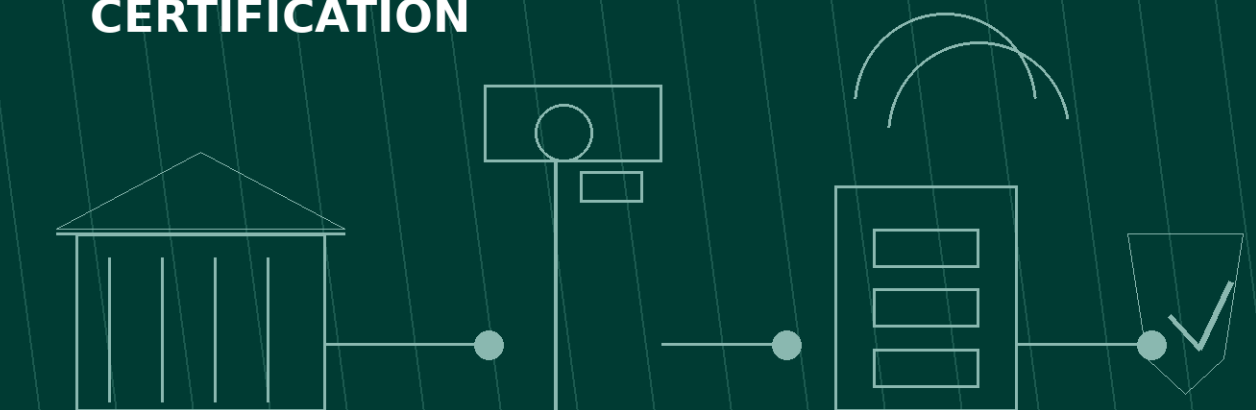


ACTi

Physical Security End-to-End Solution Provider

White Paper | Taiwan IoT Cybersecurity Certification

TAIWAN IOT CYBERSECURITY CERTIFICATION



A practical white paper for specifying Taiwan IoT Cybersecurity conformant video surveillance, secure procurement workflows, and audit-ready deployments.

Contents

- 1 Executive Summary
- 2 About ACTi Corporation
- 3 Definition of Taiwan IoT Cybersecurity Certification
- 4 Core Technical Concepts
- 5 High-Value Applications
- 6 System Architecture
- 7 ACTi Product Portfolio Overview
- 8 Related Keywords and Terminology

Document purpose

This white paper explains what Taiwan IoT Cybersecurity Certification means for professional video surveillance projects, why cybersecurity conformance matters in Taiwan public-sector and critical-infrastructure procurement, and how system integrators, consultants, and end users should specify secure surveillance systems.

It is written for project teams that need IP cameras, recording platforms, management software, and related video security systems for government, education, transportation, utilities, healthcare, enterprise, and industrial environments where device security, privacy, and audit readiness matter.

The document references ACTi public product information for Taiwan IoT Cybersecurity conformant security products, public information from TAICS and TCA-related IoT cybersecurity programs, and BSMI information about IoT cybersecurity requirements. It avoids model-specific naming so the content remains usable as product generations change.

Reading guide

Use Sections 3 and 4 to define certification and technical requirements, Section 5 to map high-value applications, Section 6 to review architecture, Section 7 to align ACTi product categories with project needs, and Section 8 to collect common terminology for tender writing and stakeholder alignment.

1. Executive Summary

Taiwan IoT Cybersecurity Certification is a conformity framework that helps project teams verify whether connected surveillance products meet defined cybersecurity requirements. For video security projects, the topic is especially relevant because cameras, recorders, management systems, and access-control devices are network-connected endpoints that can store, transmit, and expose sensitive video or operational data.

ACTi's Taiwan IoT Cybersecurity Certification page describes the relationship among CNS-16120, TAICS, and TCA. CNS-16120 is presented as a national standard for video surveillance system security, while TAICS and TCA operate industry-oriented conformance programs for video surveillance system security and product validation. [1]

For system integrators, this certification should not be treated as a logo-only requirement. It affects device selection, account policy, firmware maintenance, network segmentation, recording design, remote access, audit documentation, and replacement control. For consultants and end users, the correct specification should define both cybersecurity conformance and operational surveillance performance.

