National Institute of Cyber Security

A non-departmental public body

2023 public edition

Table of Content

1 About Us

2 Core Values

3 Principles

4 Expertise

5 Highlights

6 Location

About Us

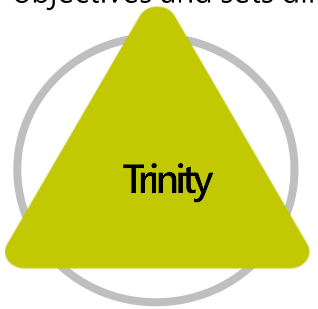
The National Institute of Cyber Security (NICS) under the Ministry of Digital Affairs (moda) was established Jan. 1, 2023, to advance the application, competence and R&D of Taiwan’ s cyber security technology.

NICS’ overarching mission is to deliver cutting-edge cyber security technical assistance and research. This augments the functions of the moda and Administration for Cyber Security(ACS). The moda drafts national cyber security policy objectives and sets direction, while ACS implements and promotes cyber security policies.

Strengthening Cyber Security Measures Together

moda

Drafts national cyber security policy objectives and sets direction



ACS

Formulates, implements and promotes national cyber security policy

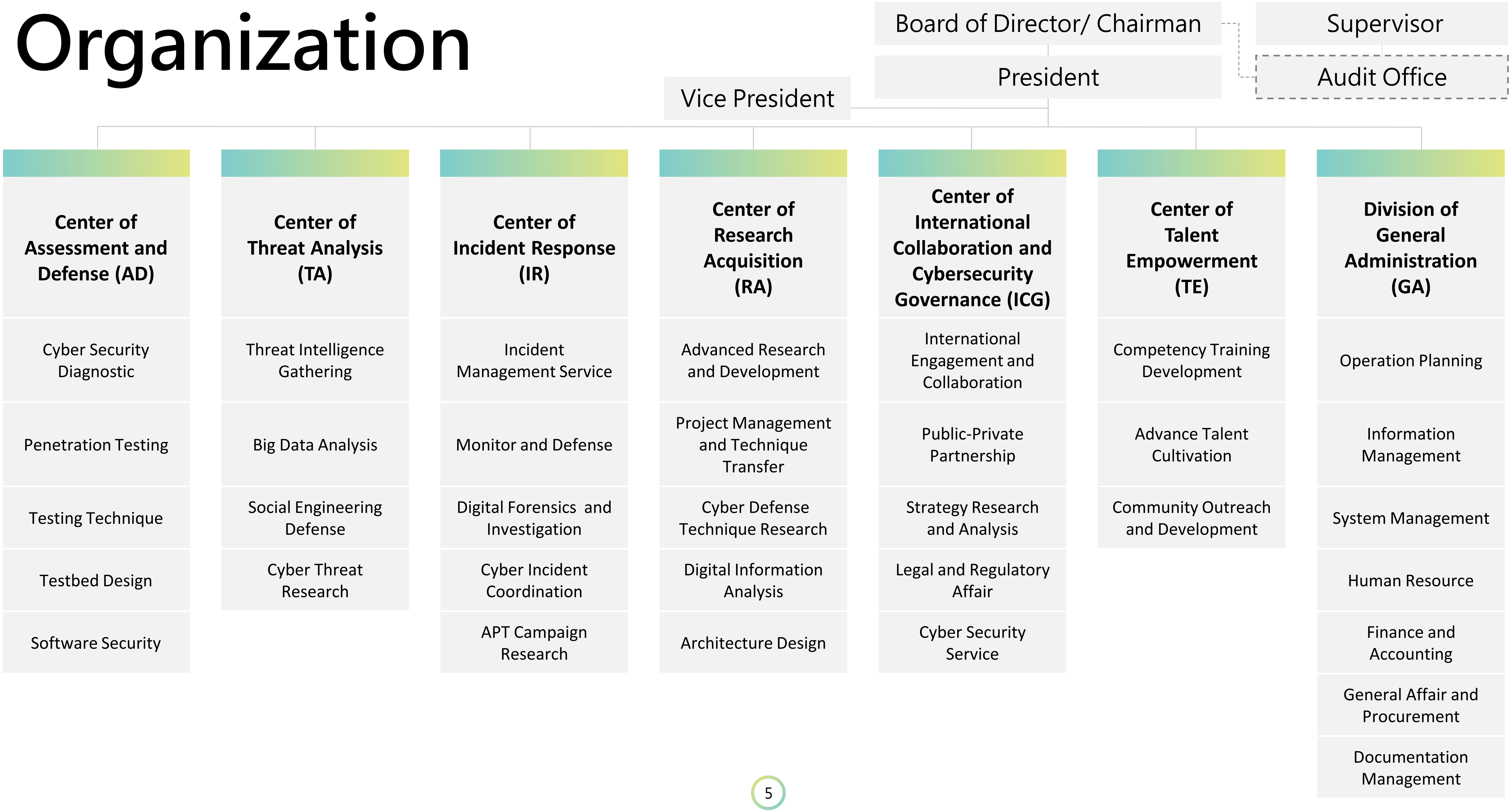
NICS

Advises on cyber security technology, R&D and cyber security expertise, supports cyber security administrative work and provides a talent empowerment program

