minister of Land, Infrastructure, and Transport, and the vice-chairman of the Financial Services Commission, the responsible chief secretary of cyber security in presidential Secretariat, the secretary charge on cyber security in National Security Office, the vice minister of Office for Government Policy Coordination and Public officials holding a rank equivalent to that of the vice-minister of the relevant central administrative agency appointed by the chairman of Strategy Council. In such cases, if the agency has two or more public officials holding a rank equivalent to that of a Vice Minister, the one in charge of cyber security shall be a member.

Strategy Council shall deliberate on the matters; to establish and to improve of national cyber security system, the relevant policies and to adjust role between institutions, to carry out the instruction of president related to national cyber securityand other matters to be referred by the chairman of Strategy Council.

The important matters which went through deliberation shall be reported to the President and the Prime Minister. Necessary matters concerning the composition, operation, etc. of the Strategy Council shall be prescribed by the chairman of the Strategy Council.

b. Counterplan Council[21)]

The national cyber securitycounterplan council(hereinafter referred to as the “Counterplan council”) shall be established under the Strategy Council so as to effectively operate the Strategy Council.

21) Article 7. of the Cyber Security Management Regulation.

The chairman of the Counterplan Council shall be the deputy general manager in charge of cyber securityof National Intelligence Service(NIS) and members shall be the public officials holding a rank equivalent to the head of department, general manager of the agency which the members of Strategy Council belong to.

The Counterplan Council shall deliberate on the matters; national cyber securitymanagement and response plans, implementation relating to decisions of the Strategy council, delegated of instructed matters by the chairman of Strategy Council, and other matters to be referred by the chairman of Counterplan Council. Necessary matters concerning the composition, operation, etc. of the Counterplan Council shall be prescribed by the chairman of the Counterplan Council.

3. National Cyber Security Center[22)]

The national cyber security center (hereinafter referred to as the "NCSC") shall be established under the NIS so as to make complex and systematic national-level response.

NCSC shall carry out an establishment of national cyber securitypolicies, an assistance in operation of Strategy council and Counterplan council, collection, analysis and dissemination of cyber threats information, ensuring of the safety of national information and communication networks, drawing up and distribution of national cyber securitymanual, investigation of accidents occurred by cyber attacks and supporting of restoration, cooperation with foreign agency relating to cyber threats information.

The Director of the NIS may establish and operate a joint response team with private, administration, and military(hereinafter referred as

22) Article 8. of the Cyber Security Management Regulation.

"Response Team") under the cyber security center in order to assess, monitor, analyze of threat elements and joint investigation etc. relating to cyber threats on national level.

The Director of NIS may, if necessary, ask the head of relevant central administrative agency, local government and public agencies for dispatching public officials and staffs in order to establish and operate a joint response team.

4. Cyber Security Measures and Cyber Crisis Response

a. Establishment and Implementation of cyber securityMeasures[23)]

The head of central administrative agency shall establish and carry out cyber security measure to protect its information and communication networks and shall direct and manage it. The head of relevant central administrative agency may let the head of public institution and the head of local government make and implement cyber security measures.

The Director of the NIS may write and distribute national cyber securitymanuals and relevant directives needed to establish cyber securitymeasures. To do this, the Director of NIS should confer with relevant head of central administrative agency in advance.

The Director of NIS may ensure the safety of information communication networks by assessing the implementation of cyber securitymeasures. If necessary, he shall recommend required measures to the head of a relevant central administrative agency. In case of local governments and public institutions, it shall be carried out by conferring with the head of relevant central administrative agency.

23) Article 9. para. 1 of the Cyber Security Management Regulation.

b. Cyber Crisis Response Excercise[24)]

The head of central administrative agency, local governments and public institutions should conduct annual cyber crisis response exercise for information communication networks. The Director of NIS may conduct a integrated cyber crisises response training for information communication networks of central administrative agency, local government and public institution to prevent from cyber crisis of national level. In this case, the Director of NIS should notify training schedule to the head of relevant agency in advance unless special reasons are provided.

The Director may ask the head of central administrative agency, the head of local government and the head of public institution for necessary correction when he decides to be necessary to take after the training.

5. Information Sharing

a. Establishment and Implementation of Cyber Security Measures[25)]

The head of central administrative agency, the head of local government and the head of public institutions shall immediately notify information as to cyber attack plans or attacks against national information and communication networks or information occurred cyber threat to the Director of National Security Office and the Director of NIS when they collected such information.

Regarding the investigation, if the head of investigative agency believes the results would cause national security threats such as national secrets

24) Article 9. para. 2. of the Cyber Security Management Regulation.
25) Article 10. para 1. of the Cyber Security Management Regulation.

leakage or damage then he should notify such information to the Director of National Security Office and the Director of NIS.

The Director of NIS shall take necessary measures when the relevant information is delivered pursuant to the section 1 and notify the outcome to the head of relevant agency reporting the information.

b. Operation of Security Control Center[26)]

The head of central administrative agency, the head of local government and the head of public institutions shall establish a body which is able to detect cyber attacks and to analyze the relevant information and to immediately respond.

But when they cannot establish and operate the security control center they may contract out it to the other security control center operated by the head of central administrative agency(including the Director of NIS), the head of local government and the head of public institutions.

The head of body establishing and operating security control center shall give the cyber attack information collected and detected to the Director of NIS and the head of relevant agencies.

The head of body establishing and operating security control center shall deploy regular staffs to operate the center. The head of body establishing and operating security control center shall, if necessary, make the staffs of security control specialized company sent out by the Minister of Science, ICT and Future Planning conduct tasks.

In this case, the Minister of Science, ICT and Future Planning shall decide the necessary matters as to appointment and management of security control center under consultation with the Director of NIS. The Director

26) Article 10. para. 2. of the Cyber Security Management Regulation.

of NIS shall decide the details like installation and operation of security control center, the scope of prioviding cyber attack information, procedure and method etc. under consultation with the head of central administrative agency.

6. Response to Cyber Attacks

a. Emergency Alerts[27)]

The Director of NIS may issue any level alerts like attention, caution, warning, seriousness concerning the ripple effects and the severity of cyber attacks to prevent and to systematic response to them. Minister of Science, ICT and Future Planning issues alerts in the private sector, the minister of Defense issues alerts in the defense sector. The Director of NIS, the minister of Science, ICT and Future Planning and the Minister of Defense should exchange relevant information before issuing emergency alerts to conduct effective alerting at national level.

The head of relevant central administrative agency has to immediately disseminate that the alert is issued to the head of public agency and the head of local government and should take proper actions.

When the Director of NIS believes the cyber attacks would cause severe damage to the national security, he may issue a serious-level alert under the consultation with the Director of National Security Office. The Director of NIS may ask for the necessary information to issue an alert pursuant to the section 1 to the head of relevant administrative agency. The head of relevant administrative agency should coordinate unless there are specific reasons.

---

27) Article 11. of the Cyber Security Management Regulation.

b. Notice of damage and restoration[28)]

The head of central administrative agency should take steps to minimize the damage when founding the signs of occurrence of cyber attacks or if the attacks occurred and should immediately notify it to the Director of National Security Office and the Director of NIS.

The head of local governments and the head of public institutions should take steps to minimize the damage when founding the signs of occurrence of cyber attacks or if the attacks occurred and should immediately notify it to the Director of National Security Office, the Director of NIS and the head of relevant central administrative agencies.

If the Director of NIS find out the signs of occurrence or the outbreak of cyber attacks or is informed the notice, he may ask for taking steps to restore and to prevent from expanding of damage to the head of relevant central administrative agency. The requested heads of relevant central administrative agencies should cooperate to it as long as there is no other special reasons.

c. Accident survey and proceeding[29)]

The Director of NIS may conduct an investigation to analyze the causation of accident occurred by cyber attacks. But, if it is assumed as a minor accident, the head of related agency may conduct own investigation. In this circumstances, the head of related agency should notify the relevant details such as an outline of the accident and measures taken to the Director of NIS.

28) Article 12. of the Cyber Security Management Regulation.
29) Article 13. of the Cyber Security Management Regulation.

After the investigation, if the Director of NIS considers the accident is suspicious of crime, he may notify it to the head of investigative agency under the consultation with the head of relevant agency.

The Director of NIS may form and operate a cyber crisis task force (hereinafter referred as "Task Force") under consultation with the head of relevant central administrative agency if the damage of cyber attacks is critically serious or if a caution-level alert was issued. A necessary subordinate office may be set up under the Task Force to analyze the cyber attacks, accident investigation, emergency response and to recover.

The details relating to the constitution and operation of the subordinate office are prescribed by the Director of NIS under the consultation with the head of relevant central administrative agency. The Director of NIS may request necessary manpower, equipment and related document to the head of relevant central administrative agency for accident investigation and recovery. The Director of NIS shall report the damage caused by a cyber attack and the response of the Task Force to the Director of National Security Office and he shall aggregate them and report to the President.

7. R&D and Education

a. Research and Development[30)]

The Director of NIS may carry forward necessary policies for improvement of level of technology and technology development necessary for a national cyber security.

30) Article 15. of the Cyber Security Management Regulation.

The head of central administrative agency may make incorporated institution responsible for the research and development of national security technology in Electronics and Telecommunications Research Institute establised pursuant to the 1 of article 8 「Act on the Establishment, Operation and Fostering of Government-Funded Science and Technology Research Institutes, etc.」 carry out relevant research and development (including the security control tasks) in order to secure relevant cyber security technology in public sector. The details relating to the research and development of technology necessary for a cyber security shall be prescribed by the Director of NIS.

b. Fostering of manpower and promotion of education[31)]

The head of relevant central administrative agency should devise measures such as securing and fostering of professional cyber security workforce, development and investment of cyber security education programs, and other necessary measures for cultivating of experts, education and promotion, etc. in order to cultivate skilled workforce needed to build an infrastructure of cyber security and to enhance understanding of citizens.

The Director of NIS shall support the measures when the head of relevant central administrative agency requests assistances in fostering of cyber security experts, education and promotion.

31) Article 16. of the Cyber Security Management Regulation.

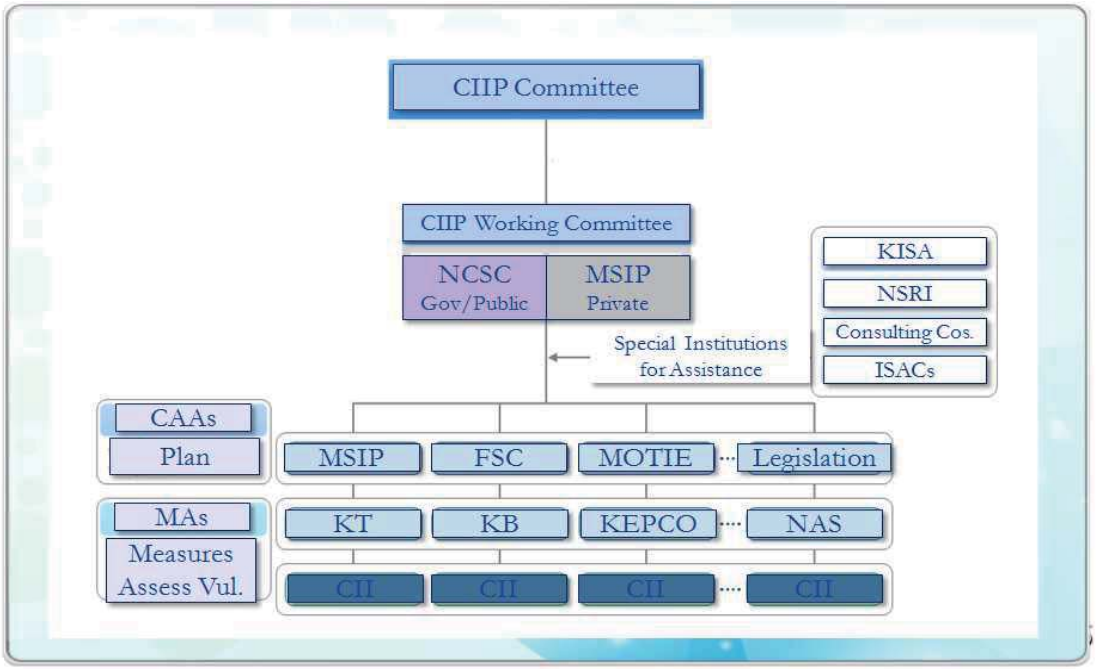
C. Critical Information Infrastructure Protection Act

1. Structure

The Act describes proper protections with pro- and post-measures. As a first step for pro-protection measures, the Act describes a central administrative authority(CAA) has an authority to designate information infrastructures to CIIs operated by management agency(MA)s under its control. A CAA may establish the detailed assessment standards and guidelines for designation and shall deliver these to MAs under its supervision. NCSC and MSIP may recommend a CAA to designate a specific information infrastructure as a CII with the new provision of recommendation for designation.

