# Taiwan's Policy for Addressing Frontier AI Cybersecurity Risks

## I. New Cybersecurity Challenges Posed by Frontier AI

Artificial intelligence (AI) is rapidly reshaping the speed, scale, and cost of cyber offense and defense. Frontier AI models with advanced capabilities in code analysis, vulnerability identification, and tool use enable threat actors to discover vulnerabilities, generate exploit code, and chain together complex attack steps more quickly, thereby further shortening the time between vulnerability discovery or disclosure and misuse.

Taiwan has established an integrated cyber defense system encompassing cybersecurity management, cybersecurity incident reporting and response, and cross-agency joint defense. This system provides an important foundation for addressing frontier AI cybersecurity risks. However, three challenges require priority attention as the threat landscape evolves. First, the accelerating speed from vulnerability discovery to the misuse of vulnerabilities to launch attacks requires existing mechanisms for vulnerability assessment, prioritization, remediation, and incident response to enable agencies to act on risk more quickly and efficiently. Second, government agencies and key industries rely heavily on information and communications technology (ICT) products, outsourced services, and third-party components. Once a vulnerability shared across the supply chain is exploited, its impact could spread rapidly across multiple agencies and industries. Third, frontier AI capabilities and critical cybersecurity intelligence remain concentrated among overseas providers, and access to these resources may be affected by technical constraints, commercial terms, or geopolitical developments. Taiwan must therefore deepen international cooperation while building domestic capabilities.

The government's policy is accordingly built around three priorities: accelerating cyber defense, strengthening ICT product security, and enhancing national cyber resilience. Building on existing cybersecurity governance and coordinated defense mechanisms, the government will implement short-, medium-, and long-term strategies according to the urgency of the risks, the maturity of institutional arrangements, and technological progress. These strategies will be reviewed and updated on an ongoing basis as frontier AI capabilities and the threat landscape evolve.

## II. Establishing an Interagency and Public-Private Collaboration Mechanism

To integrate expertise and resources of relevant ministries and agencies and respond promptly to emerging frontier AI cybersecurity risks, the Ministry of Digital Affairs has established the Task Force on Frontier AI Cybersecurity Risks. The Task Force brings together relevant ministries and agencies, as well as the competent authorities for critical infrastructure sectors. It continuously monitors developments in emerging AI technologies and cyber threats, develops protective strategies, and coordinates policy directions and resource allocation. The government will also deepen cooperation with critical infrastructure providers, the ICT and cybersecurity industries, and research institutions. Through public-private partnerships and collaboration among industry, government, academia, and research institutions, Taiwan will strengthen its overall cyber defense capabilities.

## III. Establish a Phased Cybersecurity Strategy

### 1. Short-Term Strategy: Accelerate Cyber Defense and Reduce Current Exposure

As AI accelerates vulnerability discovery and the launching of attacks, the government's short-term priority is to increase the speed of cyber defense. The government will prioritize refinements to existing mechanisms and the deployment of defensive tools ready for immediate use, thereby shortening the time from vulnerability discovery and impact assessment to remediation.

#### (1) Establish a Risk-Based Vulnerability Management Mechanism

Rising vulnerability volumes and remediation workloads require agencies to address the most serious risks first when time is limited. The government will therefore issue vulnerability management guidance and establish a mechanism for setting vulnerability remediation priorities and deadlines based on vulnerability risk, system criticality, and the actual level of exposure.

#### (2) Use AI to Accelerate Cyber Defense

The government will use AI models to develop vulnerability-scanning tools that support key government agencies and critical infrastructure providers in identifying cybersecurity vulnerabilities in important systems, where tested entities will subsequently evaluate vulnerability remediation deadlines at the earliest opportunity or adopt compensatory protective measures. It will also strengthen threat intelligence sharing and vulnerability reporting mechanisms.

AI-assisted threat intelligence analysis and signature matching will help accelerate impact assessment as well as shorten reporting and remediation times.

**(3) Strengthen Exposure Management**

Accelerating remediation alone is insufficient; cyber defense must also reduce potential points of entry. The government will strengthen exposure management and, according to each agency's risk profile and system environment, support agencies in strengthening their protective measures. This measures will reduce the risks of initial compromise and lateral movement.