Scope of Operation

1. Researching and developing cyber security technology, as well as promoting the application, technology transfer, industry-university collaboration services, international cooperation and exchanges of cyber security technology;
2. Assisting in planning and promoting national cyber security protection mechanisms;
3. Assisting government agencies and institutions by strengthening critical infrastructure in responding to major cyber security incidents;
4. Assisting in planning and supporting cyber security protection of nation’s critical infrastructure;
5. Assisting in cyber security talent planning and development while promoting cyber security awareness nationwide;
6. Supporting government agencies and institutions in cyber security protection operations with special sensitivity;
7. Supporting demands for the industry’s major development in cyber security and its regulatory initiatives; and
8. Other matters related to cyber security technology.

Organization



Board of Director/ Chairman

Supervisor

President

Audit Office

Vice President

Center of Assessment and Defense (AD)	Center of Threat Analysis (TA)	Center of Incident Response (IR)	Center of Research Acquisition (RA)	Center of International Collaboration and Cybersecurity Governance (ICG)	Center of Talent Empowerment (TE)	Division of General Administration (GA)
Cyber Security Diagnostic	Threat Intelligence Gathering	Incident Management Service	Advanced Research and Development	International Engagement and Collaboration	Competency Training Development	Operation Planning
Penetration Testing	Big Data Analysis	Monitor and Defense	Project Management and Technique Transfer	Public-Private Partnership	Advance Talent Cultivation	Information Management
Testing Technique	Social Engineering Defense	Digital Forensics and Investigation	Cyber Defense Technique Research	Strategy Research and Analysis	Community Outreach and Development	System Management
Testbed Design	Cyber Threat Research	Cyber Incident Coordination	Digital Information Analysis	Legal and Regulatory Affair		Human Resource
Software Security		APT Campaign Research	Architecture Design	Cyber Security Service		Finance and Accounting
						General Affair and Procurement
						Documentation Management

Core Values

Build a World-class Scientific Research Team in Cyber Security Resilience and **a Secure, Assured and Stable** Digital Environment

S	T	A	R	T
Security	Technology	proActiveness	Resilience	Trust
Construct Cyber Security Joint Defense	Develop and Research Advanced Cyber Security Technologies	Observe Cyber Security Status of Countries and Global Trends	Promote Public-Private Partnerships	Cultivate Cyber Security Talent
Strengthen Cyber Security Early Warning Capabilities	Spur Independent Research and Innovation	Deepen International Engagement and Collaboration	Elevate the Resilience of Critical Infrastructure	Promote Public Cyber Security Awareness

GOAL

1. **Strengthen the National Cyber Security Defense Mechanism; Enhance Cyber Security Resilience of a Smart Nation**
2. **Establish a National Cyber Security Team; Ensure Homeland Security in Cyberspace**
3. **Bolster Cyber Security Technology R&D; Promote Industrial Cyber Security Development**

