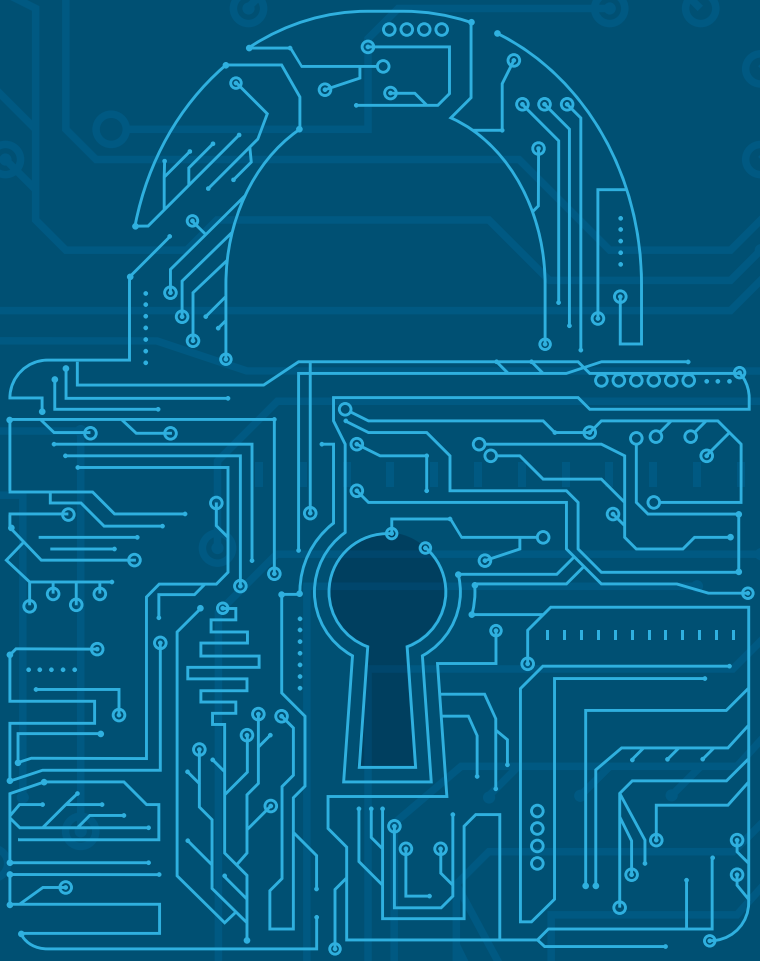
National Cybersecurity Law, Governance, and Infrastructure

IN THE REPUBLIC OF KOREA



AUTHORS

Santiago Paz
Luis Tejerina
Kang Donghuyun

SUPPORTED BY

National Health Insurance Service, Republic of Korea

Korea Internet & Security Agency

Keyword(s): cybersecurity, governance, institutional capacity, cybercrime, education, threat incident, attack, inteligence.

JEL Code(s): H11, O33, O38

Copyright © 2024 Inter-American Development Bank ("IDB"). This work is subject to a Creative Commons license CC BY 3.0 IGO (https://creativecommons.org/licenses/by/3.0/igo/legalcode). The terms and conditions indicated in the URL link must be met and the respective recognition must be granted to the IDB.

Further to section 8 of the above license, any mediation relating to disputes arising under such license shall be conducted in accordance with the WIPO Mediation Rules. Any dispute related to the use of the works of the IDB that cannot be settled amicably shall be submitted to arbitration pursuant to the United Nations Commission on International Trade Law (UNCITRAL) rules. The use of the IDB's name for any purpose other than for attribution and the use of IDB's logo shall be subject to a separate written license agreement between the IDB and the user and is not authorized as part of this license.

Note that the URL link includes terms and conditions that are an integral part of this license.

The opinions expressed in this publication are those of the authors and do not necessarily reflect the views of the Inter-American Development Bank, its Board of Directors, or the countries they represent.

Inter-American Development Bank
1300 New York Avenue, N.W.
Washington, D.C. 20577
www.iadb.org

The Institutions for Development Sector was responsible for the production of this publication.
External vendors:
Production Editor: Sarah Schineller (A&S Information Partners, LLC)
Editor: Leslie Hunter
Design: Cleiman

Table of Contents

Table Index

Figure Index

Abbreviations

ACRONYM	ORIGINAL TERMS (IN ALPHABETICAL ORDER)
API	Application Programming Interface
CCTV	Closed circuit TV
CERT	Computer Emergency Response Team
CSP	Cloud service providers
CSTEC	Cybersecurity Training and Exercise Center
dBrain	National Financial Information System
DDoS	Distributed Denial of Service
DNS	Domain Name System
EMR	Electronic medical record
ETRI	Electronics and Telecommunication Research Institute
FDS	Fraud detection system
FISCON	Financial Information Protection Conference
FSC	Financial Services Commission
FSI	Financial Security Institute
FSS	Financial Supervisory Service
GIDC	Government Integrated Data Center
GPKI	Government Public Key Infrastructure
ISMS	Information Security Management System
IoT	Internet of things
ISAC	Information Sharing and Analysis Center
KCTI	Korea Cyber Threat Intelligence (The Internet-based Information Sharing System)
KDCA	Korea Disease Control and Prevention Agency
KHIS	Korea Health Information Service
KIDS	Korea Institute of Drug Safety and risk Management
KISA	Korea Internet and Security Agency
KISDI	Korea Information Society Development Institute
KLID	Korea Local Information Research and Development Institute

KLRI	Korea Legislation Research Institution
KNPA	Korea National Police Agency
KT	Korea Telecom
LIS	Laboratory Information System
LGU+	LG Uplus
MFDS	Ministry of Food and Drug Safety
MoE	Ministry of Environment
MoF	Ministry of Finance
MoHW	Ministry of Health and Welfare
MoIS	Ministry of the Interior and Safety
MoJ	Ministry of Justice
MoLIT	Ministry of Land, Infrastructure and Transport
MoSIT	Ministry of Science and ICT
NCSC	National Cybersecurity Center
NCTI	National Cyber Threat Intelligence
NHIS	National Health Insurance Service
NIA	National Information Society Agency
NICN	National Information Communication Network
NICS	National Information and Communications Service (a.k.a. GNS)
NIDMS	National Integrated Disease Management System
NIH	National Institute of Health
NIPA	National IT Industry Promotion Agency
NIS	National Intelligence Service
NPA	National Policy Agency
NSC	National Security Council
NSO	National Security Office (NSO) (under President's Office)
NSRI	National Security Research Institute (under ETRI)
OCS	Order Communication Systems
PIMS	Personal Information Management System
PACS	Picture Archiving and Communication Systems
SKT	SK Telecom
SSIS	Social Security Information Service

Executive Summary

This document describes the foundations of cybersecurity practices in Korea, specifically, laws, regulations, governance, and foundational infrastructure.

The COVID-19 pandemic has accelerated the digital transformation of everyday life, providing a opportunity to digitize important national activities, such as the economy and education. At the same time, the shift to online and virtual activity due to the COVID-19 pandemic has expanded and deepened cyberattacks in every realm of life. This document describes the foundations of cybersecurity practices in Korea, specifically, laws, regulations, governance, and foundational infrastructure, which comprise the core components of cybersecurity practices in Korea. It also highlights a number of important lessons for improving cybersecurity practices in the country.

The first lesson is that laws and regulations are essential for the deployment of effective responses to future cyber threats. Korea has enacted many national laws related to cybersecurity, including the Resident Registration Act (1994), the Use and Protection of Credit Information Act (1995), the National Informatization Framework Act (1996), the Act on the Promotion of Information and Communications (1997), the Digital Signature Act (1999), the Act on The Protection of Information and Communications Infrastructure (2009), the Electronic Government Act (2009), the Personal Information Protection Act (2011), and others. Many of these laws have been revised to reflect current realities in Korea. These laws form the basis of national policy and governance for effective cybersecurity responses.

Second, the Korean government has implemented a pan-government national cybersecurity plan, which delineates the development of a national pan-government information protection system encompassing the public, private, national defense, and financial sectors. The National Security Council (NSC) Korea's the top administrative entity for dealing with national cybersecurity. Under the NSC, several other agencies —the NIS, NCSC, KISA, KLID, MSICT, MoIS, FSC, FSS, and FSI, among others—work closely to protect the country against cyber threats. IDB member states should promote and nurture special cybersecurity-related institutions.

Fourth, incubating information security companies to expand their business areas and scale up is critical for upgrading the nation's capacity regarding cybersecurity. The government's strong support for nurturing private cybersecurity companies will scale up the country's overall capacity. It can also provide jobs.

Finally, planning for next-generation cybersecurity strategy is important. In fact, internet of things (IoT) devices are proliferating. To combat hacking, the government plans to expand information protection certification to various fields and promote the internalization of security in various information protection and communication devices.

IDB member states are at different stages with respect to cybersecurity in terms of law, governance, infrastructure, and best practices. However, an important common element of cybersecurity is preparing against potential threats by properly describing the current situation and developing measures to address the threats. Korea's cybersecurity policy and relevant experience could provide the foundation for cybersecurity in IDB member states. NHIS is prepared to exchange ideas and share its expertise in this domain with IDB member states in the near future.

CHAPTER

1.

Korea's Legal System related to Cybersecurity

National Cybersecurity Law, Governance,
and Infrastructure in the Republic of Korea

1.1 Overview of the Legal System

This policy note describes the foundation of cybersecurity practices in Korea concerning laws, regulations, and governance. Specifically, it addresses how Korea has been ensuring the stability of cybersecurity. The Korean government has implemented a pan-government national cybersecurity plan that delineates the development of a national information protection system encompassing the public, private, national defense, and financial sectors.

1.2 Korea's Main Laws related to Cybersecurity

Korea's current information security system is based on a system of laws executed by government organizations. The Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.[1] is the basic law. Each ministry has individual laws for each task or sector. The law, initially enacted in 2001, was amended once in 2015.

As shown in Table 1, the system of information security laws covers seven major areas: (1) information security policy establishment, (2) major information and communication-based security, (3) incident response, (4) cybersecurity measures and action, (5) evaluations, certifications, and inspections, (6) electronic signature, and (7) personal information protection, including policy establishment and intrusion incident response for each security task. The security targets are divided into public and private areas.

1 It is traditional to include "etc." in Korean legislative law clauses.

The Information and Communications Network Act regulates the information security policy establishment function in the public and the private sectors. The National Cyber Safety Act separates and regulates the public and the private sectors in performing the intrusion incident response function based on the Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc. The Information and Communication Infrastructure Protection Act performs a major information and communication infrastructure protection function in the public and the private sectors, and the E-Government Act performs cybersecurity functions and regulates only the public sector.

The National Cyber Security Center of the National Intelligence Service (NIS) is responsible for the information security of the national e-government information security, and the Ministry of Interior (MoIS) is responsible for public institutions' information security.

With respect to government organizations, the information security system is a decentralized system with department processes and functions. Korea's information security was initially developed in a decentralized way because at the start of the e-government system's development, each ministry provided information security based on its process and usability after enacting the E-Government Act in 2001. This information security system and policy in Korea were developed by the public and private sectors. Currently, for the public sector, the National Cyber Security Center of the National Intelligence Service (NIS) is responsible for the information security of the national e-government information security, and the Ministry of Interior and Safety (MoIS) is responsible for public institutions' information security.

The Ministry of Science, Technology and ICT (MSICT) is responsible for private-sector information security, specifically monitoring and setting guidelines. The National Defense Agency manages military/defense-related information security. In addition, according to the Comprehensive National Cyber Security Measures announced in 2013, the Cyber Security Secretary of the Blue House National Security Office (NSO) is the main organization responsible for pan-government information security.

The National Cyber Security Center (NCSC) of the NIS performs functions such as prevention of leaks of state secrets in the public sector, protection of national information and communications networks, general coordination of national cybersecurity policies, investigation and recovery support for breaches, and cyber crisis prevention activities and attack detection. (https://eng.nis.go.kr/EID/1_7_1.do).