The second step for pro-protection measures is analysis and evaluation of vulnerabilities. According to CIIP Act, a MA shall analyze and evaluate the vulnerabilities of CIIs under its control on a regular basis. Based on the results from the analysis and evaluation of vulnerabilities, the MA shall establish and implement protection measures. NCSC, MSIP and Ministry of National Defense(MND) may review whether a MA properly implements measures to protect CII or not. A relevant CAA shall establish and implement plans for protecting CII within its authority by integrating and coordinating the measures submitted by the MAs under its supervision. Post-CII protection measures are composed with 3 parts, 1) notification, 2) resilience measures and 3) technical assistance. A MA shall, when it recognizes that the occurrence of intrusion incidents lead to the disturbance, paralysis or destruction of CII under its control, notify relevant administrative authorities and law enforcement authorities of such facts. A MA shall take necessary measures to make resilience and protect CII in a swift

manner when intrusion incidents occur. MAs may also request technical assistant, if it is necessary, to the NCSC, MSIP or specialized institutions prescribed by Presidential Decree.



2. Designation

a. CII

Information Infrastructure means an electronic systems managing and controlling infrastructures related to such sectors as national security, defense, finance, communications, transportation, energy and information and communications network under Article 2 para. 1 subpara. 1 of the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. An information infrastructure shall be a critical information infrastructure after it shall be designated as a CII.

b. Authority for Designation

Protection measures, protection plans and technical assistance described in CIIP Act shall be applied to an information infrastructure, after it shall be designated as a CII. The Act describes a CAA has an authority to designate information infrastructures to CIIs operated by MAs under its control. When a CAA performs the designation, it shall establish its own assessment standard on the designation and make a notice it to the MAs.[32] The Act and the Decree guarantee CAAs to have autonomy in designation of CIIs, because CAAs would be aware of the unique features and specific circumstances related to CIIs under its control.

However CAAs, based on its autonomy in designation of CIIs, would like to designate so many information infrastructures as CIIs, because it could not have enough experts and budgets to identify CIIs among information infrastructures under its control and it would likely to avoid liability from no designation of CIIs. Sometimes CAAs, would not designate or delay the designation, because making compliance with the Act would be burdensome. To prevent surplus designation of CII, the Act makes a process that the Committee shall have a power to make a decision on whether the CAA's designation should be proper or not. To respond no designation or delay, the Act has a provision on the Recommendation for Designation.

c. Standards and Guidelines

A central CAA may designate an information infrastructure operated by a MA under its authority, which is deemed to require protection from

32) Article 8. of the CIIP Act and article 14. of Presidential Decree on the Protection of Information and Communication Infrastructure(Herein after “Presidential Decree”)

electronic intrusions, as a CII.[33] When a CAA designate a CII, it shall take into account these standards; ⅰ) the national and social importance of duties performed by the MA; ⅱ) the agency's dependence on the information infrastructure; ⅲ) the inter-connection with other information infrastructures; ⅳ) the areas and extent of damage caused by intrusion incidents to the national security, economy and society, if any; ⅴ) the probability of intrusion incidents and the easiness of resilience thereof.

A CAA may establish the detailed assessment standards and guidelines for designation and shall deliver these to MAs under its supervision.[34] MAs shall make task force for the performance of the assessment for designation, and the task force shall select designated units and areas of the detailed infrastructure facilities, according to the standards and guidelines.

d. Recommendation for Designation

Although CIIP Act was enacted, CAAs was very reluctant to designate CIIs, because designation would bring a great burden for CAA and MAs to comply requirements and duties described in the Act. In April 2001, 4 CAAs designated 23 facilities as CIIs and in 2002, 5 CAAs designated 66 facilities. A CAA, Ministry of Information and Communication at that time, designated 7 facilities in 2004. In 2005, a CAA, Central Election Commission, designated 1 facility and in 2006 the Ministry of Information and Communication at that time, designated 5 facilities. Because CAAs had their own authority to designate CIIs, based on its own decision, there was no measure to force CAA to make designation. Therefore it

33) Article 8. para. 1. of the CIIP Act.

34) Article 14. para. 1 of the Presidential Decree.

was needed to make proper measures for CAAs to encourage enforce their designation authority.

Under this background, the CIIP Act revised in 2007 to introduce new provision of recommendation for designation. According to the provision, NCSC and MSIP may recommend a CAA to designate a specific information infrastructure as a CII.[35] In that case NCSC and MSIP shall require CAA to submit data on the relevant information infrastructure, when necessary for making a recommendation.[36] When CAAs had received the recommendation for designation, they shall designate CIIs following above designation procedure. In other words, when CAA received the recommendation, it shall make decision on the designation following above designation procedures and notify the result to NCSC or MSPI within 60days.[37] To make a recommendation, NCSC and MSIP shall establish Research Task Force to review the necessity of designation, considering above 5 designation standards.[38] Before making a recommendation, NCSC and MSIP may consult with the MA which operates a specific information infrastructure and CAA supervising the MA.[39] NCSC and MSPI shall describe necessary matters related to establishing and operating the Task Force.[40]

e. Revocation of Designation

When a MA abolishes, suspends or changes its business operations, the related CAA may revoke the designation either ex officio or upon request

35) Article 8-2. para. 1. of the CIIP Act.
36) Article 8-2. para. 2. of the CIIP Act.
37) Article 16-2. para. 3. of the Presidential Decree.
38) Article 16-2. para. 1. of the Presidential Decree.
39) Article 16-2. para. 2. of the Presidential Decree.
40) Article 16-2. para. 4. of the Presidential Decree.

of the MA.[41] When CAA is likely to revoke the designation, it shall submit this for deliberation by the Committee and in such a case, the Committee may hear MA's opinion on the revocation.[42] When the Committee makes an agreement for the revocation, CAA make a notification of the revocation to MAs and publish this in the official gazette. However, CAA may not publicly announce it, after deliberation by the Committee, when necessary for guaranteeing national security.[43] Compared with designation, revocation may be possible when a MA abolishes, suspends or changes its business operations. Therefore it is needed to revise the Act that a revocation shall be happened based on the above 5 designation standards. Furthermore the Act shall be revised to enforce the MA's interest on related to revocation, by describing Committee hearing to be mandatory.[44]

3. Evaluating Vulnerabilities and Establishing Protection Plans

a. Analysis and Evaluation of Vulnerabilities

1) Introduction and period

Because of increasing interdependency combined with greater operational complexity, CIIs have been vulnerable to technical mal functions, malicious human activities and natural disasters as well as new forms of cyber

41) Article 8. para.3. of the CIIP Act.
42) Article 8. para.5. of the CIIP Act.
43) Article 8. para. 6. of the CIIP Act.
44) Jong-hyun, Hong and Young-hyuk, Cho, A Study on the Improvement of the CIIP Act, Korea Legislation Research Institute(2014. 9), p.65.

attacks and terror.[45] Actually vulnerability means a weakness in a system that can potentially be manipulated by an unauthorized entity to allow exposure of some aspect of the system. Cyber attacks and terror against CIIs are likely to be committed through the vulnerabilities. To protect CIIs form unintentional distortion, malfunction and shutdown as a result from the cyber attacks or terror, it is urgently needed to identify vulnerabilities.

In Korea, according to CIIP Act, a MA shall analyze and evaluate the vulnerabilities of CIIs under its control on a regular basis.[46] When an information infrastructure or a facility has been newly designated as a CII, MA, which has operated the CII, shall analyze and evaluate initially the vulnerabilities within 6 months after the designation.[47] If MA does not perform the analysis and evaluation within that period with a reasonable reason, MA, with a permission from CAA, shall perform the analysis and evaluation within 9 months after the designation. After initial analysis and evaluation were performed, MA shall do these with every year period. However, when there would be a critical change in the CII or MA made a decision to perform the analysis and evaluation, MA shall have these without waiting one year.[48] The MA may ask the NSRI, KISA, Information Sharing and Analysis Centers, specific consulting companies to analyze and evaluate vulnerabilities of CII under its control.[49] MSIP shall develop and establish guidelines concerning the analysis and evaluation of vulnerabilities

45) Steven M. Bellovin. Matt Blaze. Sandy Clark and Susan Landau, Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet, Privacy Legal Scholars Conference(June 2013), p.24 (available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2312107, Last visited October 12, 2016).

46) Article 9. para. 1. of the CIIP Act.

47) Article 17. para. 1. of the Presidential Decree

48) Article 17. para. 2. of the Presidential Decree

49) Article 9. para. 3. of the CIIP Act.; Article 12 of Presidential Decree

in consultation with CAA and NCSC, and provide the guideline to the relevant CAA.[50]

2) Measures and process

In case of performing the analysis and evaluation of vulnerabilities, MA shall establish a task force.[51] To assure objectiveness and effectiveness in analysis and assessment, the task force shall be composed of managing and operating staffs of the CII and information security experts,[52] but the chief of task force shall be the CISO of the MA. The task force shall establish a "plan for analysis and evaluation of vulnerabilities" including performance method of the analysis and evaluation of vulnerabilities, review items, process, period and budgets according to the above guideline, and perform the analysis and evaluation of vulnerabilities after reporting the plan to head of MA. The T/F shall define areas and categories of the analysis and evaluation of vulnerabilities, after looking at the composition and business operation of CII. In doing this, the T/F shall divide and select detailed infrastructures and facilities in the CII, such as physical assets, software, data, personal assets, and virtual assets. Then T/F shall identify composition map and items of the CII, and develop priorities among them based on their importance and valuation in the CII. T/F shall also identify risks and threats which have actually happened or any possibility to happen. T/F shall analyze each risks and threats' cause and frequency, and effects when the intrusion or cyber incidents arise. The T/F shall identify risk points and vulnerabilities, and shall develop vulnerabilities review list. The T/F shall also assure and analyze that

50) Article 9. para. 4. of the CIIP Act
51) Article 9. para. 2. of the CIIP Act
52) Article 18. para. 1 of the Presidential Decree

vulnerability should exist or what is the degree of each vulnerability. T/F shall detect the selected vulnerabilities using 'vulnerability detect tool' retained by MA or developed by information security assistant organizations, KISA, ISACs, specific consulting companies and NSRI.[53] In addition to use the tool, the T/F shall analyze vulnerabilities in personal, physical and managerial security structures of the MA. T/F shall review the existed Protection Measures established by MA should be appropriate and effective. T/F shall evaluate relation between risks and vulnerabilities, possibility of cyber attacks and intrusion incidents, effectiveness against MA when cyber attacks and intrusion incidents arise, protection measures to be newly needed or reinforced, economic efficiency and correlation with the existed Protection Measures. MA may permit information security assistant organizations to perform the analysis and evaluation of vulnerabilities.[54] In this case, MA may not establish the task force.[55] Based on the analysis and evaluation of vulnerabilities, performed by the T/F or the information security assistant organization, MA shall develop and establish most effective protection measure, and specifically enforce and realize it.

b. Protection Measures

1) protection measures

Considering the results from the analysis and evaluation of vulnerabilities, the MA shall establish and implement protection measures, including physical and technological measures to protect the CII.[56] Protection

53) Article 12. of the Presidential Decree

54) Article 9. para. 3. of the CIIP Act.; Article 12, Article 18. para. 2. and 3. of the Presidential Decree.

55) Article 9. para. 3. of the CIIP Act.

56) Article 5. para. 1. of the CIIP Act.

measures established and developed by MA shall be submitted annually to CAA until at the end of August.[57] When the MA establishes the measures, it shall submit details of such measures to a CAA which supervises the agency.[58] Protection Measures shall be established by MA with its own decision based on the results from the analysis and evaluation of vulnerabilities. The measures shall be the fundamental and valuable materials necessary for establishing Protection Plans, developed by CAAs. Because Protection measures shall include technical measures and physical protection measures, not only virtual but also physical assets and facilities can be designated to CII.