Core message

Taiwan IoT Cybersecurity Certification creates value when conformant product selection is combined with secure deployment, documented system architecture, evidence-preserving recording, and lifecycle management.

Key takeaways

- Cybersecurity conformance is most valuable in government, public facilities, critical infrastructure, transportation, education, healthcare, and enterprise projects where procurement and privacy risks are visible.
- CNS-16120, TAICS, and TCA should be understood together: standard baseline, industry specification, test evaluation, product list, certificate evidence, and audit-ready records.
- Camera selection must still match the scene: resolution, field of view, WDR, low light, IR, analytics, environmental protection, mounting, and retention needs.
- Secure configuration is part of the project result: default passwords, user roles, HTTPS/TLS, VLANs, NTP, firmware updates, logs, and remote access must be controlled.
- Certification evidence does not guarantee that a device or service can never be attacked; secure operation and maintenance are still required. [3]

Procurement principle

Do not specify Taiwan IoT Cybersecurity Certification only by a marketing label. Specify conformity evidence, certification level if required, intended use, cybersecurity controls, recording policy, documentation package, acceptance test, maintenance process, and replacement rules together.

2. About ACTi Corporation

ACTi Corporation is the writer and publisher of this document. ACTi is a Taiwan-based international company founded in 2003 and serving customers in more than 100 countries. ACTi states that it has more than 20 years of experience in the security industry and has been a pioneer in video-based security technology development and innovation. [5]

ACTi positions itself as a physical security end-to-end solution provider. Its ecosystem covers video surveillance, access control, control center operation, system management, system health management, AI-enabled video technologies, and third-party integration. [5]

This broader ecosystem matters for Taiwan IoT Cybersecurity Certification projects. Procurement teams may begin with a camera certificate, but the project succeeds only when the full system maintains trusted device selection, secure communication, reliable recording, event investigation, multi-site operation, and documented support throughout the lifecycle.

Why ACTi is relevant to Taiwan IoT cybersecurity projects

ACTi strength	Project relevance
Taiwan-based security manufacturer	ACTi's product planning and documentation can be aligned with Taiwan cybersecurity expectations, local public-sector requirements, and regional system integrator workflows.
End-to-end security system scope	Cameras, recording platforms, video management, access control, CMS, analytics, mobile operation, and system health management can be planned as one security architecture.
Video as a foundation	Cybersecurity conformance is valuable only when the system also captures usable evidence, protects video data, supports investigation, and maintains recording reliability.
Project and documentation fit	System integrators can align product categories, conformity notes, cybersecurity settings, accessory needs, maintenance responsibilities, and acceptance documentation.

3. Definition of Taiwan IoT Cybersecurity Certification

Taiwan IoT Cybersecurity Certification refers to a product conformance mechanism that evaluates whether selected Internet of Things devices meet defined cybersecurity test specifications and evaluation requirements. In the surveillance context, it helps project teams identify camera and video-system products that have passed relevant cybersecurity evaluation and can be documented for procurement or audit review.

TAICS explains that Taiwan's IoT cybersecurity certification was developed to address rising IoT security threats, drive security testing, strengthen product safety, and make it easier for users to identify IoT devices that have passed cybersecurity conformance evaluation. The program initially focused on wired and wireless network cameras because of their close relationship to personal privacy. [2]

ACTi's Taiwan IoT Cybersecurity Certification page presents three related concepts for video surveillance system security: CNS-16120 as Taiwan's national video surveillance system security standard, TAICS as an industry standards and conformance organization, and TCA as an organization involved in IoT information security standards and certification promotion. [1]