The Ministry of Public Administration and Safety (MoPAS, formerly MoIS)[2] is in charge of security related to e-government public services. It performs functions such as discovering and analyzing security risk factors in administrative processes, distributing security guidelines to each institution, investigating and evaluating whether measures are implemented, providing information security solutions, and responding and reporting when a security incident occurs. In addition, MSICT performs functions such as securing the safety of information and communication networks in the private sector, preventing infringement accidents, strengthening cybersecurity, and establishing and generalizing private information protection policies. The Ministry of National Defense established the Armed Forces Cyber Command under the Defense Intelligence Headquarters and is in charge of information security and cyber warfare in the military sector.

2 MoPAS is the former ministry name of MoIS. In Korea, while the new president has been elected, he/she usually changes the Ministries names as well as integrates/segregates the functions of Ministries.

TABLE 1 **MAIN LAWS REGARDING CYBERSECURITY**

CATEGORY	PUBLIC		PRIVATE	
Information security policy establishment	National Informatization Framework Act Act on Promotion of Information and Communications Act on The Protection of Information And Communications Infrastructure			
Major information and communication-based security	Information and Communication Infrastructure Protection Act • Protection of major information and communication infrastructures by sectors such as public, financial, and information communication, etc.			
Incident response	National Cyber Safety Management Regulations: Response to Infringement Incidents of Public Institutions, National Cyber Safety Center (Ownership)		Information and Communications Network Act	Response to Civil Infringement Incidents
Cyber Security Measures and Action	Electronic Government Act	Establishment and Implementation of security measures such as information and communication networks		User information protection
Various evaluations, certifications, and inspections		• Security measures for electronic documents • Public sector security conformity verification system		Information Security Safety Diagnosis
	National Informatization Framework Act: Information Security System Evaluation and Certification			
Electronic signature	Electronic Government Act: Administrative electronic signature		Digital Signature Act: Certified digital signature	
Personal Information Protection	Personal Information Protection Act Resident Registration Act		Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. Use and Credit Information Protection Act	

Source: Yoon and Lee (2017).

The dates that the Acts went into effect are listed in Table 2 in chronological order.

TABLE 2 **NAME OF THE ACT AND CHRONOLOGICAL ENFORCEMENT DATES**

NAME OF THE ACT	ENFORCEMENT DATES
Resident Registration Act	1994.7.01
Use and Protection of Credit Information Act	1995.7.06
National Informatization Framework Act	1996.1.01
Act on Promotion of Information and Communications	1997.1.31
Digital Signature Act	1999.7.01
Act on The Protection of Information and Communications Infrastructure	2009.8.23
Electronic Government Act	2009.8.23
Personal Information Protection Act	2011.9.30

Source: Korea Law Information Center.

CHAPTER

2.

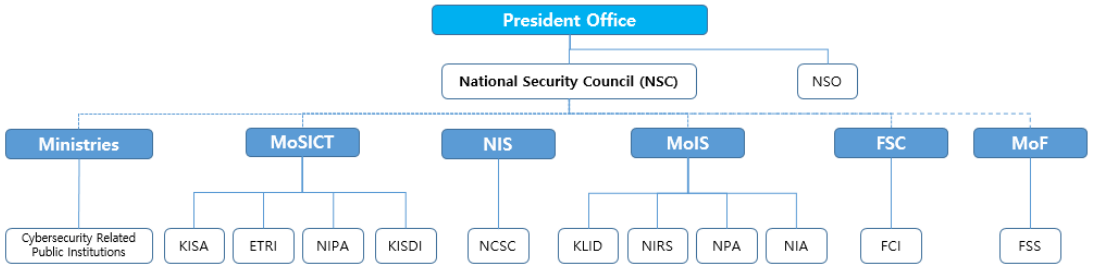
Governance and Special Institutions for Cybersecurity in Korea

National Cybersecurity Law, Governance,
and Infrastructure in the Republic of Korea

2.1 Overview of Institutional Governance for Cybersecurity

The Korean government has implemented a pan-government national cybersecurity plan, which delineates the development of a national pan-government information protection system encompassing the public, private, national defense, and financial sectors (National Intelligence Service, Ministry of Science and Technology, Financial Services Commission).

FIGURE 1 **MINISTRIES AND PUBLIC INSTITUTIONS RELATED TO CYBERSECURITY**



Ministries	Full Name	Cybersecurity Related Public Institutions	Full Name
MoSICT	Ministry of Science and ICT	KISA	Korea Internet & Security Agency
		ETRI	Electronics and Telecommunications Research Institute
		NIPA	National IT Industry Promotion Agency
		KISDI	Korea Information Society Development Institute
NIS	National Intelligence Service	NCSC	National Cyber Security Center
MoIS	Ministry of Interior and Safety	KLID	Korea Local Information and Research Institute
		NIRS	National Information Resource Service
		NPA	National Policy Agency
		NIA	National Information Society Agency
FSC	Financial Services Commission	FCI	Financial Security Institute
MoF	Ministry of Finance	FSS	Financial Supervisory Service

Source: self design.

The security monitoring structure for government and public sector organizations is built on three layers: agency-level security monitoring (government and public organizations), sector-level security monitoring (central administrative agency), and national security monitoring (NCSC). In addition, the National Cybersecurity Center (NCSC) detects and responds to cyber threats to national security and distributes cyber threat detection techniques to the agency/sector network security monitoring centers.

The central administrative agency operates 44 network security monitoring centers, providing uninterrupted security monitoring around the clock for the information and communications networks of relevant institutions and affiliated organizations. The sectoral network security monitoring centers detect and respond to cyber threats against information systems, information communications networks, and data held by the relevant national and public institutions to contain the damage. It is necessary to have professional human resources and facilities for security monitoring. If necessary, professionals from the specialized company designated by the Minister of Science and ICT may work together.

NIS monitors cyber threats in real time and promptly shares the threat intelligence with the relevant organization to minimize adverse outcomes. It shares the intelligence in real time when it is relevant for agency or sector network security monitoring centers to achieve systematical responses at the national level.

Korea's sector-level security monitoring (central administrative agency) governance at the operational level (public management agencies) is mostly performed by the Korea Internet and Security Agency (KISA) and the Korea Local Information Research & Development Institute (KLID) under the MoIS.

This report introduces cybersecurity control and monitoring performed by KISA from an inter-organizational perspective.

This report introduces cybersecurity control and monitoring performed by KISA from an inter-organizational perspective. The administrative environment of e-government has shifted from paper document-based to electronic document-based. The possibility of harm due to exposure, falsification, and damage of key information by measures was sought to ensure continuity and safe recovery. As a result, the government

guarantees the identification of administrative agencies and public officials, prevention of forgery and falsification of electronic documents, and others. In addition, an organizational digital signature authentication system (Government Public Key, or GPKI) for stable distribution infrastructure was built and operated. The report also describes national security certification by the Information Sharing & Analysis Center (ISAC) in Korea.

2.2 Central Ministries regarding Cybersecurity

2.2.1 National Security Office under President's Office

There have been many cyberattacks in Korea. North Korea had disrupted cyberspace long before South Korea had a cyber-defense system. The July 7, 2009, DDoS incident was the prelude to the cyber war on the Korean Peninsula. The National Intelligence Service, led by the Internet network and government administration network segregation project, used this opportunity to carry out a national cybersecurity project.

The March 20, 2013, cyber-terrorism attack, which caused nearly 860 billion won of direct and indirect damage, sounded another big alarm, and the government introduced a strengthened security system. At around 8:25 AM on the 8th of March, the information protection day, "John" of the anti-nuclear group, presumed to be North Korean hackers, released design drawings, image files, and official documents related to nuclear power on Twitter, causing a huge stir in Korea.

After this series of cyber threats, in April 2015, NSO, which assists the president of the Republic of Korea on matters of national security, established a cybersecurity secretariat to assist the President in centralizing the cybersecurity performance system. In July 2017, NSO presented the goal of strengthening the capability of responding to cyber threats by announcing a five-year plan for national administration.

In August 2018, NSO Office combined the intelligence secretariat and cybersecurity secretariat to reorganize into a cyber information secretariat to improve efficiency and prevent duplication of effort. On April 3, 2019, NSO announced a national cybersecurity strategy that included medium- to long-term policy directions on cybersecurity. Nine national agencies, including the MSICT, NIS, and Ministry of National Defense, prepared a national cybersecurity plan and reported it to the State Council, which was confirmed on September 3, 2019. An action plan will be implemented at the pan-governmental level.

2.2.2 National Intelligence Service

The National Intelligence Service (NIS) was established as an agency that reports directly to the president that is responsible for information and security affairs regarding national security. In 1961, the president set up the Central Intelligence Agency, and the names and functionality of the agencies were changed from those in the previous administration.

TABLE 3 **NAMES OF NATIONAL INTELLIGENCE AGENCIES IN KOREA**

CHRONOLOGY	AGENCY	PRESIDENT
1961. 9 ~ 1981	Korea Central Intelligence Agency (KCIA)	Park Jung Hee
1981 ~ 1998.12	National Security Planning Agency (NSPA)	
1998~ 1999		Kim Dae Joong
1999. 1 ~ 2008. 10	National Intelligence Service (NIS)	
2008.10 ~ 2016. 6		Lee Myoung Bak
2016. 6 ~ 2021. 6		Park Geun Hyae
2021. 6 ~		Moon Jae in

Source: self design.

The NIS performs prevention and response to cyberattacks targeting public sector and cybersecurity-related information affairs. It is governed by the National Intelligence Service Act and regulations on cybersecurity affairs. The NIS collects, prepares, and distributes cybersecurity-related information on international and domestic hacking organizations. In the performance of its duties, the NIS may investigate through surveys, document inspection, sampling, or requests for submission of materials. In addition, the NIS can request communication data under the Telecommunications Business Act and communication restricting measures for national security, and it may request communication confirmation data under the Protection of Communication Service Act.

The NIS has built and operated the National Cyber Threat Intelligence (NCTI) since 2015.

Secondly, the NIS has built and operated the National Cyber Threat Intelligence (NCTI) since 2015. In October 2020, the NIS opened the Internet-based Information Sharing System (KCTI) separately from the existing NCTI. About 300 public institutions participated, and KCTI provided cyber threat information to 13 key defense companies in Korea. Since September 2021, 96 private companies have been receiving KCTI information-sharing services, including 37 defense companies, 35 companies with core technology, 7 pharmaceutical/bio companies, and 17 energy-related companies.

Defense companies receive system access rights such as ID and password from the NIS to access the system, check cyber threat information, and

respond to various threats. Although there have been cases in which NIS has provided emergency threat information or accident investigation results to the private sector individually, KCTI is the first system established to provide stable and continuous support for cybersecurity. In addition, the system automatically transmits cyber threat information such as hacking attack types, IP addresses, and the latest malicious codes accumulated in the existing public institution target system (NCTI) to the private sector system (KCTI).

The NIS collects and assesses information at home and abroad related to national security, including cybersecurity, and reports it to the National Security Council (NSC) under Article 10 of the National Security Council Act. The NIS may take countermeasures related to cybersecurity to check, contain, and block activities of North Korea, foreign countries, foreigners, and foreign organizations that threaten national security in order to protect the safety of people.

NIS may prevent and respond to cyberattacks and threats in the public sector under the National Intelligence Service Act's regulation on cybersecurity affairs and security affairs. In addition, NIS prevents and respond to cyberattacks or threats targeting central administrative agencies (including agencies affiliated with a president and a prime minister), its affiliated central ministries, the National Human Rights Commission of Korea, the Corruption Investigation Office for High Ranking Officials, committees affiliated with an administrative agency, local governments and their affiliated organizations, public institutions under the Act on the Management of Public Institutions, major special corporations including local public corporations, the Bank of Korea, public schools, and government-funded research institutes.