2) Reviewing Protection Measures

Although the CIIP Act describes protection measures established by MA with its own decision, the Act has not any provisions related to inspect or review the performance or enforcement of the measures. This could lead the protection measures to be practically meanness. To solve these problem, Korean government amended the Act in 2007 introducing a provision under which NCSC, MSIP and MND may review whether a MA properly implements measures to protect CII or not.[59] They may notify the result of reviewing protection measures to relevant CAA.[60] They may request the relevant CAA to submit data, including details of measures to protect CII submitted by a MA, when it is necessary for reviewing.[61] The NCSC, MSIP and MND are in charge of reviewing protection measures implemented by MAs. MAs which belong to public

57) Article 8. of the Presidential Decree
58) Article 5. para..2. of the CIIP Act.
59) Article 5-2. para. 1. of the CIIP Act.; Article 9-2 of the Presidential Decree.
60) Article 5-2. para. 3. of the CIIP Act.
61) Article 5-2. para. 2. of the CIIP Act.

and governmental sector shall be reviewed by NCSC, MAs in private sector shall be reviewed by MSIP, and MAs in military sector shall be reviewed by MND.[62]

When NCSC, MSIP and MND start to the reviewing, they shall consult in advance with related CAA on the procedures of reviewing, and make a notice to MA about the reviewing procedure.[63] They also ask assistance for information security assistant organizations when it is necessary for reviewing the measures.[64] Detailed guidelines for the reviewing shall be defined by the consult between NCSC and MISP. NCSC, MISP and MND shall make a report on the result of reviewing to the Committee.[65] NCSC, MISP and MND shall recommend for MA to have improvements on its protection measures, which is likely to be necessary for complementary measures.[66] NCSC and MISP shall reflect the result of reviewing to the guidelines for next year's protection measures and protection plans.[67] NCSC and MISP shall share the results with each other to make efficient assistances for CIIP.[68]

c. Protection Plans

A relevant CAA shall establish and implement plans for protecting CII within its authority by integrating and coordinating the measures submitted by the MAs under its supervision.[69] It shall submit details on outcomes

62) Article 9-2. para. 2. of the Presidential Decree.
63) Article 9-2. para. 3. of the Presidential Decree.
64) Article 9-2. para. 4. of the Presidential Decree.
65) Article 9-3. para. 1. of the Presidential Decree.
66) Article 9-3. para. 2. of the Presidential Decree.
67) Article 9-3. para. 3. of the Presidential Decree.
68) Article 9-3. para. 4. of the Presidential Decree.
69) Article 6. para. 1. of the CIIP Act.

of implementing plans for protecting CII of the previous year and plans for the following year to the Committee for its deliberation.[70] Protection plans shall include ⅰ) matters concerning the analysis and the evaluation of vulnerabilities of CII; ⅱ) matters concerning prevention against intrusion incidents against CII and measures for the resilience thereof; ⅲ) other necessary matters concerning the protection of CII.[71]

4. Responding Cyber Incidents

a. Notification

A MA shall, when it recognizes that the occurrence of intrusion incidents lead to the disturbance, paralysis or destruction of CII under its control, notify relevant administrative authorities and law enforcement authorities of such facts. In these cases, the authorities shall take necessary steps to cut off spreading damage caused by intrusion incidents and respond urgently to such incidents.[72] The Government may provide governmental budget support, including costs incurred in recovering damage, to a MA that has contributed to preventing the spread of damage by notifying intrusion incidents.[73]

b. Resilience Measures

A MA shall take necessary measures to make resilience and protect CII in a swift manner when intrusion incidents occur.[74] It may request a

70) Article 6. para. 2. of the CIIP Act.
71) Article 6. para. 3. of the CIIP Act.
72) Article 13. para. 1. of the CIIP Act.
73) Article 13. para. 2. of the CIIP Act.
74) Article 14. para. 1. of the CIIP Act.

relevant CAA to provide assistance when it is necessary for taking measures for resilience and protection.[75] However, these assistances, shall not apply to cases for technical assistance for protection of specific CIIs.[76] The CAA provides necessary assistance for the resilience from damage, such as technological assistance, and takes appropriate measures to prevent the spread of damage.[77]

c. Technical Assistance

MAs may also request technical assistant, if it is necessary, to the NCSC, MSIP or specialized institutions prescribed by Presidential Decre e.[78] They may also ask a technical assistant when they would have an order from the Committee to review their CIIs because the CIIs would be likely to cause harm to national security or the economy and the society as a whole.[79] Technological assistances shall be ⅰ) formulation of measures to protect CII; ⅱ) prevention of intrusion incidents against CII and the resilience thereof; ⅲ) compliance with an order or recommendation for specific protection measures.[80] When a MA has a specific CII which would significantly influence on national security, it does not request for technological assistance to other institutions without asking for NCSC to have the first assistance.[81] A specific CII shall be one of the ⅰ) critical transportation facilities, such as roads, railroads, subways, airports and harbors; ⅱ) facilities for water resources and

75) Article 14. para. 2. of the CIIP Act.
76) Id.
77) Article 14. para. 3. of the CIIP Act.
78) Article 7. para. 1. of the CIIP Act.
79) Id.
80) Id.
81) Article 7. para. 2. of the CIIP Act.

energy, including electricity, gas and oil; iii) relay broadcast facilities and the national command control communication network; iv) research facilities of government-funded research institutes related to nuclear energy, the national defense and science, or advanced defense industry.[82] However, NCSC may provide technical assistance without any request from the MA, in consultation with the relevant CAAs, in cases where a substantial and imminent threat to national security exists and it is impossible to recover from damage if it waits for a MA's request.[83] However, NCSC shall not provide a technological assistance to any information infrastructure which has personal information.[84]

5. Penalty

a. Prohibited Commitments

Accessing CII by any person who has no access authority, or manipulating, destroying, concealing or leaking stored data by any person who exceeds his/her access authority; destroying the data of CII, or using programs, such as computer viruses and logic bombs, with the intention of obstructing the operation of CII; abruptly sending large amounts of signals with the intention of obstructing the operation of CII, or causing a fallacy in information processing by means, such as inducing the processing of a wrong order.[85]

Any person who disturbs, paralyzes or destroys CII, by doing above commitments, shall be punished by imprisonment with labor for not more

82) Id.
83) Id.
84) Article 7. para. 2. of the CIIP Act.
85) Article 12. of the CIIP Act.

than 10 years or by a fine not exceeding 100 million won. Any person who has attempted to above commitments shall be also subject to the punishment.[86]

b. Disclosing Confidential Information

A person, who is or has been employed following institutions, shall not disclose any confidential information obtained in the course of his or her performance of duties. The Committee organization in charge of the analysis and evaluation of the vulnerabilities of CII, relevant organizations which perform duties related to the acceptance of notification of intrusion incidents and resilience measures, information sharing and analysis center.[87]

Any person who discloses any confidential information, in violation of above, shall be punished by imprisonment with labor for not more than five years, by suspension of qualifications for not more than ten years or by a fine not exceeding 50 million won.[88]

D. Act on Measures for the Protection of Nuclear Facilities, etc. and Prevention of Radiation Disasters

1. Protect Nuclear Power Plants from Cyber Attack

Along with the technical development of computer and network systems, cyber threat and attacks against nuclear power plant have also increased. Nuclear digital system is in nature different from general information and

86) Article 28. of the CIIP Act.
87) Article 27. of the CIIP Act.
88) Article 29. of the CIIP Act.

telecommunication systems. It shall be need to response simultaneously within an order time serviced by 24hours and 7days with 30 to 40 years. Cyber attacks against nuclear power plants may cause huge damages not only human beings but also whole livings and environmental damages. Therefore comprehensive security measures shall be established in considering system life cycle, physical protection and work process. The measures shall include security measures for system developers, system maintain staffs, third party contractor and inside workers.

Protecting energy infrastructures from the cyber attacks shall be enforced by the measures, plans and responding processes described in the Act. Before the cyber attacks on nuclear power plants happened in last winter season, main issues on nuclear energy infrastructure were checking and reviewing safety operation of nuclear power plant, and appropriation of prolonging old nuclear power plant reactor's operation. However, after the cyber attacks, Korean society has requested establishing more profound and specific measures to protect nuclear energy infrastructure from cyber attacks. Following these requests, legislators of National Assembly in Korea, have proposed many bills to amend “the Act on measures for the Protection of Nuclear Facilities, etc. and Prevention of Radiation Disasters (herein after “Nuclear Protection and Prevention Act”)”.

2. Systems and Networks in Nuclear Power Plants

Nuclear power plants shall usually have developed 3 levels of systems and networks such as 1) internet network, 2) intra network and 3) independently blocked network. As the internet and intra network are separated, workers and staffs shall have a work only within the intra

network. When they want to access with internet they shall use only internet network separated from intranet work. This cause several inefficiency and inconvenient but it shall be helpful to increase security. Intra network shall be connected with the independently blocked network controlling nuclear reactor, turbine control system, main computers and operating computers, however the independently blocked network shall transfer only simple operation information to intra network. Therefore it can be said that in fact the independently blocked network closed to intra networks.

3. NSSC

In Korea two major Acts, 1) Nuclear Safety Act and 2) Nuclear Protection and Prevention Act, have regulated security issues against nuclear power plants. The purpose of the Nuclear Safety Act is to provide for matters concerning safety managements in research, development, production, use, etc. of nuclear energy, in order to ensure the prevention of disasters resulting from radiation and to contribute to public safety. The purpose of Nuclear Safety Act is to ensure safety and trustfulness of the nuclear energy, it shall not include regulation against cyber security issues related to nuclear power facilities.

However the purpose of the Nuclear Protection and Prevention Act is to strengthen the protection system of nuclear facilities to guard against an increase of the number of nuclear facilities or new threats such as terror and sabotage, and to establish legal and institutional frameworks for an efficient radiation disaster management system. According to this Act, guidelines and regulations controlling illegal transfer of nuclear materials and sabotage by cyber attacks shall be presented and regulated.

Nuclear Safety and Security Commission (herein after "NSSC") shall be established directly under Prime Minister, as a central government organization and it shall be composed of 9 commissioners including 1 chairperson who shall be the standing member of the commission after being appointed with the consent of the National Assembly. NSSC shall 1) secure the highest level of nuclear safety, 2) protect nuclear facilities from both internal and external threats, such as terrorism, 3) strengthen emergency system for any nuclear emergency or accidents, and 4) comply with international standards for the peaceful use of nuclear energy.[89]

Every nuclear business operator shall obtain approval from NSSC for the 3 following matters: ⅰ) Physical protection facilities and installations for "Protection against the illicit transfer of nuclear materials", "Measures to locate and collect lost or stolen nuclear materials", "Prevention of sabotaging nuclear facilities, etc.", and "Measures against radiological effects resulting from sabotaging nuclear facilities, ect.,[90] ⅱ) Regulations for the physical protection of nuclear facilities, etc. (hereinafter referred to as "physical protection regulations"), ⅲ) Plans for measures against the illicit transfer of nuclear materials and threats to nuclear facilities, etc. (hereinafter referred to as "protection emergency plan").[91] When an operator wants a slight alternation described by Prime Minister's Regulation, he or she shall file an alternation report to NSSC. Cyber security matters shall be included into the each above 3 matters. Physical protection of nuclear facilities operated by nuclear business operator shall be under inspection of NSSC.[92]

89) http://nssc.go.kr/nssc/en/c1/sub1.jsp(Last visited October 12, 2016)
90) Article 3. para. 2. of the Nuclear Protection and Prevention Act.
91) Article 9. of the Nuclear Protection and Prevention Act.
92) Article 12. para. 1. of the Nuclear Protection and Prevention Act.

When NSSC found certain results such as violation of physical protection regulation and insufficient emergency protection measures by the operators under the inspection, NSSC shall order the nuclear business operator to correct them.[93] NSSC also shall assess the threats against nuclear facilities and establish design based threat with every 3 years to implement physical protection measures.[94]

4. Structures

The Korea Institute of Nuclear Nonproliferation and Control (hereinafter referred to as "KINAC") shall be established in order to take steps to ensure the safeguard of nuclear energy facilities and nuclear materials and to efficiently perform the work of controlling the import and export of the nuclear materials.[95]

KINAC shall 1) conduct regulatory work on nuclear material accounting and control, 2) implement a comprehensive safeguards agreement (CSA), the additional protocol(AP) and other relevant activities, 3) implement Import & Export control governing nuclear materials and related technologies, 4) review and Inspect the physical protection status of nuclear material and facilities, 5) cooperate with the International community with regard to nuclear nonproliferation and nuclear security, 6) train, Educate and Conduct R&D activities in the area of nuclear nonproliferation and nuclear security, 7) analyze the nuclear activities of North Korea and neighboring countries, and 8) develop nuclear nonproliferation and security policies.[96]

---

93) Article 12. para. 2. of the Nuclear Protection and Prevention Act.
94) Article 7. of the Presidential Decree of the Nuclear Protection and Prevention Act.
95) Article 6. the Nuclear Safety Act
96) http://www.kinac.re.kr:8181/eng/about/about2_3.do(Last visited October 12, 2016)

NSSC shall entrust 1) threat assessment, 2) review for the approval for above "physical protection facilities and installations", "physical protection regulations" and "protection emergency plan", and 3) inspections on physical protection, to KINAC.[97] Based on the entrustment of the NSSC, KINAC has developed standards on cyber security on nuclear power facilities. Especially after recent cyber attacks and hacking against nuclear power plant, KINAC has published KINAC/RS-015.

5. KINAC/RS-015

a. Purpose and Target

The KINAC/RS-015 is to establish efficient prevention, detention, response system against cyber attacks, and minimize effects and results of cyber attacks which seek to sabotage on nuclear facilities and illegal transportation of nuclear materials.

