National Cybersecurity Basic Plan Executive Summary

□ Overview

o The Office of National Security announced the 'National Cybersecurity Basic Plan' jointly developed by 14 government ministries and organizations, including the National Intelligence Service, Ministry of Foreign Affairs, Ministry of Defense, Ministry of Science and ICT, Supreme Prosecutors' Office, and Police.

* The 'National Cybersecurity Basic Plan' is a follow-up measure to the 'Naitonal Cybersecurity Strategy' announced on February 1st, including specific implementation measures to achieve the vision and objectives of the strategy.

□ 'National Cybersecurity Basic Plan' Key Takeaways

o Composed of a total of 100 action tasks, including individual tasks (93) and joint tasks (7) from 14 ministries.

* Actively reflected expert advisory opinions from various fields, such as international strategy, law, and IT engineering during the development process

o Developed detailed plans for implementing the five strategic tasks of the previously announced 'National Cybersecurity Strategy'

* ①Strengthening Offensive Cyber Defense Activities ②Establishing a Global Cyber Cooperation Framework ③Enhancing Cyber Resilience of Critical Infrastructure ④Securing a Competitive Edge in Critical and Emerging Technologies ⑤Strengthening the Operational Foundation

① Strengthening Offensive Cyber Defense Activities

Secure deterrence by conducting preemptive and proactive cyber defense activities against cyber attacks and threat actors that undermine national security and interests, and establish a foundation for responding to 'disinformation' that divides public opinion and causes social unrest in cyberspace.

② Establishing a Global Cyber Cooperation Framework

Enhance response capabilities through cooperation and coordination with countries sharing liberal democratic values in the cybersecurity field, and contribute to building a safe and peaceful global cyberspace by actively participating in international discussions on establishing norms and building trust in cyberspace.

③ Enhancing Cyber Resilience of National Critical Infrastructure

Enhance the cyber resilience of national critical infrastructure such as major information and communication facilities and social infrastructure, as well as important information and communication systems widely used by the public, and apply policies compatible with AI and digital platform environments, such as improving the network segregation policy for national and public institutions to a 'multi-layered security' system.

④ Securing a Competitive Edge in Critical and Emerging Technologies

Foster an information security industry ecosystem based on industry-academia research collaboration, and actively cultivate core technologies that form the foundation of

national cybersecurity capabilities through expanded R&D to secure competitiveness and technological leadership in critical and emerging technologies in the international community.

⑤ Strengthening the Operational Foundation

Organically connect and harmonize the roles and responsibilities of individuals, businesses, and the government by reorganizing cybersecurity-related legal systems and organizations, and strengthen the roles and cooperation systems of each ministry overseeing protection in areas such as diplomatic security, administration, industries, economy, and education.

□ Implementation Monitoring

o The Office of National Security, as the cybersecurity control tower, and the National Intelligence Service, as the technical lead agency, plan to compile task implementation results and progresses by ministry and mange the implementation status.

ATT: Major Tasks by Ministry

ATT

Major Tasks by Ministry

Ministry (Number of Tasks)	Major Tasks
NIS(33)	o Improve technologies and legal systems related to offensive defense activities such as identifying and tracking international hacking organizations o Establish a national cybersecurity information cooperation hub o Enhance capabilities of the public-private integrated response organization (National Cyber Risk Management Unit)
MSIT(25)	o Foster an information security industry ecosystem based on industry-academia research collaboration o Support security for emerging technology industries and expand cybersecurity R&D o Raise public awareness of cybersecurity
NPS(8)	o Identify core technologies for cybercrime investigations and strengthen investigative capabilities o Enhance cooperation with domestic agencies and experts for cybercrime investigations
MOFA(6)	o Participate in international discussions on establishing norms and building trust in cyberspace o Strengthen cybersecurity solidarity with liberal democratic countries such as the US and UK
SPO(4)	o Strengthen cooperation with foreign law enforcement agencies, including joining the Cybercrime Convention
MOIS(4)	o Enhance security of National Information Resources Service o Apply security development to public sector digital services
MND(3)	o Strengthen cyber operation capabilities o Develop a Korea-Risk Management Framework
FSC(3)	o Enhance cyber threat response capabilities in the financial sector o Raise public awareness of financial security
MOE(3)	o Strengthen cybersecurity in the education sector o Enhance information security education programs and contents
MOJ(1)	o Pursue domestic tasks necessary for joining the Cybercrime Convention
MOTIE(1)	o Strengthen cybersecurity and response capabilities in industry, trade, and energy sectors
KCC(1)	o Establish policies and laws and systems to respond to disinformation
MOF(1)	o Strengthen cybersecurity in maritime and port sectors
Joint Tasks(7)	o Counter DPRK cyber propaganda and agitation (NPA-MOU) o Strengthen national encryption systems including development and distribution of post-quantum cryptogaphy (NIS-MSIT) o Develop measures for attributions, including identifying cyber threat actors (MOFA=NIS) o Secure and cultivate military cyber specialists (MND-MSIT)