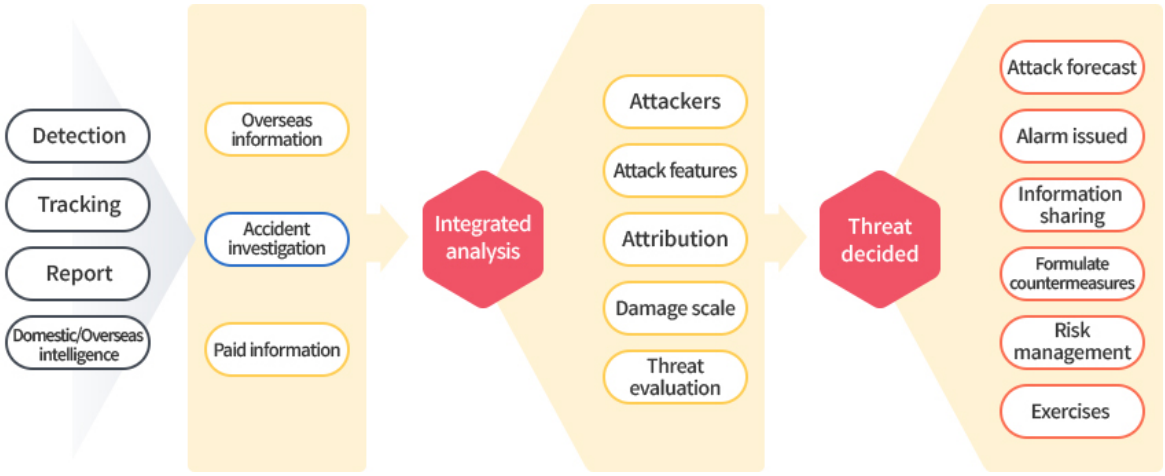
NIS may investigate the establishment and implementation of basic measures for cybersecurity. These include examination of security, verification related to the introduction and operation of the information protection system, security management consulting, education and training, actual status assessment, the establishment of a government security control system and security control targeting central administrative agency and warning, if a cyberattack occurs, investigation of attackers, analysis of the cause, and investigation of the damage.

The NIS established the National Cyber Security Center (NCSC) in February 2004 to provide comprehensive and systematic prevention of and response to cyberattacks such as the one on January 25, 2003, which caused chaos throughout the internet. The agency's name was changed to National Cyber Security Center (NCSC) on January 1, 2021, in accordance with the revision of the National Intelligence Service Act and the enactment of regulations on cybersecurity affairs. If needed for the operation of the NCSC, the director of the NIS may request cooperation from the head of the central administrative agency, such as the deployment of public officials or executives and staff members. In addition, under the NIS, National Security Research Institute (NSRI), affiliated with Electronics and Telecommunications Research Institute (ETRI), is designated as a specialized institution.

As an example, COVID-19 presented a nationwide crisis and the NCSC administered cybersecurity measures for all government institutions. NSCS's role was to develop response technologies in cooperation with specialized R&D centers to deter new cyber threats and to be equipped with defense competency against cyberattacks.

FIGURE 2

THREAT INFORMATION ANALYSIS AND DETERMINATION PROCESS IN NCSC



Source: NCSC (2022).

2.2.3 Ministry of Science and ICT

The Ministry of Science and ICT (MSICT) is responsible for protecting information in the private sector. It constructs and operates a system of prevention of and response to infringement incidents, makes recommendations for information and communication infrastructure in the private sector, analyzes and assesses weak points, and establishes and promotes policies regarding electronic authentication, the information protection industry, and the human resources in charge of information protection. Its work is based on relevant laws including the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.

After enacting the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc., Korea has mandatory protection measures to secure the stability of information and communications networks and reliability of information and countermeasures against infringement incidents. Private-sector cybersecurity incidents can have serious repercussions nationwide.

In 2017, a government reorganization changed the name of the Ministry of Science, ICT, and Future Planning to the Ministry of Science and ICT (MSICT).

In March 2013, the information protection functions that had been under the Ministry of Knowledge Economy, and Korea Communications Commission were transferred to the Ministry of Science, ICT, and Future Planning. In 2017, a government reorganization changed the name of the Ministry of Science, ICT and Future Planning to the Ministry of Science and ICT (MSICT).

MSICT promotes policies designed to build a safe cyber environment. It alleviates people's fears by making cybersecurity a government priority. It continuously monitors abnormalities in the domestic internet and detects malicious codes in 3.4 million domestic accounts. For example, if a personal computer has been infected with malicious code, MSICT immediately notifies the owner to minimize the damage.

For example, in 2017, MSICT analyzed *WannaCry* Ransom Ware in its incipient stage. That ransomware spread throughout the world simultaneously and infected over 300,000 systems in 150 countries. MSICT prepared a countermeasure to minimize damage at home, limiting the

damage to only 21 cases. In addition, MSICT endeavors to expand country-wide information protection systems and enhance the blocking ratio of malicious code and applications to prevent and respond to sophisticated cyberattacks such as Advanced Persistent Threat.

To proactively respond to a sophisticated cyber threat, the number of organizations that share cyber threat information increased from 230 in 2018 to 260 in 2019. They conducted cyber safety diagnoses for 1,200 facilities, enterprises, and internet services in four fields in the private sector (multiple use service, main information and communication infrastructure, information protection management system authentications, and Webhard).

MSICT contributes to expanding cyber safety networks for infrastructure for people's living by recommending organizations. Important facilities in the private sector such as information and communication, financial institutions, and public transportation can be designated as the main (critical) information and communication infrastructure. In addition, MSICT implements an information security and personal information management system (ISMS-P), which contains both the information security management system (ISMS) and personal information management system (PIMS). In this way, enterprises can prevent infringement incidents and enhance the ability to protect information.

To prepare a new information protection industry, in September 2017, MSICT built an information protection cluster in the second techno valley in Pangyo, Gyeonggido. Interested parties such as information protection-related enterprises, universities, and research institutions exchange information and share knowledge, providing an environment to support the development of outstanding information protection products and services and nurture would-be entrepreneurs and startups. In 2020, an office space in the information protection cluster was set up for 20 enterprises. Information protection testbeds, product display halls, training centers, and others have been built to invigorate the domestic information protection industry.

To expand the convenience of new electronic signatures and eliminate discrimination between accredited and private certificates, MSICT amended the Digital Signature Act. MSICT operates an evaluation

and authentication system that confirms electronic signature safety, reliability, and security. An evaluation and authentication system checks the safety, reliability, and security of electronic signatures to help people select the most appropriate means of electronic signature. For example, an electronic signature authentication operator may be issued a certificate that certifies compliance with the standard for electronic signature authentication operation after gaining approval from KISA, the authentication agency, and undergoing an assessment of compliance with the standard for electronic signature operation from the assessment agency.

MSICT introduced an information protection product evaluation and authentication ("CC authentication") system to improve the reliability of information protection products and enhance security. MSICT has operated a CC authentication system since 2014. There have been problems of the lack of experience and understanding of the CC authentication system and method, congestion of CC evaluation, and software security patch reassessment.

MSICT endeavors to alleviate the burden of authentication by establishing and operating system improvement T/F (including MSICT, the organizations concerned, information protection enterprises, the authentication agency, and the assessment agency) starting in June 2020 by preparing CC authentication system improvements. These include training on the CC authentication system targeting startup firms and consulting services, educational program support for training assessors, the establishment of an integrated information guidance site, the expansion of requirements for approval for the change, and extension of the expiration date for domestic CC certificate and its implementation.

MSICT announced a second plan for promoting the information protection industry (2021~2025) in June 2020 to nurture demand for information protection.

MSICT announced a second plan for promoting the information protection industry (2021~2025) in June 2020 to nurture demand for information protection. This is essential to expand online services due to the digitization of industry arising from the COVID 19 pandemic. In June 2020, the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. was revised to strengthen ICT convergence security, including by preparing the legal basis of information protection authentication.

2.2.4
Ministry of Interior and Safety

The Ministry of Interior and Safety (MoIS) has the function of protecting information based on relevant laws, including the Framework Act on National Informatization, the Electronic Government Act, and the Act on the Protection of Information and Communications Infrastructure. It built the National Information Resources Service (NIRS), the Korea Local Information Research & Development Institute (KLID), and cyber infringement response centers in 17 cities and provinces to strengthen the capacity of digital government to respond to cyber infringement.

In addition, MoIS collaborates with relevant government and public organizations to respond to the national cyber crisis after the distributed denial of service (DDoS) attack on July 7, 2009. To strengthen the capability to respond to DDoS for information systems in the national information network, the MoIS built a big data analysis and proactive information protection system (*nAEGIS*), including real-time packet analysis, DDoS attack blocking, and cyber shelter. It also constructed a next-generation cyber response system step by step as an artificial intelligence-based cyber infringement automatic response system.

To strengthen security management of the main infrastructure in local governments, such as urban railways and traffic signals, MoIS designated 102 facilities (as of December 2020) as the main information and communication infrastructure. Moreover, MoIS updated and supplied essential security infrastructure, such as inspections of vulnerability in information system and homepage security, firewalls, and one-way transmission equipment, and implemented training against cyberattacks.

MoIS implements a software development security policy that requires public agencies to apply secure coding starting from the system design stage when they develop digital government systems to prevent security vulnerability of software. It can request data and visit a site to check whether the public agency is applying the policy. To nurture experts in the diagnosis of software security vulnerabilities, MoIS provides education to train workers and public administrative staff.

MoIS prepared a grading system that classifies information systems into five grades according to the importance of the data and the service and applies security management differently according to grade. It applied the system to some central departments and metropolitan organizations on a trial basis and is preparing to expand it to all agencies. MoIS holds briefing sessions by region and informs attendees of security management standards according to the information system grade system.

MoIS prepared a next-generation authentication system to improve convenience and strengthen security. MoIS introduced the mobile identification card of a public official as the first gateway opening mobile identification card age that enables proof of identity online/offline and operates it. Public officials can enter a government office building and smart work center using a smartphone equipped with a mobile identification card of a public official and log-in work system such as integrated public official mail without government public key infrastructure (GPKI). In addition, MoIS plans to create a mobile driver's license for people who have a mobile identification card of official public service that is undergoing technical supplementation and verification.

MoIS has made a considerable effort to strengthen human capacities in organizations related to information protection in central departments, local governments, and public institutions. In addition, it set up organizations in charge of information protection in each institution to improve expertise and responsibility for information protection. It collaborates with each institution so that staff can be allocated properly and operates a national competence standard-based information protection training course to strengthen the capacity of the person in charge of information protection according to their duty level.

2.2.5 Financial Services Commission

The Financial Services Commission (FSC) protects users of electronic financial transactions, develops information security policy in the electronic area, and improves systems based on relevant laws, including the Electronic Financial Transaction Act. After the NH computer network

failure in 2011, the FSC asked financial companies to designate a chief information security officer (CISO) to manage information protection in every organization. After cyber terrorism occurred on March 20, 2013, the FSC added provisions of analysis and assessment of the vulnerability of electronic finance infrastructure, and instituted prohibition of electronic infringement and countermeasures against infringement.

FSC prepared comprehensive countermeasures for preventing the recurrence of a personal information leak in finance in collaboration with FSS-related organizations and finance associations.

Following a personal information leak incident at a credit card company in January 2014, FSC prepared comprehensive countermeasures for preventing the recurrence of a personal information leak in finance in collaboration with FSS-related organizations and finance associations. FSC prepared guidelines on the destruction of personal information, improvement in personal information acquisition forms and third-party consent, improvement in the practice of excessive exposure of resident registration numbers, construction of a system requesting suspension of credit inquiries, and conversion of terminals with enhanced security functions at credit card member stores. In addition, FSC inspected the actual state and level of customer information protection by financial companies and related organizations and took countermeasures. In addition, FSC revised regulations on electronic financial supervision to strengthen control of businesses and designated and operated a day of information security inspection to strengthen personal information protection in the financial world.