KINAC/RS-015 shall have be applied to Critical Digital Assets (CDAs) which implements Safety, Security, Emergency Preparedness(SSEP) functions and makes effects on SSEP functions when cyber attacks happen. To prevent and protect illegal transfer of nuclear materials, KINAC/RS-015 shall be applied to security networks, composed of access control system, and computers and servers covering intrusion detection system. KINAC/RS-015 shall be also applied to control networks, composed of reactor control system, detection system, protection system, technical safety system, and computers, servers, PLC and DCS in diversity system.

97) Article 7. of the Presidential Decree of the Nuclear Protection and Prevention Act

b. Main Contents

First, nuclear business operators shall make a cyber security team(CST) which shall be independent and separated from operation. They also shall describe explicitly role and liabilities of the each team members. Second they shall identify critical digital assets. Before identifying CDAs, they shall identify critical systems by doing initial consequence analysis which shall be applied to whole operating systems, communication systems, networks and support systems in nuclear power plant, deciding critical systems which would conduct adverse impact against SSEP. They shall identify critical systems which have implemented SSEP functions or SSEP functions would have defended on, or made adverse impacts on implement of SSEP functions. When a system has provided a way of access process or assist necessity system, it shall be a critical system. When a system has not implemented these functions and there is no need to protect the system as a necessity it shall not be a necessity system.

Second nuclear operators shall identify CDAs. CDA shall be a component of critical system, which shall protect critical systems when cyber attacks happened, or shall be connected with critical system directly or indirectly. Digital assets which shall 1) implement SSEP functions, 2) make adverse impacts or would make adverse impact against critical system doing SSEP function or CDAs, 3) digital assets which supply access way for critical system doing SSEP or CDAs, 4) digital assets which support critical system or CDAs, 5) CDAs which shall protect above systems from cyber attacks defined in design based threats.

Third they shall establish a Defense-in-Depth strategy. Under this strategy they shall make classifications with cyber security degrees to protect code

digital assets. The cyber security degrees are composed of level 1 to level 4, and transfer among the levels shall be controlled.

Forth they shall apply 101 cyber security measures to core digital assets. These cyber security measures are composed of technical, operational and management security measures. Technical security measures shall be composed of access control, supervision and liability, security on systems and telecommunications, user identification and certification, system enhancements such as patch. Operational security measures shall be composed of controlling media, personal security, enhancing confidentiality of system and information, maintenance, physical and environmental security, protection strategy and responding incidents. Preparing emergence plan, training and education shall be also composing operational security measures. Supply network control, security design, development and acceptance test, and managing vulnerabilities shall belong to maintenance security measures.

Finally nuclear business operators shall maintain and sustain the cyber security programs with sustainable detection and assessment, and analyzing vulnerabilities. To maintain cyber security program, the operators shall establish cyber security program, integrate it, maintain continuously, review security program, change control when necessary, and record retentions.

Ⅳ. Legislations related with Enhancing Cyber Security Industry, Securing Electronic Financial Transaction and Protecting Personal Information

A. Cyber Security Industry Enhancement Act

1. Policies and Initiatives

Announcing the plan to facilitate investment on cyber security in 2014, road map of Internet of Things(IoT) followed by the comprehensive measures to develop cyber security industry 2013, the government plans to expand national cyber security market estimating currently worth of 7trillion won(about $620 billion) to twice by 2017 so as to facilitate of cyber security investment, to develop world's top 10 cyber security products, and to enhance IoT security industrial competitiveness.

In particular, the government decided to carry gradually out four major annual strategies with the 'Ministry of Science, Information and Communications Technology and Future Planning(MSIP)' to develop cyber security industry: Expansion of demand and creation of new market, enhancement of competitiveness of the original core technology, systematic foster of cyber security experts and promotion of global cyber security company. The government also decide to conduct four plans to facilitate cyber security investment by 2017: to build an environment of cyber security investment in private sector; to expand budget related to cyber security in public sector; to promote cyber security industry; to grow human resources specialized in cyber security focusing on the field needs; and to strengthen cyber threat response system. The Korean cyber security industry strengthened

its competitiveness through a rapid progress and its exports are growing every year. It is expected that its proportion in the whole IT industry will surge with the high technology development in the future.

Following the Comprehensive Measures to enhance National Cyber Security, Korean policy makers and legislators heard many voices from individuals, vendors, and governmental institutes agencies, cyber security industry shall be encouraged to support robust cyber security activities with best technologies. Hence, Cyber Security Industry Enhancement Act was newly enacted by National Assembly in Jun. 22, 2015 and it was effected since Dec. 23, 2015.

2. Overview the Act

The Government recognized the necessary of promoting cyber security industry strategically to response actively to cyber attacks, cyber threats, new kinds of cyber finance crime etc. and to create new added values and to discover a growth industry. As enacted the 「Cyber Security Industry Enhancement Act」 (hereinafter "CSIEA")) based on the recognition, the government is able to start a business directly supporting a development of cyber security industry.[98)]

The CSIEA provides a standard as to a fair return for cyber security services continuously requested by the cyber security industry. It also recommends an use of standard contract form and provides civil-government joint monitoring system to reform unreasonable order practices. Furthermore, it provides registration requirements of assessment institution to conduct 'preparedness evaluation' which rates the level as to efforts of company preparing the cyber security such as human resources management system.

98) http://www.datanet.co.kr/news/articleView.html?idxno=95670(Last visited October 12, 2016)

To be registered as a preparedness assessment institution, it should found a professional evaluation body, and have workforce to carry out an evaluation, and retain evaluating technology and so on. It also prescribes three years expiration date of registration for an assessment institution.

In addition, it provides to make quinquennial 'cyber security industry promotion plans' to create the foundation for the systematic cyber security industry promotion and to facilitate cyber security technology development, fostering of experts, creation of new blending markets and supporting the overseas expansion. Moreover, it appoints a technology shown novelty, creativity, and availability of business as an outstanding technology to promote a cyber security core technology development and supports manufacturing and exports expenses. It also makes enable to support international cooperations, performance evaluation by evaluating the rate of company's growth, the results of technology development, cyber security experts, the contribution to job creation etc.

3. Major Contents

The purpose of this act is to contribute to creating robust information communication environment and development of national economy creating the base of data protect industry and strengthening its competitiveness by prescribing the necessary matters in cyber security industry promotion.[99] The government and local governments should set up and implement a required policy to enhance cyber security industry and make plan to secure necessary funds.[100] The Minister of MSIP should establish and implement cyber security industry promotion plan to make the purpose of

99) Article 1. of the CSIEA
100) Article 2. of the CSIEA

policy and direction as to the cyber security industry promotion.[101] The head of administrative agency or the head of public agency (hereinafter referring to as public agencies) should annually submit the purchase demand information for cyber security technology etc. to the Minister of MSIP to enhance the level of cyber security of their agencies.[102] The Minister of MSIP may provide the purchase demand information to the cyber security company.[103]

If the head of public agencies make a business contract to build cyber security system, he should first apply the manner which the bidder complying with Article 10. para 2 and 3 of 「the Act on Contracts to Which the State is a Party」 and the article13, para 2 and 4 of 「the Act on Contracts to Which a Local Government is a Party」 makes as the successful bidder. However, when it needs to contract with other methods for the character of cyber security system, it may contract otherwise.[104] The Minister of MSIP may decide the criteria to analyze and to apply the requirement of cyber security system and a technological assesment standard to select the company or person of cyber security system business.[105] The cyber security company should be previously approved in writing by the head of public agencies respectively when it contracts with the public agencies to establish cyber security system and it can contract out the whole or part of the business to other cyber security company or the sub-contractor can again subcontract the whole or part of the business to other company.[106]

---

101) Article 5. para. 1. of the CSIEA
102) Article 6. para. 1. of the CSIEA
103) Article 6. para. 2. of the CSIEA
104) Article 7. para. 1. of the CSIEA
105) Article 7. para. 2. of the CSIEA
106) Article 8. of the CSIEA

The cyber security company making contracts with the public policies to establish cyber security system has a warranty liability for the defects occurred within one year from the business complete date (the day on which the final outputs were delivered after testing and examination on the projects).[107)]

Nevertheless the condition of para 1, the cyber security company has no warranty liability on the following; ⅰ) the quality or standards of goods provided by employer are under the criteria;

ⅱ) cyber security system is built as the employer's instruction; and

ⅲ) defects are occurred by employer's malice or negligence otherwise.

However, the company shall take the liability if it does not notice it to employer even though the company knows the goods provided by employer or the instruction of employer is inappropriate.[108)]

The public agencies should make effort to pay reasonable and fair price to develop a cyber security industry and to ensure the quality of cyber security goods and services when they enter into a contract of cyber security business.[109)] The Minister of MSIP may inspect with civil-government joint monitoring and disclose the outcomes or request the correction to the employer to establish a reasonable order practice, if the employer; ⅰ) breaches the law relating to the order of the cyber security business or breaches other regulations; or ⅱ) demands a long-term maintenance and management and to maintain security with unreasonably low cost compare to the normal transaction practice.[110)] The Minister of MSIP shall make a standard contract form through consultation with the

107) Article 9. para. 1. of the CSIEA
108) Article 9. para. 2. of the CSIEA
109) Article 10. para. 1. of the CSIEA
110) Article 10. para. 2. of the CSIEA

Fair Trade Commission for a rational distribution and fair transaction of cyber security industry and may consult public agencies about using it.[111]

In order to develop cyber security technology and to promote investment, the Minister of MSIP may conduct businesses; ⅰ) survey on the level of cyber security technology and research and development of basic technology ; ⅱ) discover and develop the original core technology of cyber security in a prospective field; ⅲ) develop and support an international joint research as to cyber security technology; ⅳ) commercialize the cyber security technology and set up a cluster of local cyber security industry; ⅴ) joint research of Industry, academy and institution in cyber security technology support project; ⅵ) cyber security technology transaction activate business; or ⅶ) necessary business to develop of cyber security technology and to promote investment etc.[112]

To grow professional workforce demanded on the promotion of cyber security industry, the Minister of MSIP consulting with the head of central administrative agencies may make and enact necessary policies; ⅰ) Understanding of the demand of professional workforce and establishing a long-term supply-demand plan, ⅱ) Designation of experts education and training institutions, establishment and assistance; ⅲ) Improvement of experts education program and supply support; ⅳ) Set up a certification system related to the cyber security industry and professional workforce supply support; ⅴ) Support education as to cyber security industry in various levels of schools and other educational institutions; 6) other matters relating to fostering of experts decided by the presidential decree. and so on.[113]

111) Article 10. para. 3. of the CSIEA
112) Article 14. para. 1. of the CSIEA
113) Article 15. para. 1. of the CSIEA

The Minister of MSIP shall find out the international trends relating to cyber security industry and may enhance international cooperation.[114)]

The Minister of MSIP may conduct a performance evaluation as to cyber security products in order to ensure quality of cyber security products, to promote distribution, to protect users and to activate the convergence industry. The Minister of MSIP may appoint an assessment institution to professionally conduct the performance evaluation.[115)]

The Minister of MSIP may assist outstanding cyber security technology appointed every year as decided by the presidential decree to promote cyber security industry.[116)] The Minister of MSIP may assist an outstanding cyber security company contributing to the promotion of cyber security industry with developing and commercializing the outstanding cyber security technology.[117)]

If it is necessary to promote cyber security industry, the Minister of MSIP may offer a long-term low interest loans to cyber security company; 1) Funds needed to install, transfer, alter, supplement or expand of cyber security products and services 2) Funds needed to purchase and to reserve the raw materials, 3) Development funds for localization of cyber security products and services, 4) Funds for export of cyber security products and services, 5) Funds needed to develop a main cyber security technology and components, 6) Funds for R&D and the maintenance of idle facilities; and, 7) other funds for operation of cyber security industry.

If it is required to promote exports in cyber security industry, the Minister of MSIP may take necessary action to promote investment in

114) Article 16. para. 1..of the CSIEA
115) Article 17. of the CSIEA
116) Article 18. para. 1. of the CSIEA
117) Article 19. para. 1. of the CSIEA

cyber security industry and to expand exports market according to the presidential decree.[118]

To promote cyber security industry, the government may take necessary measures such as tax deduction according to the Restriction of Special Taxation Act, the Restriction of Special Local Taxation Act and the related taxation act.[119] According to the Presidential Decree, the government may provide financial support or other necessary supports in order to develop cyber security industry and to expand investment and to facilitate SMEs of cyber security.[120]

4. Cyber Security Service Enterprise

Intellectual data security consulting special agency designation system which has been carried out since 2001 has changed to cyber security professional service enterprise by the cyber security Industry Promotion Act. According to the act, the Minister of MSIP may appoint a person recognized as being capable to conduct tasks (as below) as a cyber security specialized enterprise; ⅰ) a task to analyze and assess the vulnerability of major IT infrastructure specified by the article 8 of Critical Information Infrastructure Protection Act, ⅱ) a task to make measures to protect major IT infrastructure; and ⅲ) a task specified by presidential decree related to cyber security services[121]

In other words, this system is to provide high quality cyber security services by appointing private agency holding speciality and credibility in

118) Article 20. of the CSIEA
119) Article 21. para. 1. of the CSIEA
120) Article 21. para. 2. of the CSIEA
121) Article 23. para. 1. of the CSIEA

cyber security consulting field so as to support the task of analyzing vulnerability in major IT infrastructure and establishing of protection measures.