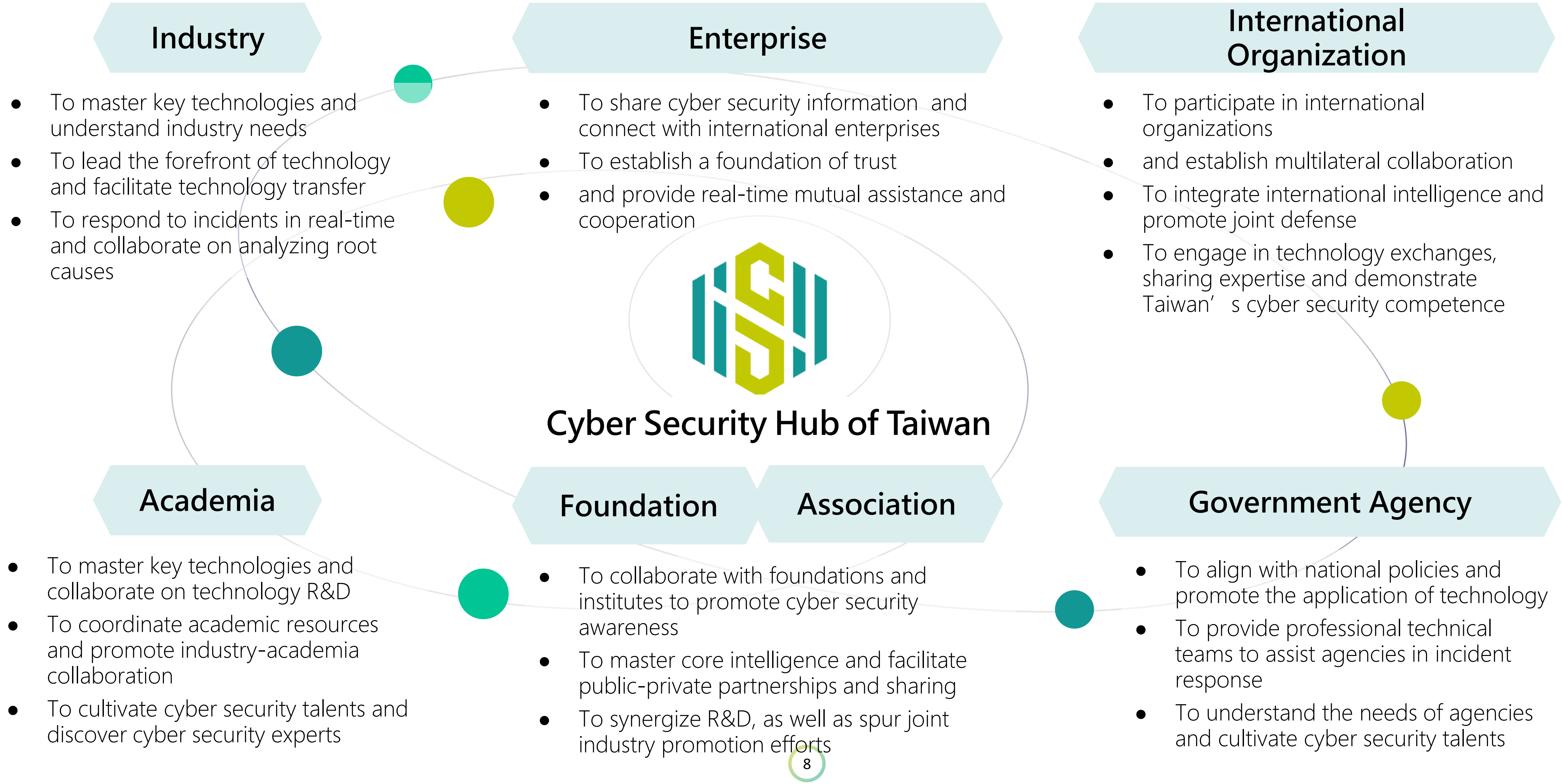
NICS Roles and Competency：
to Assist the Government in Enhancing Cyber Security Resilience and Personal Data Protection

- Cyber Security Information Gathering & Application
- Industrial Cyber Security Development Support
- Industry-Academia Service & Technical Consulting
- National Cyber Security Defense Mechanism Planning
- Cyber Security Incident Report & Response
- International Collaboration & Joint Defense in Cyber Security

Advanced Cyber Security Technology Research & Development

Cyber Security Talent Training & Assessment

Domestic and International Collaborative Platform for Public-Private Partnerships in Cyber Security



Industry

- To master key technologies and understand industry needs
- To lead the forefront of technology and facilitate technology transfer
- To respond to incidents in real-time and collaborate on analyzing root causes

Enterprise

- To share cyber security information and connect with international enterprises
- To establish a foundation of trust
- and provide real-time mutual assistance and cooperation

International Organization

- To participate in international organizations
- and establish multilateral collaboration
- To integrate international intelligence and promote joint defense
- To engage in technology exchanges, sharing expertise and demonstrate Taiwan’ s cyber security competence

Cyber Security Hub of Taiwan

Academia

- To master key technologies and collaborate on technology R&D
- To coordinate academic resources and promote industry-academia collaboration
- To cultivate cyber security talents and discover cyber security experts