In 2015, FSC abolished the regulation on the requirement to use public certificates during electronic financial transactions in the private sector. Accordingly, financial companies can autonomously apply means of authentication based on safety and convenience when adopting transaction authentication. After the regulation was abolished, using various means of authentication in place of public certificates such as biometric authentication and authentication using mobile phone SMS and QR code has increased. FSC continues to improve systems and practice to strengthen authentication based on new technology such as blockchain.

In 2016, the regulation was improved in the financial world so that the cloud could be used. In 2018, a plan to increase the use of the cloud in the financial world was announced. It expanded the scope of information stored in the cloud on personal credit information and unique identification information. This enabled FinTech enterprises to use the

cloud without special restrictions. It enabled financial companies to test big data and artificial intelligence technology freely by using a cloud platform, which makes it possible for innovative services to be launched. FSC prepared a standard for using and providing cloud services in the financial world to strengthen safety management.

As the magnitude of the damage from voice phishing has increased, in December 2018, FSC shared cybersecurity knowledge regarding financial fraud with central ministries and inspected the state of voice phishing. FSC strengthened its responses to voice phishing and cloned bankbooks. It implemented educational efforts to enhance awareness. In 2020, FSC announced a comprehensive plan (2020.6) for eliminating voice phishing to build a foundation of trust in the digital economy by responding to sophisticated voice phishing skills, such as malicious applications.

FSC also announced a comprehensive plan (2018.3) for data use and information protection in the field of finance to enhance people's trust by invigorating data use and protecting the rights of principals of information substantially. It also announced a plan (2018.5) for personal information protection in the field of finance as a follow-up measure for the comprehensive plan and revised the Credit Information Use and Protection Act (2020.2) to introduce an information protection assessment system and an information use consent grading system in the financial world so that personal credit information can be processed safely and reliably.

In addition, FSC provides a basis for the private sector-centered autonomous security system to be established as the FinTech industry has invigorated. It modified regulations on financial security, including the abolition of the preliminary security review system (2015.6), the abolition of the requirement of using a one-time password when transferring funds electronically (2016.6). FSC announced a plan (2017.3) for introducing a financial regulation testbed aiming to support experiments with innovative financial services. It supports improvement in security using new security technology and improvement in user convenience, such as support to the commercialization of blockchain joint authentication services.

There has been confusion regarding the functions of the FSC and the Financial Supervisory Service (FSS) in Korea. The main difference is that the FSC is a government department (a central ministry), while the FSS is a public institution. FSC is a committee under the Prime Minister's Office. All of its staff are government officials. On the other hand, the employees of FSS are not public officials. FSC is involved in financial administration and plays a role in making policies within a broad framework. Major policies were introduced in the media, including finances for the working class, technology finance, and fintech. FSC does not directly oversee and inspect individual financial companies. Instead, FSS provides legal and institutional procedures to monitor and inspect them.

2.3 Specialized Public Institutions regarding Cybersecurity in Korea

2.3.1 Korea Internet & Security Agency

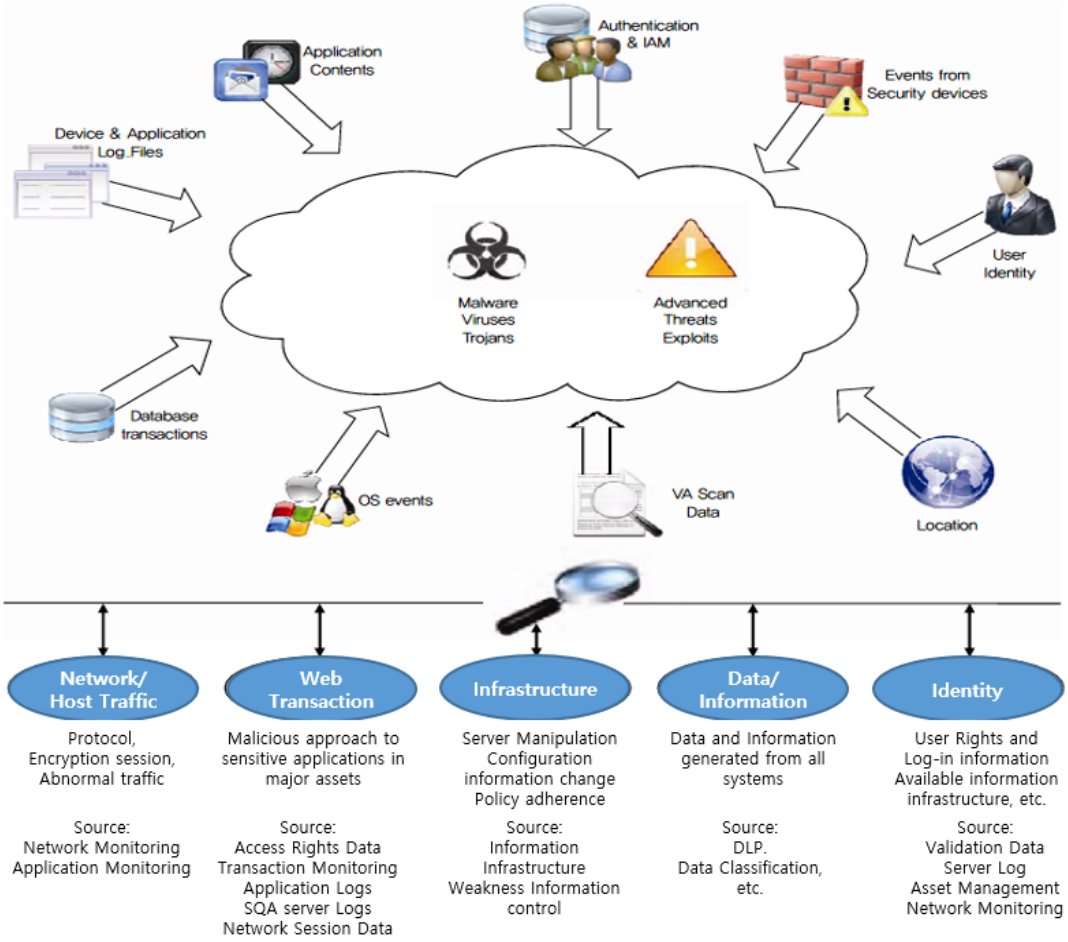
Korea Internet and Security Agency (KISA) assists the information and communication technology (ICT) sector through prevention of and response to cyber infringement, personal information protection, response to damage, building up the information protection industry, training information protection industry workers, providing information protection services to the public, running the national domain (.kr/. Korea) service, settling illegal spam-related grievances, and blockchain to create a safe basis for the Fourth Industrial Revolution based on the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.

KISA operates the Korea Internet Security Center (KISC) and continuously monitors abnormalities of internet traffic in connection with leading

domestic business communications operators and security control enterprises. It also distributes security recommendations to prevent vulnerability. In addition, KISC cooperates globally with related institutions, responds to cyber threats. and distributes computer vaccines customized for small-scale businesses and web vulnerability inspection tools free of charge. KISC operates cyber shelters to provide uninterrupted service in case of DDoS attacks.

KISA has a Cybersecurity Big Data Center that collects and analyzes threat information and shares it with the private sector to strengthen its capability to respond to infringement incidents and develop products based on cooperation between industry, academia, and research support. The Regional Information Security Support Center, which is operated in ten locations in South Korea, including the Honam region (Gwangju) and the Dongnam region (Busan), to build a regional cyber safety network that creates an information protection base by supporting customized information protection services and cooperating with the AI convergence industry (automobiles, energy, and health care) in Gwangju metropolitan city and Busan Blockchain city. Figure 3 illustrates the security analysis technology features using big data (Kim, 2017). The key features are now in use in KISA and other ISACs.

FIGURE 3 **BIG DATA ANALYSIS FOR CYBERSECURITY**



Source: Kim et al. (2017).

TABLE 4 **CYBERSECURITY BIG DATA ANALYSIS TECHNOLOGY ELEMENTS**

AREAS	EXPLANATION
Six technology areas using big data	REAL-TIME MONITORING: A technology that collects and manages data from various sources to track and analyze attack situations on system components or monitor user activity in application programs.
	THREAT INTELLIGENCE: An up-to-date information system on various threats and attack patterns enable a more accurate recognition of abnormal activities. For example, when a small amount of outbound traffic to an external IP is disguised as normal traffic and can be overlooked, it is a technology that recognizes this as threat information related to attack control.
	BEHAVIOR PROFILING: When conditions for anomalies are well defined, it is possible to define association rules to find specific conditions; since it is difficult to detect all anomalous behaviors with a rule-based methodology, behavior profiling-based anomaly detection and analysis is one of the leading technologies.
	DATA & USER MONITORING: Monitoring data/user activity, including users and their context, is an essential skill for intrusion detection and misuse detection; Essentially required to monitor privileged users and access to sensitive data
	APPLICATION MONITORING: Since application vulnerabilities are the main targets of targeted attacks, it is a technology for monitoring the activity of abnormal applications.
	ANALYTICS: A core technology of big data security analysis that analyzes the characteristics of various source information and determines whether there is an abnormality using machine learning, data mining, and network mining techniques, which are traditional methods of big data analysis.

Note: Based on these elements, big data security services by the technology used in Korea are listed in Table 5.

Source: Yoo, 2017.

TABLE 5 **BIG DATA SECURITY SERVICE CATEGORY AND EXPLANATION**

SERVICE CATEGORY	TECHNOLOGY
Big data security data collection/storage technology	STREAMING A technology that enables real-time collection of voice, audio, and video data from the Internet.
	LOG AGGREGATOR Open source technology that collects various data such as web server log, web log, transaction log, click log, DB log, etc.
	RDB AGGREGATOR Open-source technology that collects structured data from a relational database and stores it in NoSQL, such as Hadoop distributed file system.
	DISTRIBUTED FILE SYSTEM A file system that stores files on the local disk of a distributed server and processes operations such as reading and writing files by providing APIs rather than operating systems.
	IN-MEMORY DATA GRID A technology that enables high-speed parallel processing and real-time processing with multiple computers by storing data in the main memory of a distributed server
Big data analysis technology	ASSOCIATION RULE LEARNING A technique for finding the relevance and relevance of interesting topics from various variables in a large database, consisting of a set of algorithms that create and test potential rules
	CLASSIFICATION A technology that can identify the category to which new data belongs based on a training data set that includes already identified data
	CLUSTERING A statistical method for partitioning into small groups of similar individuals in which similarity characteristics are not known in advance.
	ENSEMBLE LEARNING A method of learning new hypotheses by creating multiple classifiers/ combining predictions through the classification method of machine learning.
	GENETIC ALGORITHM A technique for solving optimization problems as a computational model based on the evolutionary process of the natural world.

Big data analysis technology	OUTLIER DISCOVERY Technology that finds outliers in given data and removes factors affecting the whole or analyzes the causes of outliers.
	MACHINE LEARNING A technique for deriving an application model through precise analysis to identify malicious behaviors, find abnormal behaviors according to the hacking behavior cycle in consideration of the correlation between user behavior events, and identify malicious behaviors.
	VISUALIZATION Techniques using images, diagrams, animations, etc., to express the results of data analysis and improve the level of understanding are used as a security technology to counter cyber threats.
Privacy protection technology	PRIVACY-PRESERVING DATA MINING (PPDM) A method of performing data mining by transforming it to protect privacy or using a method to protect it and deriving the result.
	DATA PROTECTION THROUGH MASKING, ENCRYPTION, AND REDACTION If the subject that processes and analyzes the data is malicious, personal information can be easily leaked. To prevent this from occurring, data are anonymized and analyzed to remove personal information. In addition, there is a need for technology capable of deriving useful information while protecting privacy when analyzing big data security using encryption technologies, such as order-preserving encryption and operation-preserving encryption.

KISA uses 5G+ core service security internalization, such as constructing a security living lab to test the security of services such as autonomous vehicles and smart factories, to build a safe and competitive 5G+ core convergence service environment. In addition, KISA provides an IoT security authentication service so that enterprises can produce products with a high degree of security, and users can select safe products.