This system is based on the Critical Information Infrastructure Protection Act and the Cyber security Industry Promotion Act. The details as to the assessment criteria, process and manners etc. will be involved in the relevant notification.

Lately as growing the cyber threats like hacking, the period of analysis report as to the expansion and vulnerability of major IT infrastructure is shortened from biennial to annual analysis. Concerning the trends, the MSIP made a plan to improve service quality through enhancement and expansion of cyber security professional service enterprise appointment system and to activate markets. As a result, it amended the relevant laws in 2013.

First of all, it held a public hearing in September 2012 to review a part amendment bill on the enforcement regulation of the Information and Communications Technology Industry Promotion Act, and went through acceptance of opinions such as legislative notice in November. In 19 Feb. 2013, the amended Enforcement Regulation on the Information and Communications Technology Industry Promotion Act was promulgated. The amended regulation came into force in 20 May 2013. The contents of the amended regulations is, currently, transferred to the cyber security Industry Promotion Act.

In addition by the amendment of Notification No. 2013-176 of the MSIP in 15 November 2013, as a way of market invigoration the requirement to be the cyber security professional service company was eased. As a

result it lowered the barrier to entry for the start-up company intending to be a cyber security professional services company.

When the Minister of MSIP appoints the cyber security professional service company, he should publish it in the official gazette over 20 days. To appoint the company it must go through unassembled test, onsite practice, and comprehensive review.

It absolutely requires strict screening and management as the cyber security professional service company examine major IT infrastructure affecting significantly on a national security, a daily life and economic stability when cyber attacks occur.

The Minister of MSIP conducts oversight every year whether the company complies with the requirements and duties specified on the law.

If the company was appointed by the improper way like deception or was not met the criteria or caused malfunction of the major IT infrastructure by misusing or abusing the data, the government could cancel the appointment pursuant to the article 23 para 6 of the cyber security Industry Promotion Act or order the part or the whole of business suspension within three months.

On the other hand, after the appointment, if there has been changed the important matters such as the representative or executive of corporation, paid-in capital, technology workforce or cyber security management regulation etc., the cyber security professional service company should report it to the Minister of MSIP by submitting relevant documents within one month.

5. Expectancy Effects

The government proclaimed the bill of enforcement ordinance and enforcement regulation of the cyber security Industry Promotion Act on

December 2015. It also provides the promotion development of cyber security core original technology through financial support to the appointed company on expense for technology development. By enactment laws, regulations and orders it strengthen industrial virtuous circle ecosystem creating cyber security market on the demand side while it will build a base of systematic cyber security industry promotion on the supply side. At the end we look forward to the growth of industry from the various convergence area to the creation of security service as well as increasing the employment and the development of the cyber security industry.

B. Electronic Financial Transaction Act

1. Introduction

Nowadays the digital era comes and spreads out to all aspects of our lives with the development of the IT technology. It has merits and demerits because of its convenience and immediacy. Especially, the importance and practical use of electronic financial transaction has increased gradually so that we cannot live without the application of electronic financial transaction today - if not, it would cause many bothering and inconvenient troubles.

However, the continuous and persistent efforts to establish and elaborate the information and communication network system have been threatened by electronic intrusions such as hacking, computer viruses, logic or email bombs, DDos, or e-pulses, etc. Especially the electronic financial transaction are often to be the target area of hackers because the electronic intrusion on the banking system may result in the chaos and turmoil as well as the unjust pecuniary profit.

The intrusion on the electronic financial not only brings about the legal problems between the financial company and consumers, but the national problems as mentioned above. Thus, the 「Electronic Financial Transactions Act(herein after "EFTA")」 was enacted as the Act No. 7929 in Apr. 28, 2006. The purpose of this Act is to ensure the safety and reliability of electronic financial transactions by clarifying their legal relations and to promote financial conveniences for people and contribute to national economic development by creating a foundation for the sound development of the electronic financial industry.

2. Scope and Terms

a. Concept of electronic financial transaction

Ideally, the electronic financial transaction consists of electronic fund transfer which means transaction of funds with the help of electronic apparatus, electronic money transfer, electronic pre-paid payment and mobile payment etc. altogether.[122] It might be defined as the financial (bank, credits, securities and insurance etc.) transaction by means of electronic apparatus.

However, the act tells apart the electronic financial transaction from the electronic payment transaction. The former means any transaction whereby a financial company or an electronic financial business entity provides financial products and services through electronic apparatus and users use them in a non-facing and automated manner without any direct contact

122) The "electronic payment means" is an electronic funds transfer, electronic debit payment means, electronic prepayment means, electronic currency, a credit card, an electronic bond or other means of payment by electronic means.

with employees of the financial company or electronic financial business entity. The latter means any electronic financial transaction whereby a person providing a payment requires a financial company or an electronic financial business entity to transfer money to another person receiving the payment by electronic payment means.

With this the two key-words “financial company” and “electronic financial business entity” are very important to decide whether this act may be applied to or not. First, the term “financial company” means any of the following institutions, organizations or business entities: (a) An institution referred to in subparagraphs 1 through 5, 7 and 8 of Article 38 of the 「Act on the Establishment, etc. of Financial Services Commission」; (b) A specialized credit financial company established under the 「Specialized Credit Finance Business Act」; (c) A postal service agency under the 「Postal Savings and Insurance Act」; (d) A community credit cooperative and Korean Federation of Community Credit Cooperatives established under the 「Community Credit Cooperatives Act」; (e) Any other person prescribed by Presidential Decree, which is an institution, organization, or a business entity carrying on financial business and other finance-related business pursuant to Acts.[123] Second, The term “electronic financial business entity” means any person who has obtained permission or whose business has been registered (excluding any financial company) pursuant to Article 28.[124] It stipulates various types of electronic financial transaction – ⅰ) electronic funds transfer services; ⅱ) issuance and management of electronic debit payment means; ⅲ) issuance and

123) Article 2. subpara. 3. of the EFTA.
124) Article 2. subpara. 4. of the EFTA.

management of electronic prepayment means; ⅳ) electronic payment settlement agency services etc.[125)]

The counterpart of this "financial company" and "electronic financial business entity" is defined as "user" which means any person who conducts an electronic financial transaction under a contract concluded with a financial company or an electronic financial business entity for facilitating electronic financial transactions.[126)]

b. Main terms of the Act

Besides, the electronic financial transaction is mainly characterized with some special ways to transact and contract. First, it should be through electronic apparatus means any apparatus used to transmit or process electronic financial transaction information by electronic means, such as a cash dispenser, automatic teller machine, debit terminal, computer, telephone, or other devices that transmit or process information by electronic means.[127)]

Second, the "transaction request" is very important because it means any request whereby a user asks a financial company or an electronic financial business entity to process electronic financial transactions pursuant to the electronic financial transaction contract. It enables the automated contract which is implemented without face-to-face authentication. Therefore, the public certification is very important to ensure the safety and reliability of electronic financial transactions.

Third, the "means of access" means any of the following means or information which is used to issue a transaction request in electronic financial transactions or to secure the authenticity and accuracy of users

125) Article 28. para. 2. of the EFTA.
126) Article 2. subpara. 7. of the EFTA.
127) Article 2. subpara. 1. of the EFTA.

and the details of such transaction.[128] There are five concrete means of access allowed and specified to enable the electronic financial transaction. (a) An electronic card or other electronic information equivalent thereto; (b) An electronic signature creating key defined in subparagraph 4 of Article 2 of the Digital Signature Act and a certificate referred to in subparagraph 7 of the said Article; (c) A user number registered with a financial company or an electronic financial business entity; (d) Biological information of users; (e) A password required to use the means or information referred to in item (a) or (b).[129]

It is very important in electronic financial transaction therefore a financial company or an electronic financial business entity shall select, use and manage the means of access necessary for electronic financial transactions and confirm the identity and authority of a user, the details of a transaction request.[130] A financial company or an electronic financial business entity shall issue the means of access only if an application is made by the user after verifying the identity of such user.[131] However it may be also issued without the user's application nor the verification of the user's identity.[132] No one shall commit any of the following acts unless otherwise expressly provided for in other Acts with respect to the use and management of a means of access.[133] Provided, That the same shall not apply to cases where it is necessary to transfer an electronic

128) Article 2. subpara. 10. of the EFTA.

129) Id.

130) Article 6. para. 1. of the EFTA.

131) Article 6. para. 2. first sentence of the EFTA.

132) Article 6. para. 2. second sentence of the EFTA. The detailed cases, described in the provision, are as follows : ⅰ) in case of an electronic prepayment means or electronic currency ; ⅱ) where a user's consent is obtained for the renewal, replacement, etc. of the means of access, as prescribed by Presidential Decree.

133) Article 6. para. 3. first sentence of the EFTA.

prepayment means or electronic currency, or to offer it as security.[134] The means of access is the key-factor in electronic financial transaction, so that the loss or theft of means of access can bring about complicate legal problems, including the liability and compensation for damages of the financial company or an electronic financial business entity and users.

3. Security

a. Ensure security

Electronic Financial Transaction is the convenient and quick ways o transact in the area of finance, so that it enables the financial companies or an electronic financial business entities to provide the user with new service and to enhance their profit. Notwithstanding this merits, the Electronic Financial Transaction might cause big problems and turmoil if the hacking incidents on the IT network system occurs. Therefore it becomes more important to ensure the confidence of user by keeping the safety of information network system - its authenticity, confidentiality, integrity, availability and legitimate use should be provided without errors.

1) Duty to Ensure security

A financial company or an electronic financial business entity and its or his/her subsidiary electronic financial business entity shall perform its

134) Article 6. para. 3. second sentence of the EFTA. The detailed conducts, described in the provision, as follows : ⅰ) transferring or taking over a means of access; ⅱ) borrowing or lending a means of access, or storing, delivering or distributing a means of access, accompanied by receipt, demand or promise of any compensation; ⅲ) Borrowing or lending a means of access, or storing, delivering or distributing a means of access, for the purpose of using it for any crime or with the knowledge of the fact that it will be used for any crime; ⅳ) providing a means of access as the object of pledge; ⅴ) arranging any act referred to in ⅰ) through ⅳ).

or his/her duties of a good manager to ensure the safe processing of electronic financial transactions.[135] So, they shall be liable for the loss arising from any of the incidents which injured against a user and which may be considered as the lack of duty to ensure security.