Foundation

Association

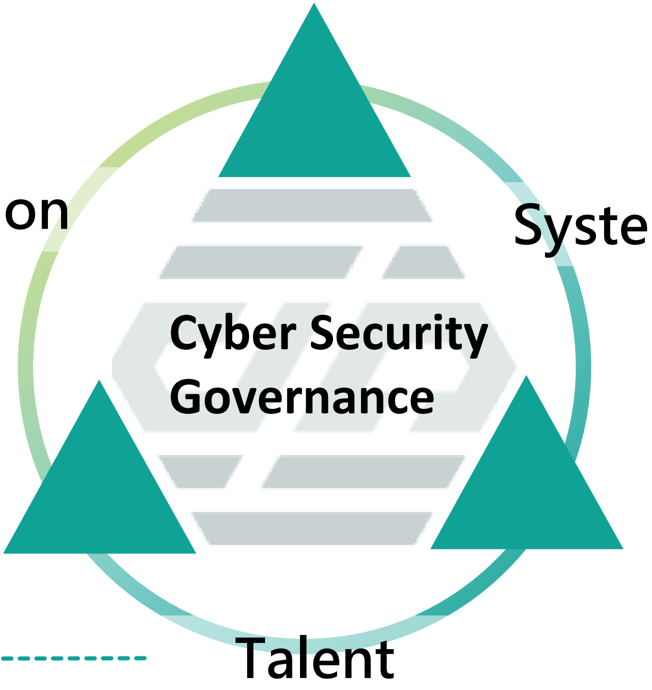
- To collaborate with foundations and institutes to promote cyber security awareness
- To master core intelligence and facilitate public-private partnerships and sharing
- To synergize R&D, as well as spur joint industry promotion efforts

Government Agency

- To align with national policies and promote the application of technology
- To provide professional technical teams to assist agencies in incident response
- To understand the needs of agencies and cultivate cyber security talents

Principles

NICS adopts the three key dimensions of information, system and talent as its fundamental principles for the development of cyber security governance. NICS aims to assist in enhancing the overall national cyber security governance of Taiwan through the collective practices of all units within the institute.



To enhance the value of information and increase intelligence application

To strengthen the resilience of information and communication systems with technology as the foundation

To cultivate cyber security talents through public-private partnerships

Expertise

Center of Assessment and Defense

Support agencies in proactive prevention and enhance system security protection
Foster cyber security offensive and defensive skills, as well as cultivate professionals in cross-border practical operations

Center of Incident Response

Protect, warn and monitor key agencies, as well as provide 24/7 reporting and response
Track footprints, conduct professional forensics and root cause analysis of incidents

Center of Threat Analysis

Gather and analyze threat intelligence, as well as provide early warnings to reduce damage
Promote the enhancement of automated deployment to counter threats in real-time

Center of Research Acquisition

Integrate R&D capablilty from various fields and promote advanced technology research
Strengthen the implementation of technology applications and enhance the resilience of agencies

Center of International Collaboration and Cybersecurity Governance

Actively share cyber security information and deepen international engagement and collaboration
Conduct research and analysis on significant policies, as well as provide advice for protective technologies

Center of Talent Empowerment

Enhance cyber security awareness among the public and drive the adoption of practical protective measures
Align with international development trends and cultivate cross-sector cyber security talents

Current Highlights

Center of Assessment and Defense(AD)

Develop trustworthy AI mechanisms for assessment

Center of Research Acquisition(RA)

Promote zero-trust mechanisms and digital message protection

Center of Threat Analysis(TA)

Develop automated blacklist deployment mechanism and comprehensive analysis of threat intelligence

Center of Incident Response(IR)