KISA operates a cybersecurity human resources center to contribute to the development of the State. It builds human capacity in field of information protection, enhancing Korea's global competitiveness and building a security training ecology. In particular, KISA cultivates about 1,500 people of ability every year through a cyber training center (*Security Gym*) and the best cybersecurity worker (*K-Shield*) cultivation project, which aims to cultivate workers who can use convergence security knowledge. KISA has held a de-identification technology competition every year since

2018. It supports training for cultivating experts in false name processing, customized consulting, testbed operation, and others.

KISA takes the lead in settling various ICT disputes and cyber grievances in the age of the Fourth Industrial Revolution. It advises on all problems related to the internet, such as personal information infringement, illegal spam, phishing, and smishing through a free phone call connected to 118 everywhere in the country at all hours.

Finally, My PC Helper service (https://www.boho.or.kr/webprotect/pcSecCheck.do) inspects the PC security of the personal user. KISA's ICT Dispute Settlement Support Center settles disputes in the areas of electronic transactions, internet addresses, the information protection industry, and online advertising through advising and mediation to enhance safety and solve problems of inconvenience.

2.3.2

National Security Research Institute

The National Security Research Institute (NSRI), established in 2000, specializes in information protection based on the Act on the Establishment, Operation and Fostering of Government-Funded Science and Technology Research Institutes, etc. NSRI conducts research and development for cybersecurity in the public sector, research on cryptography, responses to hacking, and construction of the related foundation. NSRI continues to widen the scope of security technology research and development, responding to technical developments such as unmanned vehicle threat analysis and strengthening cloud reliability. In addition, NSRI performs research on policy for cybersecurity and provides it to affiliated institutions.

NSRI has operated Cybersecurity Training and Exercise Center (CSTEC) since 2014, aiming to improve the ability to respond to the national crisis at the national level to foster competent people after recognizing the importance of cultivating capable people for strengthening cybersecurity at the national level. The center provides the curriculum of cyber crisis

prevention, safety checks and evaluation, cyber threat detection and response, incident analysis and measures, and actual training. In addition, it develops new training content to respond to cyberattacks targeting future technologies such as smart cars and robots. NSRI also conducts research and development to obtain training centers and online training technology to implement international cyber joint training with international communities.

2.3.3 Financial Security Institute

The Financial Security Institute (FSI) was established in April 2015 with the Information Sharing and Analysis Center (ISAC) functions.

The Financial Security Institute (FSI) was established in April 2015 with the Information Sharing and Analysis Center (ISAC) functions. FSI shares and disseminates information on vulnerability and infringement factors of information and communications infrastructure in the field of finance, operating real-time infringement warning and analysis systems, analyzing and evaluating the vulnerability of main information and communications infrastructure, and supporting the establishment of a countermeasure for protection, such as Finance ISAC, under the Act on the Protection of Information and Communications Infrastructure.

FSI responds to infringement, including establishment and operation of infringement information sharing system, forecasting and warning of infringement, operation of the integrated security control center in the financial world, investigation and analysis of infringement, collection and analysis of high-risk malicious code, establishment and operation of a DDoS attack emergency response center, and implementation of an infringement emergency response drill as an agency to respond to infringement under regulation on electronic financial supervision.

In addition, FSI analyzes and evaluates the vulnerability of electronic financial infrastructure, supporting financial companies' inspection of vulnerability and supporting subsidiary electronic financial business operators' inspection of vulnerability as an agency specializing in analyzing and evaluating vulnerability. In addition, since 2019, FSI has supported the safety assessment of cloud service providers that financial companies intend to use. FSI supports the prevention of cyber

infringement and the spread of damage through early detection of new vulnerabilities that threaten electronic financial transactions by implementing bug bounty in the financial world and producing and sharing cyber threat intelligence reports.

FSI builds and operates a fraud detection system (FDS), which allows abnormal financial transaction information in a financial company to be shared with other financial companies and detects and blocks malignant file attacks early by building a real-time malignant file detecting system. In addition, through a comprehensive plan for eradicating voice phishing, FSI organized an FDS task force in charge of advancing FDS centering around commercial banks and large-sized electronic financial business operators and operated it to prepare a technical solution to prevent and respond to voice phishing. It builds a worldwide voice phishing fraud information-sharing system to improve responses to new voice phishing fraud.

Since 2019, FSI has operated financial security RegTech[3] portal (regtech.fsec.or.kr). The portal has provided financial security services such as financial security compliance automation, intelligence retrieval and warning, automatic creation of the report, and a financial security counseling service to support financial companies' compliance with regulation and to strengthen the capability to respond to regulation. It developed and distributed a financial security-related guide, and it is standardizing financial security through the operation of a financial security standardization council to support financial companies' ability to strengthen autonomous security capability.

FSI supports improvement in awareness of information protection by investigating and sharing financial security statistics and exemplary cases, announcing prospects for digital finance and cybersecurity issues, operating the financial information protection council and financial security forum service bureau, holding financial information protection conference (FISCON) and financial security contests, holding seminars inviting chief executive officers from financial companies, and publishing a quarterly journal, *Electronic Finance and Financial Security*.

3 "RegTech" is a compound word of regulation and technology. It connotes a service/technology that manages and complies with financial-related regulations using various technologies.

CHAPTER

3.

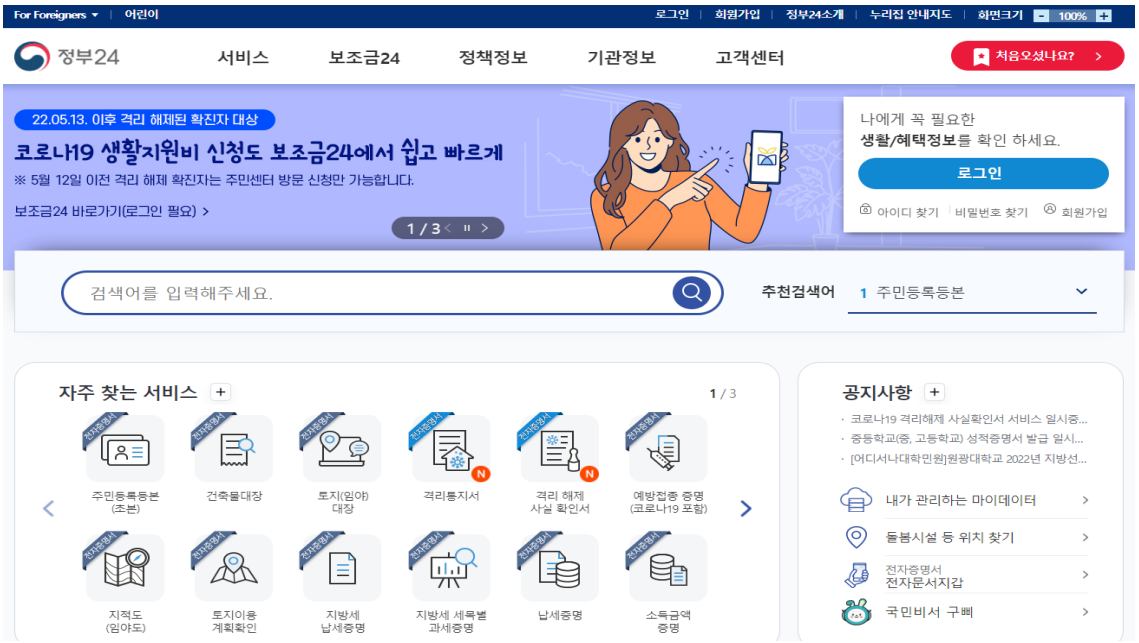
E-Government Infrastructure for Cybersecurity

National Cybersecurity Law, Governance, and Infrastructure in the Republic of Korea

3.1 E-Government Infrastructure of Korea Overview

3.1.1 E-Government System

FIGURE 4 **E-GOV PORTAL INTERFACE**



Source: www.egov.kr.

The Korean e-government system is well known as a world-class e-government system. In 2020, the United Nations' e-Government Evaluation ranked Korea second in the e-Government Development Index (1) among 193 member states, and ranked three countries first in the online participation index (Korea, the United States, and Estonia). These e-government resources are being effectively used for the COVID-19 pandemic response in Korea. Nine out of 10 people use e-government

services, and the satisfaction rate is 97.8 percent, as reported in the 2021 e-Government Service Usage Survey (Korea Policy Briefing, 2022).

The Korean government has introduced approximately 19,000 e-government services, many of which have received global praise and recognition. Furthermore, Korea's e-government has enhanced the efficiency and transparency of the public sector, significantly improved services for citizens, and expanded citizens' opportunities to participate in the policy-making process.

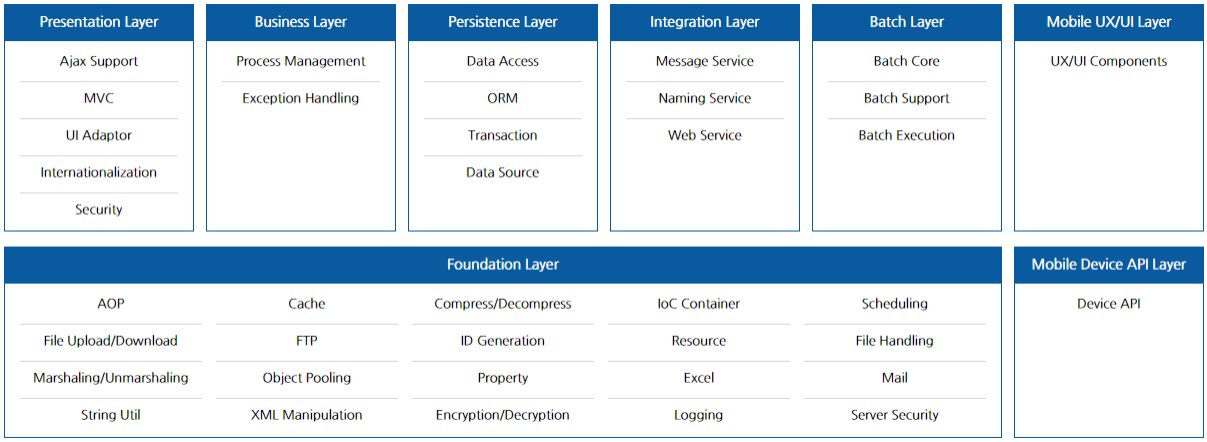
TABLE 6 **E-GOVERNMENT HISTORY AND MAJOR ACHIEVEMENTS**

	PRESIDENT KIM DAE JOONG	PRESIDENT ROH MOO HYUN	PRESIDENT LEE MYOUNG BAK	PRESIDENT PARK GEUN HYE	PRESIDENT MOON JAE IN
Time	1998~2003	2003~2008	2008~2013	2013~2017	2017~2022
Task Name	E-government 11 Strategies	E-government Roadmap and 31 Strategies	National e-Gov Strategies (no specific name)	National e-Gov Strategies (no specific name)	National e-Gov Strategies (no specific name)
Major Goals	Electronic processing of government affairs and public services	Multi-ministerial service linkage	Capable and knowledgeable government	Information disclosure, sharing, and collaboration	Implementing intelligent government
		Expanding Electronic Citizen Participation	Administrative service linkage and integration	competent government	
Major Out-comes	Establishment of a single window for civil complaints (Minwon 24)	Online public participation (Kookmin Shinmungo)	Expansion of joint use of administrative information	The original information disclosure system	Promotion of issuance of Blockchain-based electronic certificates
	Internet comprehensive national tax service (Hometax)	Comprehensive National Customs Network and National Welfare Service	e-Government Standard Framework (eGovFrame)	Open national information resources and build a public data portal	Expansion of the cloud-based business system
	Establishment of electronic approval and distribution of electronic documents	Establishment of an integrated criminal justice information system	Pan-Government Information Technology Architecture (EA)	Integrated administrative service provision (Government 24)	Establishment of public secretarial service

Source: Ministry of Interior and Safety (2022)

The e-government system in Korea is mostly built on the standard development framework known as the eGovFramework, a platform-specific standardized development framework for public sector IT projects in Korea. Developed by the Korean government, it can be used by every person worldwide. The Runtime Environment is the foundation of software applications and provides the basic functionality required to run enterprise applications composed of 8 service layers and 39 services.