And the intention or negligence of a subsidiary electronic financial business entity in relation to electronic financial transactions shall be deemed the intention or negligence of the relevant financial company or electronic financial business entity.[136] If any financial company or electronic financial business entity compensates the user for any loss caused by the intention or negligence of its or his/her subsidiary electronic financial business entity, it or he/she may claim and take the compensation against the subsidiary electronic financial business entity.[137]

2) Duty to make and comply with the standards related to the security and certification technologies

In order to ensure the security and reliability of electronic financial transactions, a financial company or an electronic financial business entity shall comply with the standards determined by the Financial Services Commission with respect to the information technology sector, such as human resources, facilities, electronic apparatus, and expenses for conducting electronic transmissions or processing, the electronic financial affairs and certification methods including the use of certificates under the 「Digital Signature Act」.[138]

The Financial Services Commission shall not compel the use of any specific technology or service when determining the standards and shall

135) Article 21. para. 1. of the EFTA.
136) Article 11. para. 1. of the EFTA.
137) Article 11. para. 2. of the EFTA.
138) Article 21. para. 2. of the EFTA.

endeavor to promote the fair competition of security and certification technologies.[139] For safe electronic financial transactions, the financial companies or electronic financial business entities shall annually establish a plan for the information technology sector and submit it to the Financial Services Commission after obtaining confirmation and signature of its or his/her representative.[140]

3) Analyzing and Assessing Vulnerability of Electronic Financial Infrastructure

To ensure the security and reliability of electronic financial transactions, a financial company and an electronic financial business entity shall analyze and assess the following matters with respect to its or his/her electronic financial infrastructure and report the findings therefrom (referring to the findings from analysis and assessment of vulnerability, where conducted under Article 9 of the 「Act on the Protection of Information and Communications Infrastructure」) to the Financial Services Commission: ⅰ) matters relating to the organization, facilities and internal control of the information technology sector; ⅱ) matters relating to electronic apparatus and the means of access of the information technology sector; ⅲ) matters relating to measures to respond to infringements in order to maintain electronic financial transactions etc.[141]

A financial company and an electronic financial business entity shall establish and implement a plan to take necessary complementary measures based on the findings from analysis and assessment of vulnerability in the electronic financial infrastructure.[142] The Financial Services Commission

139) Article 21. para. 3. of the EFTA.
140) Article 21. para. 4. of the EFTA.
141) Article 21-3. para. 1. of the EFTA.
142) Article 21-3. para. 2. of the EFTA.

may require public officials under its control to inspect the findings from analysis and assessment of vulnerability in the electronic financial infrastructure and the actual status of implementing complementary measures.[143] Details of and procedures for analysis and assessment of vulnerability in the electronic financial infrastructure and the establishment and implementation of the plan and other necessary matters shall be the Matters concerning the data processing system, etc. of subsidiary electronic financial business entities linked to the information technology sector or the other matters necessary for securing stability and reliability of electronic financial transactions which are determined and publicly announced by the Financial Services Commission.[144]

4) Prohibition against Electronic Infringement

No person shall commit any of the following offences: ⅰ) for anyone without access authority to access electronic financial infrastructure, or for anyone with access authority to fabricate, destroy, hide or lose the stored data beyond his/her authority; ⅱ) installing programs, such as computer virus, logic bomb or mail bomb, for the purpose of destroying data of electronic financial infrastructure or obstructing the operation of electronic financial infrastructure; ⅲ) causing errors or hindrance to electronic financial infrastructure by methods, such as sending mass signal, high-powered electromagnetic wave or data simultaneously or having fraudulent commands be processed, for the purpose of obstructing the stable operation of electronic financial infrastructure.[145]

143) Article 21-3. para. 3. of the EFTA.
144) Article 21-3. para. 4. of the EFTA.
145) Article 21-4. of the EFTA.

If an incident, such as disturbance or paralysis of electronic financial infrastructure, occurs due to an electronic infringement, the relevant financial company and electronic financial business entity shall, without delay, inform the Financial Services Commission and shall analyze the causes thereof and take necessary measures to prevent the spread of damage.[146]

After this notification of infringement incidents, The Financial Services Commission shall perform the following duties to respond to infringement incidents: ⅰ) collecting and disseminating information on infringement incidents; ⅱ) issuing preannouncements and warnings about infringement incidents; ⅲ) taking emergency measures against infringement incidents; ⅳ) other matters prescribed by Presidential Decree for responding to infringement incidents.[147] The Presidential Decree describes following duties should be performed by Financial Services Commission based on the above provision : ⅰ) Matters concerning the operation of a headquarter for countermeasures against infringement accidents that control and manage responses to infringement accidents and the designation of an institution for responding to infringement accidents to urgently cope therewith; ⅱ) matters concerning the establishment of contingency plans, training, etc. to cope with infringement accidents; ⅲ) investigation of infringement accidents and matters concerning requests for the provision, etc. of information on a relevant financial company, electronic financial business entity, subsidiary electronic financial business entity, etc.; ⅳ) matters concerning notification, etc. of security weaknesses to a person that has manufactured infringement accident-related software used by financial companies and electronic financial business entities, relevant administrative agencies, etc.[148]

146) Article 21-5. of the EFTA.
147) Article 21-6. of the EFTA.
148) Article 11-6. para. 1. of the Presidential Decree of EFTA.

b. Creation and Preservation of Electronic Financial Transaction Records

A financial company and an electronic financial business entity shall create the records necessary to trace and search the details of electronic financial transactions or to verify or correct any error in such details and shall preserve them for a period prescribed by Presidential Decree within up to five years.

If the preservation period, 5years, elapses and any commercial transaction relation, including financial transactions, is terminated, a financial company, etc. shall, within five years, destroy the relevant electronic financial transaction records (excluding credit information under the Credit Information Use and Protection Act) provided that this shall not apply in any of the following cases: 1. Where it is inevitable to meet any obligation under other Acts; 2. Other cases determined by the Financial Services Commission, where it is necessary to preserve electronic financial transaction records.

The types, preservation methods, destruction procedures and methods of electronic financial transaction records to be preserved by financial companies and an electronic financial business entity and the standards for determining the day when a commercial transaction relation is terminated shall be prescribed by Presidential Decree. According to the decree, It should be the form of documents, microfilms, disks or magnetic tapes and other electronic data processing medium and 1, 3, 5 years are different due to the type and importance of the information.

4. Protecting the user of electronic financial transaction

a. Terms and Conditions

1) Preparation and Alteration of Terms and Conditions

When a financial company or an electronic financial business entity intends to prepare or alter the terms and conditions for electronic financial transactions, it or he/she shall in advance report thereon to the Financial Services Commission.[149] Provided, that in cases determined by the Financial Services Commission which do not adversely affect the rights, interests or duties of users, a report may be file to the Financial Services Commission within ten days after the terms and conditions is prepared or altered.[150]

The Financial Services Commission may recommend a financial company or an electronic financial business entity to alter the terms and conditions if necessary to maintain orderly electronic financial transactions.[151] And the Financial Services Commission may determine the period and procedures for reporting the preparation or alteration of the terms and conditions and other necessary matters.[152]

2) Clarification of Terms and Conditions and Notification of Alterations

Any financial company or electronic financial business entity shall clarify the terms and conditions in concluding a contract for electronic financial transactions with a user, and, at the request of a user, deliver a copy of

149) Article 25. para. 1. first sentence of the EFTA.
150) Article 25. para. 1. second sentence of the EFTA.
151) Article 25. para. 2. of the EFTA.
152) Article 25. para. 3. of the EFTA.

the terms and conditions to the user, along with explaining the details thereof, in the manner prescribed by the Financial Services Commission.[153)]

No financial company or electronic financial business entity shall assert that the details of the terms and conditions are included in the relevant contract if it or he/she has concluded a contract without clarifying the terms and conditions with a user or delivering its copy.[154)]

Any financial company or electronic financial business entity shall, if it or he/she has altered the terms and conditions, publish the altered terms and conditions and inform the users thereof by one month prior to the enforcement of the altered terms and conditions, in the manner prescribed by the Financial Services Commission.[155)] However, if the terms and conditions are urgently altered due to any amendment to Acts and subordinate statutes, it or he/she shall promptly publish the terms and conditions so altered and inform the users thereof.[156)]

Any user may terminate a contract for electronic financial transactions by no later than the business day immediately preceding the enforcement date of the altered terms and conditions after the details of the altered terms and conditions are published or informed.[157)] When the user fails to raise an objection against the details of the altered terms and conditions within the period, he/she shall be deemed to have approved the altered terms and conditions.[158)]

---

153) Article 24. para. 1. of the EFTA.
154) Article 24. para. 2. of the EFTA.
155) Article 24. para. 3. first sentence of the EFTA.
156) Article 24. para. 3. second sentence of the EFTA.
157) Article 24. para. 4. first sentence of the EFTA.
158) Article 24. para. 4. second sentence of the EFTA.

b. Prohibiton to provide the user information

No one who recognizes the existence of any of the following matters in the course of performing duties relating to electronic financial transactions shall provide or disclose such information to any third party or use it for any purpose other than his/her duties without the consent of the relevant user: ⅰ) the matters relating to the identity of the user; ⅱ) the information or materials relating to the accounts, the means of access, and the details and results of electronic financial transactions of the user.[159)]

If a person who provides or leaks any electronic financial transaction information to any other person or uses such information for any purpose other than his/her duties (including a person issuing an electronic prepayment means applicable mutatis mutandis, he/she shall be punished by imprisonment with labor for not more than ten years, or by a fine not exceeding 100 million won.[160)]

However, this prohibition shall not apply to cases provided for in the proviso to the Article 4 (1) of the 「Act on Real Name Financial Transactions and Confidentiality」 or in any other Act. This exception is prescribed narrowly to keep the privacy and protect the private information.

c. Settlement and Mediation of Disputes

Any financial company or electronic financial business entity shall prepare procedures to reflect reasonable opinions or complaints presented by users in relation to electronic financial transactions and to compensate for any loss sustained by users in the course of conducting electronic financial

159) Article 26. of the EFTA.

160) Article 49. para. 1. subpara. 4. of the EFTA.

transactions.[161] When a user has an objection to the processing of electronic financial transactions, he/she may demand the settlement of dispute, such as compensation for losses, pursuant to the procedures mentioned above or file an application for mediation of dispute with the Financial Supervisory Service, the Korea Consumer Agency, etc.[162] Any financial company or electronic financial business entity shall clarify the procedures in concluding a contract for electronic financial transactions to inform the user how to use the settlement and mediation of disputes.[163]

d. Permission and Registration of Electronic Financial Business

Any person who intends to engage in a business issuing and managing electronic currencies shall obtain permission therefor from the Financial Services Commission.[164] Any person who intends to provide any of the following services shall register himself/herself with the Financial Services Commission[165] : ⅰ) electronic funds transfer services; ⅱ) issuance and management of electronic debit payment means; ⅲ) issuance and management of electronic prepayment means; ⅳ) electronic payment settlement agency services.[166] Any person who intends to obtain permission shall be a stock company with a capital of at least five billion won.[167]

The scope of the business issuing and managing the electronic currencies which is needed to be registered or exempted is prescribed at the statute and decrees with complexity. However the reason and legislative intent to

161) Article 27. para. 1. of the EFTA.
162) Article 27. para. 2. of the EFTA.
163) Article 27. para. 3. of the EFTA.
164) Article 28. para. 1. of the EFTA.
165) This regulation shall not apply to the banks provided for in the Banking Act etc.
166) Article 28. para. 2. of the EFTA.
167) Article 18. para. 1. of the Presidential Decree of EFTA.

require the permission and registration is to make an entry regulation with the judgement of Financial Services Commission in advance. Likewise, any person who intends to engage in a business registering and managing electronic bonds shall register himself/herself with the Financial Services Commission.

Any person who intends to obtain permission or file for registration to engage in a business issuing and managing electronic currencies or electronic bonds shall meet all of the following requirements : ⅰ) he/she shall hold the capital or fundamental property(at least five billion won); ⅱ) he/she shall be equipped with professional human resources and physical installations, such as computer equipment, sufficient to protect users and carry out the intended business; ⅲ) he/she shall meet the standards of financial soundness prescribed by Presidential Decree; ⅳ) he/she shall have a proper and sound plan necessary to execute the business concerned; ⅴ) he/she shall secure the major investors prescribed by Presidential Decree, with sufficient investment capability, sound financial state and social credit.[168]

There are some standards of disqualification for permission and registration, so that none of the following persons are entitled to permission or registration : ⅰ) a corporation for which one year has not yet passed since its registration was cancelled and a person who was a large stockholder of the corporation at the time of cancellation of such registration and for whom one year has not yet passed since the registration was cancelled; ⅱ) a corporation for which three years have not yet passed since its permission or registration was revoked and a person who was a large stockholder of the corporation at the time of such revocation and for

168) Article 31. para. 1. of the EFTA.

whom three years have not yet passed since such revocation; iii) a company which is in process of the rehabilitation procedure pursuant to the Debtor Rehabilitation and Bankruptcy Act and the large stockholders of such company; iv) any person who has failed to pay a debt within an agreed period in financial transactions and other commercial transactions and who is determined by the Financial Services Commission; v) any person who has been punished by a fine or heavier punishment for violating the finance-related Acts or subordinate statutes prescribed by Presidential Decree within the three years preceding the date of application for permission or registration; vi) a corporation whose large stockholder falls as mentioned above.[169]

e. Supervision and Inspection of the Financial Supervisory Service

1) Financial Company and electronic financial business entities

The Financial Supervisory Service following the instructions from the Financial Services Commission shall supervise whether financial companies and electronic financial business entities abide by the 「Electronic Financial Transaction Act」 or orders issued by FSC.[170] The Governor of the Financial Supervisory Service may require a financial company or an electronic financial business entity to report on its or his/her business operations and financial conditions if necessary to conduct supervision.[171]

The Governor of the Financial Supervisory Service may inspect the electronic financial business and other related financial conditions of a financial company and an electronic financial business entity and, if deemed necessary to conduct such inspection, ask the financial company and the

169) Article 32. para. 1. of the EFTA.
170) Article 39. para. 1. of the EFTA.
171) Article 39. para. 2. of the EFTA.

electronic financial business entity to submit data relating to its or his/her business operations and financial conditions or to order the attendance of all relevant persons.[172] Any person who conducts an inspection shall carry an identification indicating his/her authority and present it to relevant persons.[173] Upon conducting an inspection the Governor of the Financial Supervisory Service shall report the findings there from to the Financial Services Commission, as determined by the Financial Services Commission.[174]