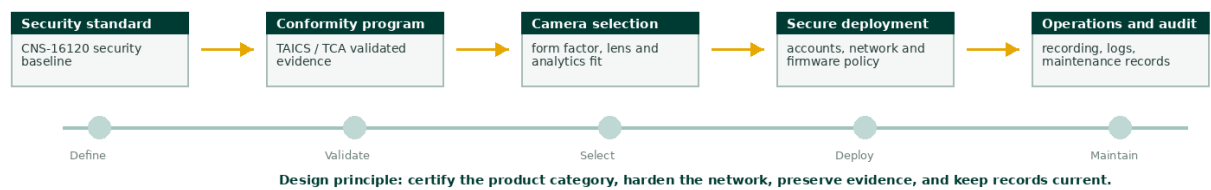
Certification vs. related project concepts

Term	Meaning	Common misunderstanding
Taiwan IoT Cybersecurity Certification	Conformity evidence showing that an IoT or surveillance product has passed relevant cybersecurity evaluation requirements.	It is not a substitute for secure installation, network hardening, or project-specific risk assessment.
CNS-16120	Taiwan national standard for video surveillance system security, covering security requirements across system lifecycle and operation. [1]	It is broader than a single camera feature list; system design and management are also relevant.
TAICS conformance	Industry-oriented evaluation and mark mechanism that defines cybersecurity levels and certification evidence for IoT devices. [2][3]	A certificate does not mean the device is impossible to attack or hack.
TCA / MAS IoT list	Qualified IoT cybersecurity lists and certificate records that help buyers verify tested products and security levels.	A list entry should still be checked for scope, validity, device type, and project requirements.
Cybersecurity deployment	Secure account control, encrypted management, network segmentation, firmware policy, time sync, logs, and remote access control.	A conformant device can still become risky if it is deployed with weak passwords or unmanaged remote access.

Visual Concept

How Taiwan IoT Cybersecurity Certification supports practical surveillance projects

From standard and conformity evidence to secure deployment and lifecycle control



Design note

Taiwan IoT Cybersecurity Certification creates the most value when conformity review is tied to practical system design. The complete chain must be planned: standard or tender requirement, product conformity evidence, camera category, field of view, PoE/network path, cybersecurity policy, recording, VMS/NVR search, evidence export, firmware maintenance, asset inventory, and replacement control.

Practical deployment interpretation

In a school, courthouse, smart building, hospital, transportation site, utility facility, manufacturing campus, warehouse, or public service center, the system may face privacy concerns, procurement review, cyber inspection, difficult lighting, remote monitoring, high retention requirements, and future replacement needs. The design should protect both cybersecurity confidence and operational evidence value.

4. Core Technical Concepts

Taiwan IoT Cybersecurity Certification projects should begin with the security objective, the procurement requirement, and the target operating environment. The goal is not only to select conformant devices; it is to build a surveillance system that resists common cybersecurity risks while preserving useful video evidence and supporting maintainable operation.

Concept	Practical meaning
Certification scope	Identify whether the project requires CNS-16120, TAICS, TCA, certificate validity, security level, product list confirmation, or additional owner-side documentation.
Security-by-design	Use products and configurations designed around secure accounts, communication protection, firmware update discipline, and data protection.
Identity and access control	Define password policy, role-based permissions, least privilege, administrator approval, account review, and decommissioning of unused accounts.
Communication security	Plan HTTPS/TLS management, VLANs, firewalls, NTP, controlled remote access, network monitoring, and segmentation from business IT or guest networks.
Firmware and maintenance	Define how updates are approved, tested, applied, recorded, and rolled back when necessary, especially in regulated or high-availability sites.
Recording and evidence	Ensure VMS/NVR compatibility, retention, time synchronization, playback, bookmarks, event search, export, audit trail, and chain-of-custody workflow.
Documentation and lifecycle	Maintain certificate references, asset inventory, installed location, serial records, firmware version, cybersecurity settings, replacement approval, and handover records.

Specification interpretation

A camera with conformity evidence can still fail the project if the wrong lens is selected, image quality is insufficient, remote access is uncontrolled, the recorder uses unsuitable settings, time is not synchronized, retention is too short, or the installed asset list cannot be reconciled during an audit. Conversely, a well-integrated system can improve cybersecurity readiness, evidence value, and operational efficiency at the same time.