FIGURE 5 **EGOVFRAME RUNTIME ENVIRONMENT**



Source: www.egoveframe.kr

The Development Environment of the e-Government Standard Framework (eGovFrame) is a collection of development tools for effectively using various functions provided by the Runtime Environment to develop more precise and efficient applications. The environment is composed of four service toolsets.

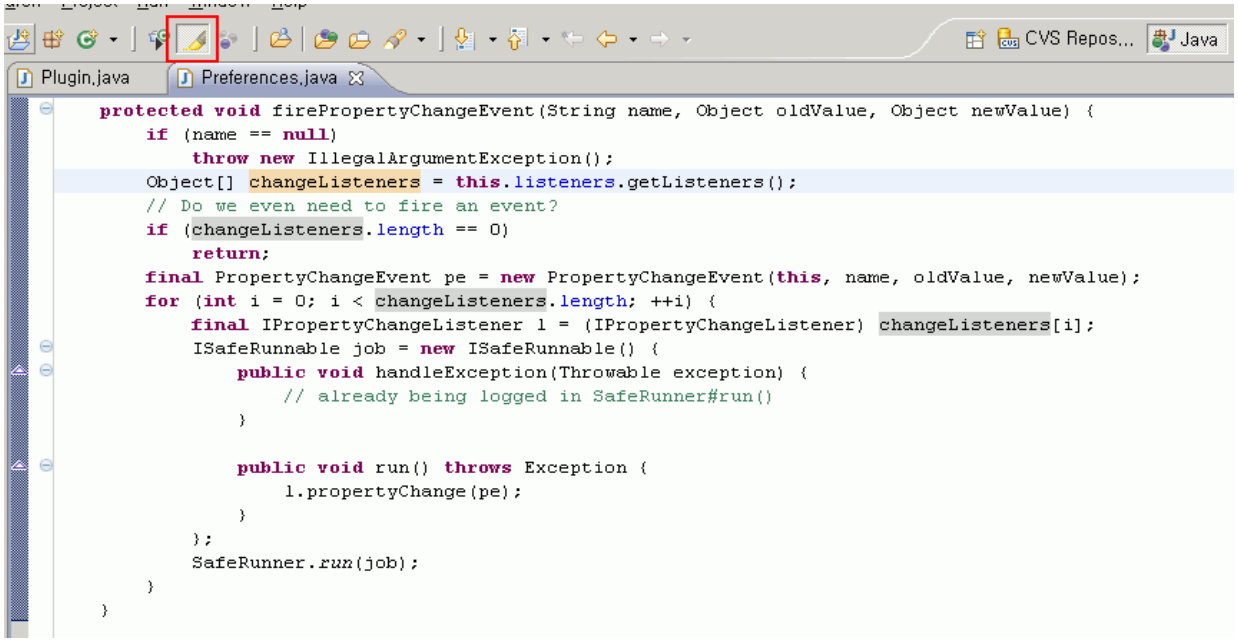
TABLE 7 **EGOVFRAME DEVELOPMENT FRAMEWORK**

CATEGORY	TOOLSET
Implementation Toolset	As a collection of tools for supporting the coding process provides several tools such as Editor, Debug and Methodology & Template.
Test Toolset	As a collection of tools for testing the written code provides several tools such as Unit Test, Test Automation, Test Coverage, and Test Reporting.
Build Toolset	As a collection of tools for compiling, building and deploying the written code and it provides Build and Deploy functions.
Configuration Management Toolset	As a collection of tools providing (1) Configuration Management Tool for identifying configuration item attributes, registering them and managing the changes, and (2) Change Management Tool for registering and searching configuration issues.

Source: www.egoveframe.kr.

The eGovFrame is developed based on Eclipse, which is an integrated development environment (IDE) based on Java created by the Eclipse Foundation. The eGovFrame also provides additional functions for the e-Government Framework, such as Perspective, Menu, and New Project Wizard, in addition to Eclipse's basic functions, such as Code Assist, Quick Fix, Loading Code Style, Code Templates, String Search, Quick Type Hierarchy, Quick Outline, Source Code Navigation, Mark Occurrences, and Local History.

FIGURE 6 EGOVFRAME JAVA CODING EXAMPLE



Source: www.egoveframe.kr

A common component is a set of components developed focusing on functions that can be reused in common when constructing an information system Table 7. These common components make coding easier for easy customization and reuse in e-government projects.

TABLE 8 **COMMON COMPONENTS OF E-GOVERNMENT SYSTEMS**

CATEGORY		DETAILED FUNCTION
Common technical service (136 types)	Security	8 types, including real name verification, authority management, encryption/decryption, etc.
	User directory/ integrated authentication	3 types, including general login, certificate login, and policy management.
	User Support	55 types, including user management, consultation management, survey management, FAQ, Q&A, etc.
	Collaboration	8 types, including a bulletin board, blog management, community management, address book management, etc.
	System Management	27 types, including common code, menu management, log management, institution code reception, etc.
	System/Service Integration	4 types, including management of the connection status, affiliated organizations, etc.
	Stats/Reporting	6 types, including post statistics, access statistics, report statistics, etc.
Element technology service (utility) (104 types)		104 types, including calendar, format/calculation/ conversion, number validity/format validity check, etc.

Source: www.egoveframe.kr

Almost every system these days, especially for government information systems, including cybersecurity systems in Korea, is built based on the eGovFrame standard framework for development.

3.1.2 Government Communication Networks

Government networks can be segmented into K-Net, Individual Communication Networks, and the National Information and Communication Service (a.k.a. GNS). National Backbone Network (K-Net) was built in 2009 as a broadband transmission network leased by the Ministry of Government Administration and Home Affairs to distribute

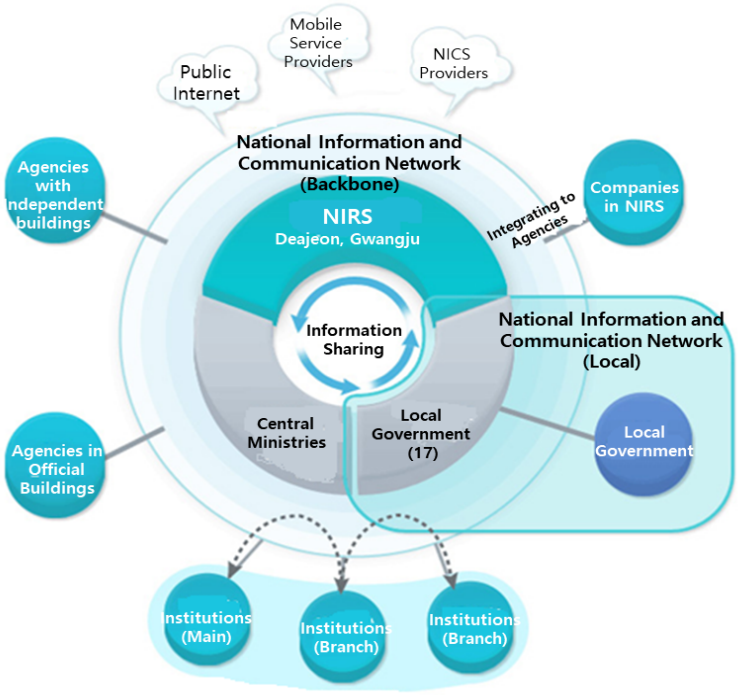
information, including electronic document distribution between administrative agencies, the National Financial Information System (dBrain), and Internet use. It is being used to connect and jointly use national institutions by connecting the government integrated computer center, government complexes, and 17 metropolitan cities and provinces.

The individual communication network is a dedicated communication network operated separately by 29 ministries by renting a line from a telecommunication company to connect the headquarters, regional offices, and government offices. The Ministry of Land, Infrastructure and Transport operates the Land Transport Information Network. The Ministry of Employment and Labor operates the integrated network of the Ministry of Employment and Labor. The public procurement administrative network of the Public Procurement Service, the meteorological observation network of the Korea Meteorological Administration, and the patent network of the Korean Intellectual Property Office are also individual communication networks for each department.

The National Information and Communication Service (GNS) is a system that standardizes the technical requirements, fees, and service contents related to information and communications networks.

Finally, the National Information and Communication Service (GNS) is a system that standardizes the technical requirements, fees, and service contents related to information and communications networks. Local governments form a national information communication network for each region that connects metropolitan cities and provinces to cities. The governmental backbone network monitors the inflow of unnecessary traffic from administrative agencies in advance. It provides various service bases to administrative agencies by linking with GNS operators and internet service operators. The government network is described in Figure 7.

FIGURE 7 **NATIONAL INFORMATION COMMUNICATION NETWORK**



Source: www.gns.kr

Administrative institutions use national information and communications services and national information and communications networks to configure communication environments for individual communications networks, inter-agency connections, and commercial internet access, to perform administrative tasks and provide services to the public. In addition, NICS is a national communication network established by private telecommunications service providers that provide quality-guaranteed telecommunications services at low cost to administrative agencies.

TABLE 9 **NATIONAL INFORMATION AND COMMUNICATION NETWORK SERVICE CATEGORY**

CATEGORY	PROVIDERS	SERVICE AREAS
A Group	KTsat, KT Consortium, LGU+, CJ Hello Consortium, SKB, SKT Consortium	Dedicated Network, Backbone Network
B·C Group	KT, SKB, LGU+, CJ Hello Consortium	Internet, Internet Phone, Mobile Internet Phone
D Group	KT, SKB, LGU+, CJ Hello Consortium	Wireless Data Service, IoT Service
E Group	KTsat, KT Consortium, LGU+, CJ Hello Consortium, SKB, SKT Consortium, Dreamline, Sekyoung Broadcasting	CCTV Service

source: www.gns.kr

3.1.3 Government Integrated Data Center

Since the 1990s, when Korean government ministries began adopting e-government systems, they have made great strides. However, problems have arisen caused by redundant investment in computing resources, lack of expertise, a poor computing environment, and security vulnerabilities. In 2005, to comprehensively address some of these issues, the Korean government established a data center dedicated to government use. This center was the first of its kind in the world. The Government Integrated Data Center (GIDC) is the core infrastructure for information resource management.

GIDC integrates, operates, and manages over 1,400 e-government systems. These systems had previously been operated individually by 44 central government organizations. Data Center 1 was established in Daejeon in 2005, and Data Center 2 in Gwangju in 2007. The first process that GIDC performed was to relocate all the servers and hardware to one place. Gradually, it integrated the software and services and now provides customized services to users.

FIGURE 8 **DAEJEON GIDC OPERATED BY NIRS**

Source: www.nirs.kr

GIDC integrates, manages, and operates over 47,000 hardware and software components for 44 central government ministries. A large-scale system is managed in real-time using 'n-TOPS,' an integration and operating system developed with Korea's technologies. Furthermore, GIDC is a hub for cybersecurity. In addition, GIDC protects national IT resources from various cyber threats. By using 'e-ANSI Sung,' an integrated security system developed internally, GIDC can block hacking attempts, viruses, DDoS attacks, and other cyber threats from accessing e-government systems.

Furthermore, GIDC developed a resource pool through integrated purchases of all IT resources that each government organization needs. Simultaneously, it developed a cloud-computing environment, where government organizations can borrow hardware or software through the internet. Integrated operation of e-government systems significantly reduced the average monthly failure time per piece of equipment, decreasing it from 67 minutes before GIDC was built to only 4 minutes in 2014.

Also, integrated security measures allow it to protect against cyber threats, from DDoS attack detection to block, in only 20 minutes. Now that government ministries do not have to develop and operate their systems but can rely on systems put into place by e-government and access information resources as needed, the cost for development and operation has decreased by 30 percent (MoIS, 2022).