When a financial company or an electronic financial business entity is deemed likely to undermine the sound operation of the financial company or electronic financial business entity in violation of any statutes, decrees, order or guideline, the Financial Services Commission may, upon recommendation of the Governor of the Financial Supervisory Service, take any of the following measures or authorize the Governor of the Financial Supervisory Service to take any measure : ⅰ) issuing an order to correct the relevant offence; ⅱ) issuing a caution or warning against a financial company or an electronic financial business entity; ⅲ) demanding caution, warning or reprimand against an executive officer or employee; ⅳ) recommending dismissal of an executive officer or demanding suspension of performance of his/her duties.[175]

2) Outside Orders by subsidiary electronic financial business entity

Where a financial company or an electronic financial business entity concludes or alters a contract with its or his/her subsidiary electronic financial business entity for affiliation, entrustment or outside orders in

172) Article 39. para. 3. of the EFTA.
173) Article 39. para. 4. of the EFTA.
174) Article 39. para. 5. of the EFTA.
175) Article 39. para. 6. of the EFTA.

relation to electronic financial transactions (including where a subsidiary electronic financial business entity concludes or alters a contract with another subsidiary electronic financial business entity for outside orders, etc.), it or he/she shall meet the standards determined by the Financial Services Commission to ensure the safety and reliability of electronic financial transactions and the soundness of the financial company and electronic financial business entity.[176)]

The Financial Services Commission may direct the financial company or electronic financial business entity to correct or supplement the relevant contents of the contract where the contents of a contract are deemed likely to undermine the operational soundness of a financial company or an electronic financial business entity and the rights and interests of users.[177)]

When the Governor of the Financial Supervisory Service conducts an inspection of a financial company or an electronic financial business entity in relation to outside orders, he/she may request its or his/her subsidiary electronic financial business entity to submit data pursuant to the standards determined by the Financial Services Commission.[178)] When a subsidiary electronic financial business entity fails to submit data or submit insufficient data, the Governor of the Financial Supervisory Service may investigate the relevant subsidiary electronic financial business entity directly.[179)] Then, The Governor of the Financial Supervisory Service may request the information as follows from a subsidiary electronic financial business entity, if deemed necessary for conducting an direct investigation : ⅰ) submitting a written statement relating to matters subject to such investigation; ⅱ) submitting

176) Article 40. para. 1. of the EFTA.
177) Article 40. para. 2. of the EFTA.
178) Article 40. para. 3. of the EFTA.
179) Article 40. para. 4. of the EFTA.

a ledger, document or other articles necessary for such investigation; iii) attendance of a relevant person.[180]

A subsidiary electronic financial business entity entrusted with any duties related to the data protection of the information technology sector shall not re-entrust such duties to a third party.[181] Provided, that this shall not apply to cases recognized by the Financial Services Commission within the extent not impairing the protection and safe processing of electronic financial transaction information.[182]

C. Personal Information Protection Act

1. Introduction

Before PIPA comes into force, individual acts by field such as 「Act on the Protection of Personal Information maintained by Public Institutions (Herein after "Public Personal Information")」, 「Credit Information Use and Protection Act」, 「Act on Promotion of Information and Communications Network Utilization and Information Protection, ect.(Herein after "Network Act")」, 「Act on the Protection, Use, ect. of Location Information」 have regulated the processing of personal information.

On the other hand, NGOs have demanded to improve legislations related to online privacy protection ever since 1999. It strongly urged to establish Personal Information Protection Act and independent Personal Information Protection Commission in that setting the social system for personal information is required to build a secure information society.

180) Article 40. para. 5. of the EFTA.
181) Article 40. para. 6. first sentence of the EFTA.
182) Article 40. para. 6. second sentence of the EFTA.

On November 22, 2004. Roh Hoe-chan, a member of the National Assembly, proposed a bill on personal information protection frame work consisting of the basic principles of personal information protection, practical realization of remedies, th establishment of personal information protection committee as an independent authority, the introduction of class action etc. On July 11, 2005. Lee eun young, assemblywoman, submitted a bill on personal information protection, with 「Public Personal Information(Partial Amendment)」, 「Network Act(Partial Amendment)」 that various opinions from all walks of life are reflected to enact personal information protection act in a way conformed with growing public demand. On October 17, 2005. Lee hae hoon, assemblyman, for the purpose of comprehensive personal information system which embrace both public and private sectors, proposed a bill on personal information protection repealing 「Public Personal Information」 and deleting related clauses with personal information protection from 「Network Act」. However these three bills are automatically disposed due to the National Assembly members' indifference meanwhile 17th National Assembly term was terminated.

18th National Assembly also attempted to make general personal information protection law by integrating public and private sectors. Other bills on personal information protection were submitted by Lee Hye hoon on August 8, 2008, by Byeon jae il on October 27, 2008, by government on November 28.

Above three bills are submitted to the National Assembly's general session in 2008, and then proposed to Security and Public Administration Committee for the first review. Government proposal, under which personal information protection committee has the authority to deliberate, while policy

making, enforcement, supervision authorities are granted to Ministry of Security and Public Administration, was critically called into question. With respect to this, on January 19, 2010. National Human Rights Commission of Korea expressed its opinion saying that independent organization and budget of personal information protection committee should be guaranteed to fulfill own function.

On April 15, 2010. bill screening subcommittee under Security and Public Administration Committee decided to make alternative which reflects each ministry's position and the National Assembly' requirements. The alternative prepared by Security and Public Administration Committee on April 19, 2010. provides that personal information protection committee belonging to a president has authorities to deliberate and decide. With respect to promote system, Ministry of Security and Public Administration controls overall enforcement except recommendation of correction for constitutional institution which is transferred to personal information protection committee. And it also stipulates personal information protection committee's authority to request data for deliberation and decision. This alternative was finally resolved at the plenary session after going through Legislation and Judiciary committee's vote on March 10, 2011, promulgated on March 29, 2011. and then has going into effect since 2011. 9. 30.

2. Personal Information

According the PIPA, the personal information means information that pertains to a living person, including the full name, resident registration number, images, etc., by which the individual in question can be identified,

(including information by which the individual in question cannot be identified but can be identified through simple combination with other information).[183] On the other hand, according to the 「Network Act」, personal information means the information pertaining to an individual alive, which contains information identifying a specific person with a name, a national identification number, or similar in the form of a code, letters, voice, sound, motion picture, or any other form (including information that makes it impracticable to identify a specific person by itself, but that enables to identify such person easily if combined with another information). Thus, these two pieces of legislation are almost the same with respect to what is personal information.

In conclusion, personal information generally includes 1) the voluntariness of the information, 2) a living person's information, 3) relevance with a specific person, 4) the possibility of identifying. While the voluntariness of the information, the information pertaining to an individual alive are less controversial, and the relevance with a specific person is broadly accepted, the possibility of identifying plays a key role in reality. The possibility of identifying includes that the information by which the individual in question cannot be directly identified but can be identified through simple combination with other information.

In addition, PIPA also defines other concepts, such as owner of information, personal information file, personal information manager. The "owner of information" means a person who can be identified by the managed information and therefore is the subject of the given piece of information.[184] And the "personal information file" means an aggregate of personal information

183) Article 2. subpara. 1 of the PIPA.
184) Article 2. subpara. 3. of the PIPA.

systematically arranged or organized according to a specific rule in order for the personal information to be readily retrievable.[185] The "personal information manager" means a public institution, corporate body, organization, individual, etc. who manages personal information directly or via another person to administer personal information files as part of his/her duties.[186]

3. Using, Collecting and Providing Personal Information with Consent

a. collect and use personal information

The most significant point in process of collection and use of personal information is to obtain the consent from a owner of information and notify them of certain matters.

A personal information manager may collect personal information and use it for the intended purpose of collection in any of the following cases : 1) where he/she has obtained the consent of a owner of information, 2) where there exist special provisions in any Act or it is inevitable to fulfill an obligation imposed by or under any statute, 3) where it is inevitable for a public institution to perform its affairs provided for in any statute, etc., 4) where it is inevitably necessary for entering into and performing a contract with a owner of information, 5) where it is deemed obviously necessary for physical safety and property interests of a owner of information or a third person when the owner of information or his/her legal representative cannot give prior consent because he/she is unable to express his/her intention or by reason of his/her unidentified address, etc.,

185) Article 2. subpara. 4. of the PIPA.
186) Article 2. subpara. 5. of the PIPA.

6) where it is necessary for a personal information manager to realize his/her legitimate interests and this obviously takes precedence over the rights of a owner of information.[187] In such cases, this shall be limited to cases where such information is substantially relevant to a personal information manager's legitimate interests and reasonable scope is not exceeded.[188]

When a personal information manager obtains consent he/she shall notify a owner of information of the following matters : 1) purposes for which personal information is collected and used, 2) items of personal information to be collected, 3) period for which personal information is held and used., 4) fact that a owner of information has a right to reject to give his/her consent and details of a disadvantage, if any, due to his/her rejection to give consent.[189] When the personal information manager changes any of the above-mentioned matters he/she shall inform the same and obtain consent thereto.[190]

b. method to obtain consent

When a personal information manager obtains the consent of a owner of information about the management of personal information, he/she shall classify respective matters requiring consent and notify the owner of information of such matters to clearly understand them, and obtain consent respectively to such matters.[191]

187) Article 15. para. 1. of the PIPA.
188) Article 16. para. 1. of the PIPA.
189) Article 15. para. 2. first sentence of the PIPA.
190) Article 15. para. 2. second sentence of the PIPA.
191) Article 22. para. 1. of the PIPA.

When a personal information manager obtains the consent of personal information related to collected and used,[192] provided information,[193] sensitive information,[194] and unique identified information, he/she shall classify the personal information that can be managed without obtaining the consent of the owner of information and the personal information requiring the consent of the owner of information for the purpose of entering into a contract with the owner of information.[195] In such cases, a personal information manager is responsible for proving that the subject personal information is the one that can be managed without obtaining consent.[196]

When a personal information manager intends to obtain the consent of a owner of information on the management of his/her personal information in order to publicize or solicit the sale of goods or services to him/her, the personal information manager shall notify the owner of information thereof to clearly understand this and obtain his/her consent thereto.[197] No personal information manager shall refuse to provide a owner of information with goods or services on the ground that the owner of information fails to give his/her consent to matters he/she is entitled to give selective consent.[198] When a personal information manager needs to obtain consent required under this Act in order to manage personal information of a child under the age of 14 years, he/she shall obtain the consent of his/her legal guardian. In such cases, minimum information necessary for

192) Article 15. para. 1. of the PIPA.
193) Article 17. para. 1. of the PIPA.
194) Article 23. para. 1. subpara. 1. of the PIPA.
195) Article 22. para. 1. first sentence of the PIPA.
196) Article 22. para. 1. second sentence of the PIPA.
197) Article 22. para. 3. of the PIPA.
198) Article 22. para. 4. of the PIPA.

obtaining the consent of the legal guardian may be directly collected from the relevant child without consent of the legal guardian.[199]

c. Restrictions

Where a personal information manager collects personal information, he/she shall collect minimum information necessary for achieving the purpose thereof, and in such cases, the personal information manager is responsible for proving that he/she collects the minimum personal information.[200] Where a personal information manager collects personal information with the consent of a owner of information, he/she shall collect it after making a specific notification of the fact that the latter may choose not to consent to the collection of personal information other than the minium information required.[201] A personal information manager shall not reject providing a owner of information with goods or services on the ground that the owner of information does not give consent to collect his/her personal information other than the minimum necessary information.[202]

No person who receives personal information from a personal information manager shall use such personal information for any purpose other than the intended purpose of providing or provide a third person with such information.[203] However, when he/she has obtained separate consent from a owner of information, or there are special provisions exist in any other Act, he or she can use that information.[204]

---

199) Article 22. para. 4. of the PIPA.
200) Article 16. para. 1. of the PIPA.
201) Article 16. para. 2. of the PIPA.
202) Article 16. para. 3. of the PIPA.
203) Article 19. of the PIPA.
204) Id.

4. Safety management on Personal Information

a. Duty to Take Safety Measures

A personal information manager shall establish an internal administration plan, keep access records, and take technical, administrative and physical measures necessary for securing safety, in order to prevent personal information from loss, theft, leakage, alteration or damage.[205]

Therefore, a personal information manager should control access first to protect personal information. To this end, access authority of personal information system from necessity should be strictly empowered only to those who manage personal information and those who must handle personal information inevitably.