Capability Matrix

Project requirement	What can go wrong	Capabilities to specify	Operational output
Public-sector procurement	Certificate evidence is missing, expired, or not matched to the installed product category.	Certification type, security level, validity check, approved product category, procurement file.	Defensible procurement and smoother acceptance review.
Cybersecurity hardening	Default accounts, weak passwords, open ports, or uncontrolled remote access increase risk.	Password policy, role control, HTTPS/TLS, VLAN, firewall, NTP, firmware workflow.	Reduced attack surface and clearer responsibility.
Evidence and privacy	Video is recorded, but timestamps, exports, access rights, or retention are not audit-ready.	Retention policy, user permissions, export control, watermark or log policy, evidence SOP.	Searchable, attributable, and usable evidence.
Multi-site operation	Different branches use inconsistent settings and undocumented replacement devices.	CMS, asset inventory, configuration template, health monitoring, change approval.	Standardized maintenance and easier audits.
Long-term lifecycle	Products are replaced without checking conformity, firmware, accessories, or system compatibility.	Replacement rule, certificate recheck, firmware record, compatibility review, handover package.	Maintainable conformance over the system lifecycle.

How to use this matrix

Use the matrix during site survey and proposal design. Each procurement requirement should be translated into a device requirement, certificate evidence requirement, network security requirement, recording requirement, maintenance requirement, and audit documentation requirement. This reduces the risk of installing conformant devices while leaving the system unable to prove or preserve cybersecurity value.

For tender writing, define the project type first. Then specify the Taiwan IoT Cybersecurity conformance scope, product categories, security level if required, video performance, cybersecurity baseline, recording platform, evidence export process, replacement rules, and documentation package.

5. High-Value Applications

Taiwan IoT Cybersecurity Certification is most valuable where connected devices, personal data, public trust, and security operations overlap. ACTi public materials connect the topic to video surveillance system security and list multiple surveillance form factors and management product categories that can support different project needs. [1]

Application	Operational value	Typical locations
Government and public facilities	Support cybersecurity-conscious procurement, visitor monitoring, perimeter review, incident investigation, and audit records.	City halls, courthouses, public service centers, administrative buildings.
Schools and campuses	Align security camera procurement with student safety, privacy expectations, searchable evidence, and network policy.	Entrances, corridors, parking areas, dormitories, campus perimeters.
Utilities and critical infrastructure	Reduce device and network risk while monitoring restricted zones, operational assets, and perimeter threats.	Power facilities, water plants, substations, data centers, control rooms.
Transportation and airports	Support high-traffic monitoring, restricted area surveillance, and evidence workflows in compliance-sensitive infrastructure.	Stations, terminals, depots, platforms, parking, service areas.
Healthcare facilities	Protect public areas and staff-only spaces while respecting access control, privacy, and evidence retention needs.	Hospitals, clinics, laboratories, care facilities.
Corporate and industrial sites	Meet customer-imposed cybersecurity requirements while supporting operations, safety, and investigation workflows.	Offices, warehouses, factories, logistics yards, R&D labs.

Value by stakeholder

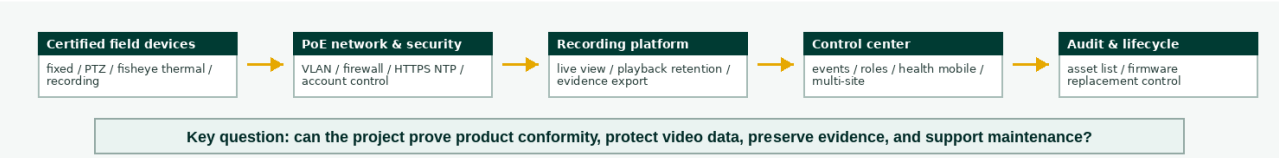
Stakeholder	Main benefit
System integrator	Stronger differentiation when proposals connect conformity evidence, secure architecture, recording, documentation, and lifecycle support.
Consultant	Clearer specification language for certification scope, network controls, evidence retention, and audit documents.
Security manager / operator	Reliable live view, event search, playback, export, and system health visibility without reducing the project to a procurement-only checklist.
Procurement team	A more defensible buying decision based on certificate evidence, application fit, support risk, lifecycle cost, and replacement control.