FIGURE 9 **GWANGJU GIDC OPERATED BY NIRS**

Source: www.nirs.kr

The international community is evaluating GIDC as an ideal e-government model. It won the FutureGOV Award in the area of data centers in 2010 and the IT Governance Excellence Award from the ICT Service Management Forum in 2011. About 400 high-level public officials learn about GIDC each year. GIDC was exported to Mongolia and Nepal in 2007 and Vietnam in 2011.

FIGURE 10 GIDC CONTROL CENTER

Source: www.nirs.kr

3.3 Protecting E-Government Infrastructure of Korea

3.3.1 E-government Cybersecurity

Korea ranked top 10 in the world UN e-government evaluation from 2005 to 2008. It brought many changes to people's actual lives. For example, applying for a passport required seven documents, including a resident registration card, two photos, a copy of resident registration, an abstract of resident registration, an overseas travel permit, and a copy of the family register. The applicant had to visit a district office and the regional military

manpower office. These documents had to be submitted to the passport issuance office. The period between application and passport issuance was extensive. With the introduction of the e-government system, information sharing between administrative agencies has become smooth, and applying for a passport now requires only an application and a photo. In addition, there are fewer documents to prepare and fewer visits to administrative agencies. In 2006 alone, 30 million fewer documents were required, amounting to a savings of 180 billion won.

Since April 2006, the number of intrusion accidents by public institutions has been steadily increasing by 2-3 percent.

Separately, some experts pointed out three areas in e-government that need to be strengthened in Korea. The first was the expansion of the security organization. According to the announcement of the NCSC, since April 2006, the number of intrusion accidents by public institutions has been steadily increasing by 2-3 percent. As the size of the attack increases, the size of the defense organization should also increase, requiring greater elaboration of cybersecurity responses.

The second was that the security controls on the information system should be further strengthened. For example, the contents of the equipment that were opened to the public for e-government services, such as web servers, domain name systems (DNS) servers, and mail servers, were in good security condition, but the internal information system was not. Furthermore, in many cases, patches for known vulnerabilities have not been implemented.

The third was that the system for responding to infringement incidents should be further strengthened for the central administrative agencies, the four major base sections (Seoul, Gwacheon, Daejeon, Seoul government building annex), and the sections connected with local governments. A separate security enhancement plan and data leakage prevention plan should be prepared because there are weak points in the connection section between the central and city-gun-gu. Since 2004, great improvements have indeed been made in security policy, asset management, human security, physical environment security, and access control. However, there is still room for improvement.

Security enhancement was one of the key projects in 2007 set by the e-government. The biggest issue in sharing administrative information was protecting personal information. To protect personal information, only

information obtained with the prior consent of the public can be used jointly. In addition, to guarantee the public's right to make decisions about personal information, details of the shared use of personal information can be checked at any time through the G4C website. In addition, to increase objectivity, if there is a risk of personal information infringement, the Minister of the Interior and Home Affairs can withdraw or suspend the approval of joint use after deliberation by the Administrative Information Joint Use Committee.

The security enhancement plan includes installation of e-government security control centers in 16 cities and provinces with relatively poor security, and strengthening of user authentication and access control systems that apply the latest security technologies. Web firewall installation and e-government security infrastructure expansion were also included in the plan. In addition, to prevent misuse and leakage of information, the number of e-government officials was minimized, and the review of information users' access to information was strengthened. Finally, it was decided to prohibit the storage of key government information on public officials' PCs and keep documents after major policy reports and decision-making on internal servers such as Onnara System. In 2007, the top 10 security measures for e-government services were also announced.

The dependence of national infrastructures such as administration, broadcasting, communications, finance, and energy on ICT has increased due to the development of information and communications infrastructure in 2001. Electronic infringement behavior, such as hacking, malicious code circulation, and DDoS attacks, has emerged as the new threat. MoSICT is responsible for protecting the main infrastructure, as stipulated in the Act on the Protection of Information and Communications Infrastructure.

The Information and Communication Infrastructure Protection Committee falls under the Prime Minister's office. The Committee consists of no more than 25 members, including one chairperson. The chairperson is the head of the Office of Government Policy Coordination. The members of the Committee are public officials at the vice-ministerial level of central administrative agencies prescribed by the Presidential Decree and others commissioned by the chairperson. To ensure the Committee's efficient

operation, there are working committees in charge of the public sector and the private sector, respectively.

Designation of main infrastructure will be based on the following five criteria:

- The national and social importance of the work performed by the agency managing the relevant information and communication infrastructure
- Dependence on information and communications infrastructure for business performed by institutions (stipulated in the law)
- Interconnection with other information and communication infrastructure
- The scale and scope of damage to national security and the economy and society in the event of an intrusion
- Possibility of occurrence of an intrusion accident or ease of recovery

The Act stipulates the prohibition of critical information and communication infrastructure infringement: No one shall engage in the following activities:

- The action of a person who does not have access right to access major information and communications infrastructure, or an act of a person who has access right to manipulate, destroy, hide, or leak stored data over the authority
- Injecting programs such as computer viruses to destroy data on critical information and communications infrastructure or obstruct the operation of critical information and communications infrastructure
- An action that causes an error in information processing, such as sending a large number of signals at once to interfere with the operation of major information and communication infrastructure or illegal process orders

Diverse ISACs monitor these infringement action/network behaviors in ministries including KLID, KISA, FSC, FSI, and others. This information is shared with the upper levels, including the National Cybersecurity Center.

When the head of a management agency becomes aware that major information and communications infrastructure under their jurisdiction has been disrupted, paralyzed, or destroyed due to an intrusion accident, they shall notify the relevant administrative agency, investigation agency, or KISA. In this case, the relevant agencies can take the necessary measures to prevent the spread of damage from the intrusion accident and respond promptly.

Although disturbance or paralysis of main information and communications infrastructure may cause enormous economic losses and social confusion, laws designed to prevent electronic infringement behavior and build response systems are inadequate. Accordingly, the Act on the Protection of Information and Communications Infrastructure was enacted to build the government's response system to protect information and communications that operate the main infrastructure from electronic infringement behavior such as hacking or malicious code.

The enforcement decree, amended in 2012, specified more organizational and operational methods suitable for changes in working committees by reflecting matters entrusted according to the amendment of the Act on the Protection of Information and Communications Infrastructure in December 2007. Matters about a report on the implementation of protective measures by the head of NIS and about the recommendation for designation of main information and communications infrastructure were included. Moreover, some imperfections were improved and complemented. For example, the cycle of analyzing and assessing vulnerability was shortened from two years to one, and the scope of institutions subject to protection by main information and communications infrastructure was expanded.

In 2015, ISAC established the basis to provide technical and financial support to analyze cyber threats.

In 2015, ISAC established the basis to provide technical and financial support to analyze cyber threats jointly by institutions that manage infrastructure and invigorate information sharing.

By 2018, the Information and Communication Infrastructure Protection Committee and its working committee could decide whether a facility can be designated as a main (critical) infrastructure. This is very effective for identifying critical infrastructure and guaranteeing policy penetration.

In 2019, the legal basis provided that in case it is necessary to protect main information and communications infrastructure from cyber threats, a new form of electronic infringement behavior or analysis and vulnerability assessment was needed as a serious change in main information. Communications infrastructure is created, and the heads of central administrative agencies may order the head of the relevant institution to analyze and assess the vulnerability of the main information and communications infrastructure.

Concern about security incidents by programs which enable access to information and communications network detouring normal protection or certification procedures or backdoor entries to technological devices recently were provided as examples of electronic infringement behavior. The following measures were included:

- Establishing measures for the protection of main information and communications infrastructure and checking whether they have been implemented
- Drawing up plans for protection of main information and communications infrastructure centering around relevant central administrative agency
- Designating main information and communications infrastructure and analysis of weak points
- Recommending designation of main information and communications infrastructure
- Protecting and responding to infringement incidents
- Building and operating information sharing and analysis center

CHAPTER

4.

Discussion

4.1 New Cybersecurity National Strategy and Action Plan (2022)

In February 2022, the Korean government announced the Strategic Plan to Foster Cybersecurity Industry. The new national cybersecurity strategy encompasses diverse aspects of information security in the nation. The main elements of the strategy are as follows:

First, the government will create a new cybersecurity market to secure the growth engines of the nation. The new market will be an artificial intelligence-based security market, a non-face-to-face security market, a convergence security market, and others. As cyber threats become more intelligent and advanced, the need for artificial intelligence technology combined with the development of more intelligent security products and services is increasing.

In addition, the global artificial intelligence security market is growing. By 2025, Korea will nurture 60 innovative cybersecurity companies that develop artificial intelligence-based security products and services such as automatic detection and response of security threats and security control automation. In addition, the Korean government has accumulated 800 million cases of information security data composed of malicious code and infringement incident data. The government will open it up so that domestic security companies can use it for cybersecurity product development.

Next is the field of convergence security. There is a need to preemptively respond to security threats in ICT convergence environments such as autonomous vehicles, digital healthcare, and smart factories.

The Korean government is building a convergence security base with five security living labs. Korean cities such as Pangyo, Ansan, Gunsan, Busan, and Wonju plan to build specialized convergence security living labs for testbeds. For example, in Anyang, immersive content security at

the Digital Content Center, smart factory security in Ansan, autonomous vehicles in Gunsan, digital health care security in Wonju, and smart city in Busan were established to provide a convergence security base and link with the Security Living Lab. Therefore, the government plans to develop one-stop package security applications connected with security models for medical devices, automobile convergence security technology, and smart factory technology.

The second strategy is to foster a global first-class cybersecurity company. To commercialize new growth technologies and products, the government supports the development of leading cybersecurity technologies and products based on advanced information security technologies to support the growth of information security companies. As an excellent information protection technology or product, the government can designate it according to Article 18 of the Information Security Industry Act.

The third strategic agenda is support to mergers and acquisitions (M&A). The government plans to nurture information security venture companies to expand their business areas and scale up through inter-company collaboration or M&As.

Unlike previous passive approaches for private company nurturing, the government now plans to promote active collaboration and M&As by inducing collaboration between leading companies with distribution channels and early companies with superior technology. This will lead to integrated security solutions and support domestic and overseas market development together.

The fourth strategic agenda is ecosystem expansion to strengthen the foundation of the cybersecurity industry.

The fourth strategic agenda is ecosystem expansion to strengthen the foundation of the cybersecurity industry. The information protection disclosure system was introduced at the end of last year. For companies of a certain size or larger, it is mandatory to disclose investments in information protection or to secure dedicated manpower. Through this, it will be the purpose of inducing investment in information protection and competitive investment while protecting users' right to know.

The fifth agenda is the expansion and advancement of information security certification. Internet of things (IoT) devices are proliferating.

In response to hacking, the government plans to expand information protection certification to various fields, such as thermal imaging cameras, door locks, drones, medical X-rays, and others, and promote the internalization of security for various information protection and information communication devices.

The government revised the software installation standards and notices for intelligent home network facilities at the end of 2021. The government supported the application of home and home appliance IoT security to apartment houses and developed test automation tools in response to the growing demand for IoT security certification.

The government also included some projects for small and medium-sized enterprises (SMEs) and local support in this plan. By expanding the cybersecurity safety net of SMEs and regions, the government plans to eliminate the security blind spots and meet new demands for information protection in the private sector. In particular, since SMEs cannot invest in security, the government provides information protection consulting, security product introduction support, solutions to ransomware, and three types of ransomware response sets. By supporting businesses that support data safety, the government also plans to support these products, solutions, and backup services for 8,300 SMEs. In addition, to strengthen local information protection, a new regional information protection council composed of local academia, industry, and local governments was established, centered on ten information protection support centers across the country to internalize security in connection with regional strategic industries and foster information security personnel.

The last strategic agenda is securing the competitiveness of next-generation cybersecurity technology. In the field of cybersecurity, the competition for global technological supremacy is intensifying. Accordingly, the Ministry of Science and ICT (pan-government) selected cybersecurity as one of the 'Top 10 Essential Strategic Technologies' in December 2021. Accordingly, the scale of information security R&D was increased by more than 24 percent to 92.8 billion won (US$90 million) this year compared to 77 billion won (US$70 million) last year (Joint Ministries, 2022).