Furthermore, where a personal information handler is changed due to personnel transfers such as retirement, a provider of information and communication services shall immediately alter or cancel the authority to access a personal information processing system. A personal information manager shall inspect and supervise files of records of access to the personal information processing system at least once a month and preserve those files to examine the system etc. more than 6 months. A provider of information and communication services shall store encrypted passwords in one-way in order to prevent decoding. A provider of information and communication services shall store information such as resident registration number, passport number, drivers license number, Foreign Registration Number, credit card number, account number, bio-metric information with encryption algorithm for safety. A provider of information and communication

205) Article 29. of the PIPA.

services shall install security program such as anti-virus vaccine software in order to block intrusion by malicious programs.

b. Establishment and Disclosure of Personal Information Management Policies

A personal information manager shall establish personal information management policies.[206] In such cases, a public institution shall establish such personal information management policies for personal information files to be registered.[207] The policy shall contains ⅰ) purpose for which personal information is managed, ⅱ) period for which personal information is held and used, ⅲ) Matters concerning providing a third person with personal information, ⅳ) matters concerning entrusting the management of personal information, ⅴ) matters concerning the rights and duties of a owner of information, and how to exercise them, ⅵ) other matters prescribed by Presidential Decree concerning the management of personal information.[208]

Where a personal information manager establishes or amends the personal information management policies, he/she shall disclose them.[209] Where the details of the personal information management policies are inconsistent with those of a contract entered into between a personal information manager and a owner of information, whichever is more advantageous to the owner of information shall govern.[210]

The Minister of Government Administration and Home Affairs may draw up a guideline for preparing the personal information management policies

206) Article 30. para. 1. of the PIPA.
207) Id.
208) Id.
209) Article 30. para. 2. of the PIPA.
210) Article 30. para. 3. of the PIPA.

and recommend a personal information manager to comply therewith.[211]

c. Designation of Personal Information Protection Managers

A personal information manager shall designate a personal information protection manager to take overall responsibility for the management of personal information.[212]

A personal information protection manager shall conduct ⅰ) establishing and implement a personal information protection plan, ⅱ) periodically investigating and improving personal information management status and practices, ⅲ) handling complaints concerning the management of personal information and remedying damage therefrom, ⅳ) establishing an internal control system to prevent the leakage and misuse of personal information, ⅴ) establishing and implementing an education plan for the protection of personal information, ⅵ) protecting, administering and supervising personal information files, ⅶ) other duties prescribed by Presidential Decree for the appropriate management of personal information.[213]

d. Certification of Personal Information Protection

Ministry of Interior certificate that whether a personal information manager's measures related to personal information management and protection are in accordance with this act.[214] The validity period of certification is three years.[215]

---

211) Article 30. para. 4. of the PIPA.
212) Article 31. para. 1. of the PIPA.
213) Article 31. para. 2. of the PIPA.
214) Article 32-2. para. 1. of the PIPA.
215) Article 32-2. para. 2. of the PIPA.

The minister of Interior. may revoke the certification, where ⅰ) having received the certification of personal information protection in a false or otherwise unjustifiable manner, ⅱ) refusing or obstructing the ex post facto management, ⅲ) falling short of the standards for certification, ⅳ) violating personal information protection-related legislation and the reason for violation is grave, are found.[216] Ministry of Interior shall carry out follow-up management at least once a year in order to maintain the efficiency of personal information protection certification.[217]

e. Personal Information Impact Assessment

Where the administration of personal information files meeting the standards prescribed by Presidential Decree is likely to infringe on the personal information of a owner of information, the head of a public institution shall conduct an assessment (hereinafter referred to as "impact assessment") to analyze risk factors and discover improvements, and submit the results thereof to the Minister of Interior, and in such cases, the head of a public institution shall request any agency designated by the Minister of Interior.[218] In conducting impact assessment, ⅰ) number of personal information to be managed, ⅱ) whether personal information is provided to a third person, ⅲ) risk of infringing on the rights of a owner of information and the degree of risk, ⅳ) other matters prescribed by Presidential Decree, shall be considered.

216) Article 32-2. para. 3. of the PIPA.
217) Article 32-2. para. 4. of the PIPA.
218) Article 33. para. 1. of the PIPA.

f. Notification

When a personal information manager becomes aware that personal information has leaked out, he/she shall notify the relevant owner of information of the following matters without delay: ⅰ) items of leaked personal information, ⅱ) when and how personal information has leaked, ⅲ) information on means, etc. available to a owner of information to minimize damage that could inflicted on by leakage, ⅳ) a person information manager's actions and damage remedy procedures, ⅴ) a department in charge of receiving reporting, etc. and contact if damage is inflicted on a owner of information.[219]

Where personal information has leaked, a personal information manager shall prepare measures to minimize the damage therefrom, and take necessary measures.[220]

219) Article 34. para. 1. of the PIPA.
220) Article 34. para. 2. of the PIPA.

Ⅴ. Conclusion

Computer networks and information systems have governed daily human lives in this society. But a lot of cyber attacks, this society have been suffered, have made great threats on core functions operated by the networks and systems. This society has also been significantly exposed to cyber attacks due to advanced internet infrastructure, widely spreaded smart-phones and has accumulated experiences in response to cyber attacks from North Korea.

To respond cyber attacks, a state shall design appropriate legislations and national plans to respond against cyber attacks and enhance digital economy. Korea has also been struggle to make efficient legislations and policies to combat cyber attacks and enhance digital economy based on advanced information and communication technologies.

Nationwide responding system against cyber attacks shall be described in National Cyber Security Management Regulation. Following the regulation, Korean government authorities shall develop, establish, and perform the policies and initiatives related with cyber security. The regulation shall describe roles, duties and liabilities of government authorities such as Office of National Security in Blue House and National Cyber Security Center in National Intelligence Service. It also describe information sharing among government authorities.

Protecting Critical Information Infrastructure(CII) from cyber attacks is very important in National Security, because it can maintain core functions to operate a state and daily human lives, such as energy, banking, health, water and so on. Korean government has enacted Critical Information

Infrastructure Protection Act since 2002. The Act has made national structure to protect CII from cyber attacks and described the provisions on designation on CII, evaluating vulnerabilities and establishing protection plans, responding cyber incidents, and penalties.

Protecting nuclear power plants from cyber attacks has been national agenda in Korea after North Korean cyber attacks against KHNP. Korea has enacted Nuclear Protection and Prevention Act to strengthen the protection system of nuclear facilities. Under the Act, the Korea Institute of Nuclear Nonproliferation and Control(KINAC) shall establish KINAC/RS-015 to protect nuclear facilities from cyber attacks.

Following the Comprehensive Measures to enhance National Cyber Security, Korean policy makers and legislators heard many voices from individuals, vendors, and governmental institutes agencies, cyber security industry shall be encouraged to support robust cyber security activities with best technologies. Hence, Cyber Security Industry Enhancement Act was newly enacted. According to the Act, Korean central and local government, and municipals shall establish and perform policies to encourage cyber security industry and prepare measures to allocate budgets to fulfill that policies.

Electronic financial transaction is the convenient and quick ways to transact in the area of finance, so that it enables the financial companies or an electronic financial business entities to provide the user with new service and to enhance their profit. Notwithstanding this merits, the electronic financial transaction might cause big problems and turmoil if the hacking incidents on the IT network system occurs. Therefore it becomes more important to ensure the confidence of user by keeping the safety of information network system - its authenticity, confidentiality, integrity, availability and

legitimate use should be provided without errors. To make secure and reliable electronic financial transactions, the “Electronic Financial Transactions Act” has been enacted.

After suffering several significant personal information disclosed cases, National Assembly members proposed a bill to independently and wholely focusing on personal information protection. The bill enacted to be an Act at March 29, 2011. and has been effected since 2011. 9. 30. According to the Act, personal information is defined as information that pertains to a living person, including the full name, resident registration number, images, etc., by which the individual in question can be identified. To protect the personal information, the Act describes that when a personal information manager is in the process of collection and use of personal information, he/she shall obtain the consent from a owner of information and notify them of certain matters. The Act also describes that a personal information manager shall establish an internal administration plan, keep access records, and take technical, administrative and physical measures necessary for securing safety, in order to prevent personal information from loss, theft, leakage, alteration or damage. He/she shall also have to establish and disclose of Personal Information Management Policies, and to designate Personal Information Protection Managers. Ministry of Interior certificate personal information protection measures in accordance with the Act. When a personal information manager becomes aware that personal information has leaked out, he/she shall notify the relevant holder of the information.

As understanding of the cyber security legislation, other countries establish a confidence in the cyberspace, which contributes to sustainable development and prosperity in the region economy and ensuring stability in cyberspace. By understanding Korea’s national structure to responding cyber attacks,

law and policies related to critical information infrastructure including nuclear power plants protection law and policy, enhancing information security industry, securing electronic financial transactions, and protecting personal information, the countries would establish robust cyber security laws and policies to responding cyber attacks. To support for the countries to establish the laws and policies, Korea is also able to expand to the emerging markets and strength cooperation on relevant industry with increasing demands for products related to cyber security. Therefore, it is likely to encourage sustainable cooperation on cyber security sector among Asian countries and the other countries in the world, after this research introduce Korean cyber security system and operation to the world. Besides, this research is likely to assist materializing the value of creative economy and accompanied growth through the cyber security.

References

Articles

Korea Institute for National Unification(KINU): North Korea Domestic and Foreign Policy Evaluation and Outlook after Kim Jong-un seizing the Power: 11th KINU Unification Forum(2015)

Tobias Feakin: Playing Blind-Man's Buff: Estimating North Korea's Cyber Capabilities: International Journal of Korean Unification Studies, vol. 22, no. 2 (2013)

Il Seok Oh(Luke), Seung Youl Lee, So Jeong KIM: Designing Effective Responding Legal and Political Measures against North Korea's Cyber Attacks: Institute for National Security Strategy(IISS) Policy Studies, vol.186 (2015)

Il Seok Oh(Luke), A Study on the Compensated "Damages" arising from Breach of Duty to Protect Personal Information, Vol. 19, No.3, Ewha Law Journal(Ewha University)(March, 2015)

Il Seok Oh(Luke), A Legal Study on Enhancing Security Authority's Cyber Security Activities, Vol. 20, No.3, Journal of Law and Science(Hannam University)(October, 2014)

Il Seok Oh(Luke), Recommendations on Reforming Critical Information Infrastructure Protection Act of Korea with a View from Risk Allocation, Vol. 19, No.1, Ewha Law Journal(Ewha University) 293(September, 2014)

Moon Taek Kwon: A Study on Countermeasures to the North Korean Asymmetric Strategy - 'Cyber Surprise Attack': Journal of Information and Security, vol. 10(4) (2010)

Dakota L. Wood: 2015 Index of U.S. Military Strength: The Heritage Foundation (2015)

Australian Strategic Policy Institute(ASPI), Cyber Maturity in the Asia-Pacific Region (2014)

Sunha Bae, Sangdon Prark, So Jeong Kim: A Study on the Development for the National cyber security Capability Assessment Criteria: Journal of the Korea Institute of Information Security & Cryptology, vol. 25, No. 5 (2015)

James Andrew Lewis, Denise E. Zheng: Significant Cyber Events: Center for Strategic & International Studies(CSIS) (2016)

So Jeong Kim, Sangdon Park: A Study on Cyber Cecurity Policy in the Context of International Security: Journal of Informational and Security, vol. 13. no. 6 (2013)

Sangdon Park, Injung Kim: A Study on Tasks for the Legal Improvement for the Governance System in Cybersecurity: Journal of Informational and Security, vol. 13. no. 4 (2013)

Websites

http://english.yonhapnews.co.kr/northkorea/2013/10/04/62/0401000000AEN20131004007400320F.html

http://www.heritage.org/research/reports/2015/03/the-us-needs-to-respond-to-north-koreas-latest-cyber-attack

http://www.databreaches.net/20-million-people-fall-victim-to-south-korea-data-leak-fss-calls-on-financial-institutions-to-improve-protections-against-insider-leaks/

http://www.securityweek.com/20-million-people-fall-victim-south-korea-data-leak

http://www.kookje.co.kr/news2011/asp/newsbody.asp?code=0300&key=20150106.22008193319

https://en.wikipedia.org/wiki/Internet_fraud

https://en.wiktionary.org/wiki/cyberviolence

http://khnews.kheraldm.com/view.php?ud=20151208000959&md=20151211003712_BL

http://news.mk.co.kr/newsRead.php?year=2015&no=611797

https://en.wikipedia.org/wiki/Phishing

https://en.wikipedia.org/wiki/Pharming

http://news.mk.co.kr/column/view.php?year=2014&no=3423

http://www.mt.co.kr/view/mtview.php?type=1&no=2015012908211802132&outlink=1

Laws and Regulations

National Cyber Safety Management Regulation

Critical Information Infrastructure Protection Act

Act on measures for the Protection of Nuclear Facilities, etc. and Prevention of Radiation Disasters

Cyber Security Industry Enhancement Act

Electronic Financial Transaction Act