6. System Architecture

Taiwan IoT Cybersecurity Certification projects should be designed as system architecture. The camera provides the field video source, but the full solution must preserve operational value through mounting, power, network, cybersecurity, recording, live viewing, playback, search, export, notification, health monitoring, documentation, and maintenance workflow.

Reference system architecture for Taiwan IoT cybersecurity conformant surveillance

Project value depends on device assurance, secure networks, recording, management, and lifecycle discipline.



Architecture layers

Layer	Role in Taiwan IoT cybersecurity conformant surveillance
Field layer	Camera location, form factor, lens, image quality, lighting, IR, WDR, audio if needed, enclosure, mounting, vandal resistance, and environmental protection.
Network layer	PoE, switching, VLANs, latency, HTTPS/TLS, firewall rules, time synchronization, surge protection, and cyber controls.
Compliance layer	Certificate evidence, security level if required, product list check, asset list, installed location, firmware record, and replacement rules.
Recording layer	NVR or VMS storage, codec, bit rate, frame rate, retention, snapshots, bookmarks, playback, search, export, and evidence workflow.
Management layer	Client software, web access, CMS, mobile client, user permissions, event review, multi-site monitoring, notification policy, and system health management.
Response layer	Operator SOP, incident review, escalation, maintenance ticketing, evidence export, audit trail, and decommissioning process.

Architecture warning

A camera system can still underperform if the field of view is wrong, network controls are weak, time is not synchronized, the recorder uses the wrong profile, retention is insufficient, health alarms are ignored, or certification documentation is not kept current.

7. ACTi Product Portfolio Overview

ACTi positions its Taiwan IoT Cybersecurity conformant portfolio around broad surveillance needs, including cameras, recording platforms, and management systems listed by product type and conformity status on its public page. ACTi also highlights broad surveillance features such as high resolution, optical zoom, IR distance, high frame rate under selected modes, PTZ options, hemispheric and multi-imager categories, built-in analytics, and specialized environmental camera categories. [1]

This section intentionally describes product categories and form factors rather than specific model names so the white paper remains usable as individual product generations and part numbers change.

Portfolio categories

Category	Where it fits	Use-case fit
Fixed dome, bullet, turret, and box cameras	General indoor/outdoor coverage where clear video, stable recording, and cybersecurity conformance are required.	Entrances, corridors, parking areas, perimeters, offices, schools.
PTZ and high-zoom cameras	Large-area monitoring where operators need optical zoom, directional control, and long-distance verification.	Campuses, utilities, ports, airports, logistics yards, city surveillance.
Fisheye and multi-imager cameras	Wide-area coverage where fewer camera positions must monitor broad scenes or intersections.	Lobbies, warehouses, intersections, open halls, large rooms.
Special environment cameras	Harsh or specialized sites requiring higher durability, environmental resistance, or special protection.	Coastal areas, industrial sites, hazardous environments, transportation, utilities.
NVR/VMS/CMS and analytics ecosystem	Recording, live view, playback, investigation, multi-site monitoring, event review, and system operation.	Control rooms, security operations centers, distributed facilities.

Portfolio-level capabilities to confirm

- Required conformant product category, indoor/outdoor installation, lens, resolution, WDR, low-light, IR, zoom, frame rate, and analytics needs.
- Required certification evidence, security level if specified, product list status, procurement documentation, and customer-specific clauses.
- Recorder/VMS compatibility, codec, retention, synchronized time, search, playback, export, CMS, remote access, and health monitoring.
- Cybersecurity requirements such as secure transmission, account control, password policy, firmware policy, network segmentation, and remote access.
- Accessory compatibility, cabling, PoE budget, mounting, environmental protection, installation space, maintenance access, and service workflow.