To effectively respond to cyberattacks, the development of new technologies will promote development centered on the three major response systems: deterrence-protection-detection-response, and security technologies in preparation for the introduction of future technologies such as supply chain security technology in response to global supply chain threats, and 6G (6th Generation Mobile Connectivity)/ quantum technologies.

4.2 Future Policy and Governance of Cybersecurity for IDB Member States

Future cybersecurity will be associated with the characteristics of the Fourth Industrial Revolution. Some examples are hyper-connectivity, customized service, automation, device intelligence, and others. Cyber threats include information leakage, financial fraud, physical attack, denial of service attack, and others. Cybersecurity is needed not only for information devices but also for smart cars. For example, remote control can be used for bombing or the assassination of key figures. It can cause traffic congestion by interfering with traffic signals through DDoS attacks and can threaten national security by infringing on personal privacy and identifying trends of key people through GPS communication hacking. Furthermore, giving incorrect location information to smart cars may cause traffic congestion and risk the lives of passengers. For these reasons, future cybersecurity should be associated with people's daily lives.

Based on the policy and governance practices of cybersecurity in Korea, several recommendations can be offered to the IDB member states.

First, laws and regulations are essential for effective responses to future cyber threats. Korea has enacted many laws, such as the Resident Registration Act (1994), the Use and Protection of Credit Information Act (1995), the National Informatization Framework Act (1996), the Act on Promotion of Information and Communications (1997), the Digital Signature Act (1999), the Act on The Protection of Information and Communications Infrastructure (2009), the Electronic Government Act (2009), and the Personal Information Protection Act (2011), among others. These Acts have been revised multiple times reflect new realities in Korea.

The national e-government plan was strongly supported because of the laws, think tanks, and public institutions.

Second, it is important to have strong policies based on laws and to nurture special cybersecurity institutions that do not change from one administration to the next. Korea has several specialized cybersecurity public institutions. There have been five presidents since the start of e-government and cybersecurity national plans. However, the national e-government plan was strongly supported by all of them because of the laws, think tanks, and public institutions.

Third, concurrent cybersecurity capacity is important to ensure the effectiveness of the Living Lab approach. The Korean government built a convergence security base with five security living labs in different cities—Pangyo, Ansan, Gunsan, Busan, and Wonju—to build specialized convergence security living labs for testbeds. These cybersecurity living labs will develop cybersecurity for autonomous vehicles, digital healthcare, smart factories, and other new technology.

Fourth, incubating information security companies to expand their business areas and scale-up is critical for upgrading national capacity regarding cybersecurity. The government's strong support for nurturing the private companies of cybersecurity will scale up the nation's overall capacity while increasing employment.

Fifth, it is important to expand and advance information security certification. IoT devices are proliferating. In response to hacking, governments must expand information protection certification to various fields, such as thermal imaging cameras, door locks, drones, medical X-rays, and others, and promote the internalization of security for various information protection and information communication devices.

IDB member states vary in terms of law, governance, infrastructure, and best practices with respect to cybersecurity. Regardless of the stage they are in, it is essential to protect their societies against future potential threats by properly identifying the current situation and preparing relevant measures to solve the issues. Korea's cybersecurity policy and relevant experience may provide a model for the promotion of a sound and safe digital world in IDB member states. NHIS is ready to share thoughts and expertise in this domain with IDB member states in the nearest future.

References

Reports and Articles

Jeong H. J. et al. 2009, Informatization of Healthcare and Information Security Systems. *Information Security Scholarly Journal* 19. Information Security Academy.

Jeong, H. T. 2016. National-Level Use of Health Care Big Data and Its Policy Implications. *Health & Welfare Forum*, Korea Institute for Health and Social Affairs. 55–71.

Joint Ministries. 2021. Digital Government Innovation Strategy Planning in the Post Corona Era, Republic of Korea.

Joint Ministries. 2019. Digital Government Innovation Promotion Plan, Republic of Korea.

Jung, J. and J. Kim. 2015. Medical Information Security According to the U-Healthcare Environment Issue. *Journal of the Korean Society for Multimedia* 19(3).

Kim, J. 2021, Special Entry Control System, Ministry of Health and Welfare.

Korea Development Institute (KDI). 2008. Feasibility Study on Digitalization of Public Healthcare. KDI Report.

KISA. 2021. Direction of ICT Technology Development and Cybersecurity Policy for Future Digital Trust.

Kim, J. H., et al. 2013. Technical Trends of Cybersecurity with Big Data. *Electronics and Telecommunications Trends*. ETRI Publication.

Kim, S. Y. et al. 2013. A Study on the Security Policy Improvement Using Big Data. *Journal of The Korea Institute of Information Security & Cryptology (JKIISC)* 23(5): 969-976.

Korea Institute of Science and Technology Evaluation (KISTI). 2016. Internet of Things Development and Paradigm Change in Security. KISTI Publication No. 14.

Korea Policy Briefing https://www.korea.kr/news/policyNewsView.do?newsId=148899323

Lee D. 2021. National Infectious Disease Management in Korea. Korea Disease Control and Prevention Agency.

Lee, S. 2021. COVID-19 Contact Tracing System. Korea Agency for Infrastructure Technology Advancement.

Ministry of Interior and Safety (MoIS). 2019. Smart Government Basic Plan.

Ministry of Interior and Safety (MoIS) and NIA. The Second e-Government Main Strategy.

MOHW. 2017. Guidelines for Standard Application of Clinical Information Exchange. MOHW of Korea.

MOHW. 2021. Operational Guideline of Respiratory Disease and Fever Clinic. MOHW of Korea.

MoSICT. 2019. Guide to the Evaluation and Certification of Information Security Products.

MoSICT. 2021. National Information White Paper 2021.

NIRS. 2021. Information and Communications Service Guidelines, 2021.11.17.

Park, J.-S. et al. 2017. Emergency Use Authorization of In-Vitro Diagnostics for Infectious Disease. KDCA.

Park, S. and S. J. Kim. 2013. A Study on Cybersecurity Bills for the Legislation of Cybersecurity Act in Korea. *Convergence Security Journal* 3(6): 91-98.

Shin, I. C. 2021. Self-Quarantine Management in Korea, Ministry of Interior and Safety.

Shin, J. H. et al. 2004. Improvement of Security Vulnerability of the Internet of High-Speed National Networks. *The 21st Korea Information Processing Society Spring Conference Papers* Volume 1237.

Wang, S. H. 2018. Public Health Information Legislative Guidance for Data Governance: Legislative Issue Brief. Korea Legislation Research Institute, Vol 32.

Yi, H. K. 2021. Governance for Disaster Risk Management in Korea: Focusing on COVID-19, Mistry of Interior and Safety.

Yoo, H. 2022. Data Story. Online Publication [URL] https://dataonair.or.kr/db-tech-reference/d-story/data-story/?mod=document&uid=62870

Yoon, G. 2020. Changes and Tasks in Korea's Healthcare System in Times of the Covid-19 Pandemic: Healthcare Forum. Korea Institute for Health and Social Affairs.

Yoon, K. and K. Kun. 2014. "Information Security System Problems and Solution: Focusing on Public Sector. *Korea Public Management Journal* 31(4): 195-216.

Central Ministries and Public Institutions regarding Cybersecurity referred

Financial Security Institute (FSI) URL] www.fsi.or.kr

Financial Services Commission (FSC) [URL] https://www.fsc.go.rk

Government Integrated Data Center (GIDC) [URL] www.nirs.or.kr

Korea Internet and Security Agency (KISA) [URL] https://www.kisa.or.kr

Ministry of Interior and Safety (MoIS) [URL] https://www.mois.go.kr

Ministry of Science and ICT (MoSICT) [URL] https://www.msit.go.kr

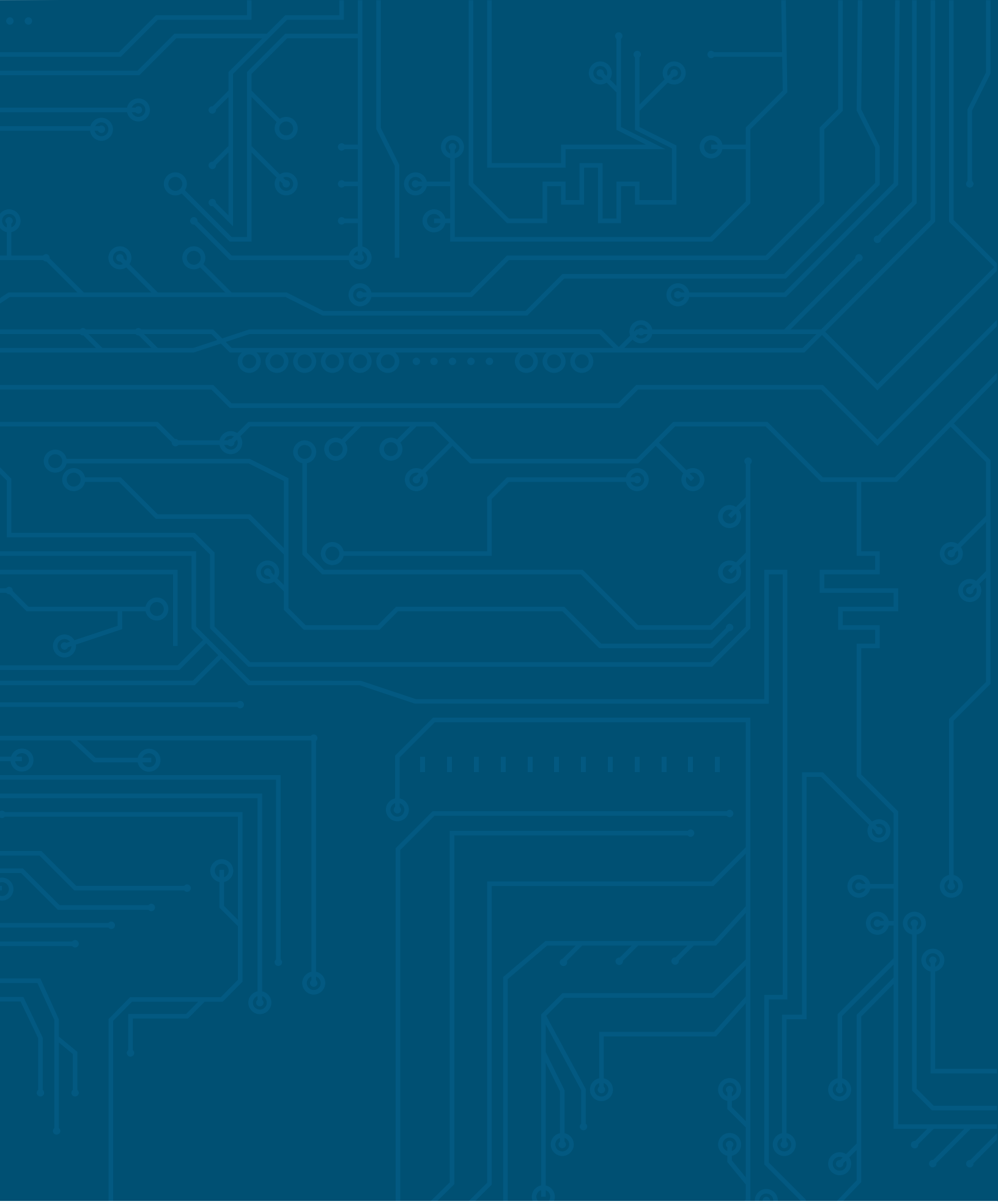
National Health Insurance Service (NHIS) [URL] www.nhis.or.kr

National Information Communication Network [URL] www.gns.kr

National Intelligence Service (NIS) [URL] https://www.nis.go.kr

National Security Research Institute (NSRI) [URL] https://www.nsri.or.kr

Korea Legislation Research Institution (KLRI) [URL] https://www.klri.re.kr/


KISA
Korea Internet & Security Agency
h·well
NHIS
National Health
Insurance Service
IDB