Investigate and assist handling personal data incidents

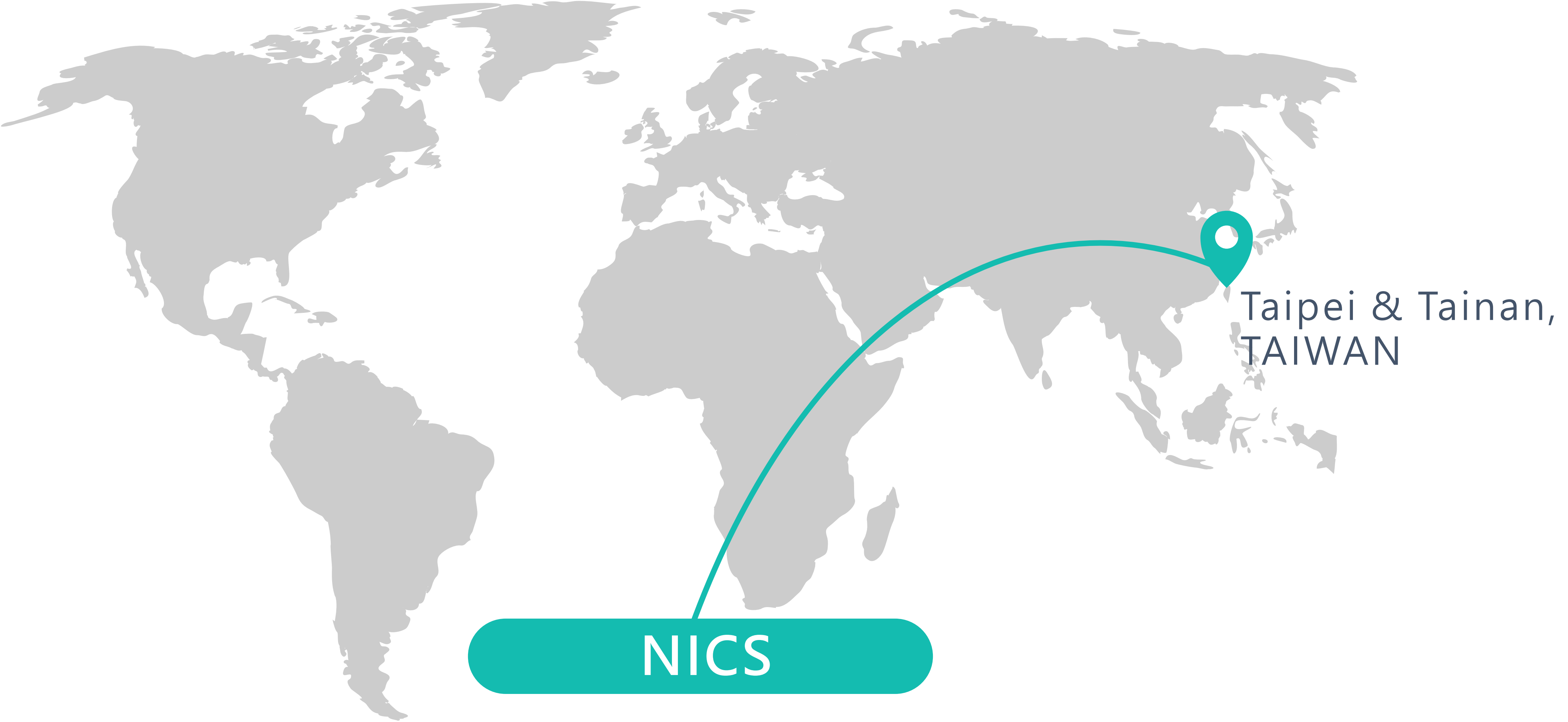
Center of International Collaboration and Cybersecurity Governance (ICG)

Strengthen international cooperation in cyber security joint defense, enhance critical infrastructure protection

Center of Talent Empowerment(TE)

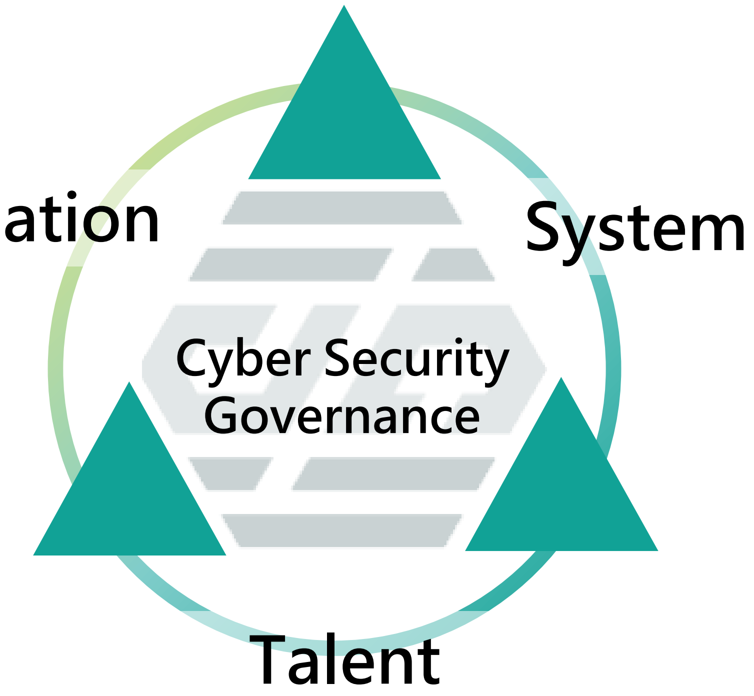
Develop competency standards for Chief Information Security Officer (CISO) and Cyber Security Incident Engineer roles

Location



Mid-Term Development Directions

Continuously improve cyber security information gathering, integration and analysis, as well as proactive defense mechanisms



Research and develop digital message protection technologies, facilitate the application of key technology transfers

Integrate the CERT/CC reporting mechanism, continuously improve the efficiency of incident reporting and response

Enhance cyber security literacy among the public through public-private partnerships, improve cyber security talent development in the public and private sector