**2. Medium-Term Strategy: Strengthen ICT Product and Supply Chain Security**

As frontier AI lowers the barriers to discovering and abusing vulnerabilities, the scope of government cybersecurity governance must extend beyond agencies' internal systems. Over the medium term, the government should extend the scope of cybersecurity governance to products and supply chains, progressively embedding secure-by-design principles in government procurement, product security, and supplier management.

**(1) Strengthen Government Procurement and Product Security**

Products available under inter-entity supply contracts consolidate items for common needs across government agencies, and a vulnerability in a single product can therefore create a shared risk across agencies. The government will apply secure-by-design principles, review both the product approval and listing mechanism and the cybersecurity management mechanism, and prioritize automated vulnerability scanning for software products. It will also require suppliers to remediate vulnerabilities within a specified period, reducing the risk of vulnerabilities spreading across agencies.

**(2) Strengthen Supply Chain Cybersecurity**

The government will continue to encourage companies to join the cybersecurity alliance operated by the Taiwan Computer Emergency Response Team/Coordination Center (TWCERT/CC), enabling them to receive timely cybersecurity alerts. To improve the security of contracted suppliers and third-party components, the government will promote the adoption of software bills of materials (SBOMs), conduct joint audits of contracted suppliers, and support suppliers in establishing product security incident response teams (PSIRTs). Together, these measures will strengthen capabilities to respond to and manage product vulnerabilities and cybersecurity incidents.

### 3. Long-Term Strategy: Deepen International Cooperation and Build Domestic AI-Enabled Cyber Defense Capabilities

Frontier AI models and vulnerability research require substantial investments in technology, computing resources, data, and talent. As AI technologies continue to advance worldwide, Taiwan must both deepen international cooperation and build domestic capabilities. International cooperation will keep Taiwan connected to the world's leading models, technologies, and threat intelligence, while domestic capabilities will enable Taiwan to sustain critical cyber defenses if external access or supply conditions change.

#### (1) Deepen International Cybersecurity Cooperation and Threat Intelligence Sharing

The government will continue to deepen cybersecurity cooperation with international partners. Drawing on the combined strengths of government, research institutions, and the private sector, it will expand channels for exchange, seek access to and use of international frontier AI models, and strengthen mechanisms for sharing threat intelligence on critical vulnerabilities and emerging threats. By maintaining close ties to the world's leading frontier AI ecosystems, Taiwan will gain timely access to threat intelligence and combine advanced cybersecurity technologies from international partners to support vulnerability scanning and analysis, thereby enabling more targeted deployment of defensive measures and strengthen national cyber defense as a whole.

#### (2) Develop Domestic AI-Enabled Cyber Defense Capabilities

Building domestic capabilities is essential to safeguarding Taiwan's core security. Through collaboration among industry, government, academia, and research institutions, the government will build a cyber defense ecosystem grounded in the concept of "sovereign AI." This effort will develop the models, data, tools, validation environments, and specialized talent needed to develop Taiwan's domestic AI capabilities for cybersecurity. Building on these foundations, the government will develop AI-enabled cyber defense technologies and systems tailored to the operational needs of Taiwan's government agencies, critical infrastructure, and key industries. In doing so, the government will strengthen cybersecurity sovereignty and ensure that its critical cyber defense capabilities maintain a high degree of autonomy, controllability, and resilience.

## IV. Conclusion: Faster Defense and Greater Resilience for the Frontier AI Era

Frontier AI capabilities and applications will continue to evolve, and their effects on cyber offense and defense may change across models, tools, and patterns of use. In the face of rapidly evolving and uncertain risks, the policy priority is to establish institutional mechanisms and capabilities that can continuously monitor risks, adapt defenses, and act swiftly.

This policy provides a framework for addressing current risks and capability needs. Through the Task Force on Frontier AI Cybersecurity Risks, the government will continue to bring together ministries and agencies, critical infrastructure providers, industry, and the research community; track technological capabilities, the threat landscape, and international policy developments; and coordinate related work and resource allocation. Implementation measures will be reviewed and updated in light of changes in risk, technological maturity, and outcomes. Together, these efforts will enable Taiwan to identify risks earlier, act more rapidly, and strengthen Taiwan's overall resilience to frontier AI cybersecurity risks.