Overview of the Information and Communication Security Technology Center (ICST)

The Center's Mission

In order to establish a reliable information and communications security infrastructure in Taiwan, the Executive Yuan officially approved the first phase of the *National Information and Communication Infrastructure Security Mechanism Plan* during its No.2,718 meeting session on January 17, 2001 and formed the National Information and Communication Security Taskforce (NICST) to carry out the Plan from 2001 to 2004. Shortly thereafter, the Information and Communication Security Technology Center (ICST) was established in March of 2001.

From 2005 to 2012, the Executive Yuan actively promoted the implementation of the second phase (2005–2008) of the *National Information and Communication Infrastructure Security Mechanism Plan* and the *National Strategy for Cybersecurity Development Program* (2009–2012). The Executive Yuan, assisted by various ministries, commissions, administrations, and local city and county governments, rapidly achieved the milestone of establishing a comprehensive information security system and national information security capability.

In consideration of a deteriorating information security situation, the Executive Yuan amended the Guidelines for Establishing the National Information and Communication Security Taskforce in March of 2011 and set up the Office of Information and Communication Security (OICS) in order to enhance national information security policy planning, improve efficiency of information security notification and contingency planning, and expedite implementation of major information security programs. In coordination with Executive Yuan restructuring on January 1, 2012, the OICS became a permanent taskforce of the Executive Yuan. Pursuant to the Guidelines for Establishing the Office of Information and Communication Security, in addition to performing information and communication security operations and supervising the ICST, the OICS is responsible for the following primary duties:

1. Development and promotion of national information security policy and measures.
2. Notification, response, and review of national information security incidents.
3. Promotion and review of major national information security programs.
4. Coordination, liaison and promotion of national information security-related legislation and regulations.

According to the revised Guidelines for Establishing the National Information and Communication Security Taskforce promulgated in January of 2013, the NICST is charged with coordinating, liaising, and promoting information security-related matters. Two systems have been established under the Taskforce: Internet Protection and Cybercrime Investigation and Prevention. These operations are overseen by the OICS, the Ministry of Justice, and the Ministry of the Interior.

Internet protection system comprises Standard and Norm Working Group, Awareness and Training Working Group, Audit Working Group, and Government Information and Communication Security Working Group were created. The Government Information and Communication Security Working Group, led by the OICS, is responsible for formulating and promoting the security mechanism used to protect various information and communication services provided by the government to the public, offer guidance to government agencies concerning information and communication security technical services, provide information and communication security protection and respond to security incidents, and ensure that sufficient numbers of information and communication security personnel are trained and accessible by government institutions.

The ICST is required to assist the OICS in carrying out the duties of the Government Information and Communication Security Working Group and provide government agencies with technical services such as preventive security protection, real-time warning and response strategies during incidents, and follow-up recovery plans. In addition, the ICST must comply with the various sub-project requirements listed in the *National Strategy for Cybersecurity Development Program* (2013–

2016), which includes promoting information security configurations in information security infrastructures, enhancing second-line monitoring services and intelligence gathering for information security protection management, strengthening information security contingency functions and recovery capabilities, and establishing the mechanism of Security Project Management Office (SPMO) . These sub-project requirements required the ICST to establish SPMO and high-quality information security environment, implement and promote information security services, control information security and improve personnel competency, and research and develop autonomous technology. The ICST must also provide information security technology, consulting services, and engage in international exchanges in order to achieve the following four strategic objectives: (1) Enhancing national information security policies and establishing a secure information environment; (2) Improving information security protection management and sharing diverse intelligence on information security; (3) Building a firm foundation for information security technology capabilities and integrating practical technological applications; and (4) Expanding information security talent cultivation and increasing international information security exchanges. The ICST's primary job duties consist of the following:

1. To provide information security technology, consulting services, and management services, improve the government's information security project management framework, and improve the information security defense capability of government agencies.
2. To raise information security management awareness and promote the application of sophisticated information security specifications to build a high-quality information security environment.
3. The Government Security Operation Center is a second-tier surveillance unit that collects and analyzes government security incidents. The Government Security Operation Center also engages in broad-scale intelligence gathering for the sake of national security and to improve the information security, incident management measures, and incident reporting and response capacities of government agencies.
4. To upgrade government information reporting and response procedures, improve the information security information-sharing mechanism, and enrich the content shared by the Government-Information Sharing and Analysis Center (G-ISAC).
5. To perform information security audit checks, plan government configuration baseline educational training, and enhance the government’s cyber and information system security protection capacity.
6. To provide information security training to government employees and formulate evaluation programs, train information security personnel, and arrange information security activities to raise information security awareness nationwide.

ICST Timeline

Date	**Milestones**
2001.1	Established the Information & Communication Security Technology Center (ICST).
2002.12	BS 7799 certified.
2003.10	Held the first information security drill.
2004.12	Created a 24*7 Government NSOC Information Security Protection Platform.
2005.6	Ported over and re-integrated the government information security incident notification and response website.
2005.6	First to discover “Zero-day” malware and notify vendors to carry out immediate rectification.
2005.10	Held the first social engineering drill.
2006.7	CNS 17800/ISO 27001 Certified.
2006.9	Established the Information Incident Analysis Lab and the Cyber Incident Simulation Lab.
2006.12	Hosted the first Collegiate Information Security Competition.
2008.6	Awarded First Place in the “FIRST Global Information Security Best Practices Competition”.
2008.10	Director Pei-wen Liu was Inducted by the $(ISC)^2$ as an Honoree for the "Senior Information Security Professional" Category at the Second Annual Information Security Leadership Achievements Program (ISLA).
2009.6	ISO 20000 and ISO 27001 Certified.
2009.9	Established the Cyber Security Simulation Lab.

2010.3	Officially launched G-ISAC.
2010.4	Officially launched the Information Security Surveillance and Management System (developed in-house).
2011.10	The Information Security Simulation Lab developed a fuzz testing capability which lead to the identification of a total of 34 Common Vulnerability Enumerations (CVEs) in software used globally.
2012.7	Deputy Director Jia-chyi Wu was Inducted by the $(ISC)^2$ as an Honoree for the "Senior Information Security Professional" Category at the Sixth Annual Information Security Leadership Achievements Program (ISLA).
2012.11	BS 10012, ISO 20000 and ISO 27001 certified by adopting a 3-in-1 management system.
2013.1	Officially included information security service in a common supply contract while acting as the Information Security Project Management Office (SPMO) for the government.
2013.11	Held the first nation-wide large-scale cyber security drill to test the prevention and response capabilities of the Executive Yuan's 33 affiliated second-tier agencies.

Technical Service Hotline: +886-2-27339922
Fax Hotline: +886-2-27331655
Site Issues Services: +886-2-66311626
Email：cas@icst.org.tw