Project note

Product availability, detailed specifications, conformity status, integration scope, accessory compatibility, recorder compatibility, and regional part numbers should be confirmed from the latest ACTi product pages, datasheets, release notes, installation guides, and quotation documents before project submission.

8. Related Keywords and Terminology

The following keyword reference groups collect common terms related to Taiwan IoT Cybersecurity Certification, video surveillance system security, secure procurement, system architecture, cybersecurity, evidence management, and project planning.

Core topic keywords

Taiwan IoT Cybersecurity Certification, Taiwan IoT cybersecurity, IoT cybersecurity mark, cybersecurity conformant camera, cybersecurity certified camera, secure IP camera, secure video surveillance, video surveillance system security, surveillance cybersecurity, IoT security evaluation

Standards and certification keywords

CNS-16120, TAICS, TCA, Taipei Computer Association, Taiwan Association of Information and Communication Standards, IoT cybersecurity conformance, qualified IoT cybersecurity list, cybersecurity certificate, security level, conformity evaluation

Camera and hardware keywords

IP camera, dome camera, bullet camera, turret camera, box camera, PTZ camera, fisheye camera, multi-imager camera, thermal camera, anti-corrosion camera, explosion-protected camera, PoE camera, edge analytics camera

Cybersecurity control keywords

HTTPS, TLS, VLAN, firewall, password policy, account management, role-based access control, time synchronization, secure firmware, signed firmware, remote access control, device hardening, network segmentation, audit log

Software and integration keywords

VMS integration, NVR recording, CMS monitoring, video playback, evidence export, event search, user permissions, mobile client, notification workflow, system health management, asset inventory, firmware management

Performance keywords

high-resolution surveillance, WDR camera, low-light camera, IR illumination, optical zoom, frame rate, H.265, multi-streaming, people detection, vehicle detection, classification, recognition, perimeter monitoring

Application keywords

government facility surveillance, school security cameras, utility site monitoring, airport surveillance, transit security, hospital security cameras, critical infrastructure security, corporate compliance surveillance, warehouse security, perimeter surveillance

Common Question Phrases

what is Taiwan IoT Cybersecurity Certification, what is CNS-16120, what is TAICS IoT cybersecurity certification, what is TCA IoT cybersecurity certification, how to specify cybersecurity certified cameras, how to verify IoT cybersecurity conformance, how to document camera cybersecurity procurement, how to design a secure surveillance system, how to replace uncertified cameras, how to integrate cybersecurity conformant cameras with VMS, how to retain video evidence, how to export surveillance evidence, how to secure IP cameras, how to manage camera firmware, how to prepare for a surveillance cybersecurity audit

Source notes

Ref.	Source
[1]	ACTi Corporation, "Taiwan IoT Cybersecurity Certification," official product category page. URL: https://www.acti.com/products/taiwan-cybersecurity . Accessed: June 30, 2026.
[2]	Taiwan Association of Information and Communication Standards, "About IoT Cybersecurity Certification," official product certification page. URL: https://www.taics.org.tw/eng/Validation01.aspx?validateType_id=1 . Accessed: June 30, 2026.
[3]	Taiwan Association of Information and Communication Standards, "IoT Cybersecurity Mark," official product certification page. URL: https://www.taics.org.tw/eng/Validation01.aspx?validateType_id=2 . Accessed: June 30, 2026.
[4]	Bureau of Standards, Metrology and Inspection, "BSMI Included Cybersecurity Requirements in the Voluntary Product Certification Program for 4 Internet of Things Devices," official regulatory update. Accessed: June 30, 2026.
[5]	ACTi Corporation, "About ACTi," official corporate page. URL: https://www.acti.com/corporate . Accessed: June 30, 2026.
[6]	Mobile Application Security Alliance, "Qualified Internet of Things Cybersecurity List," official IoT list page. URL: https://www.mas.org.tw/iot/passed . Accessed: June 30, 2026.

Revision note

This document is a marketing and technical education white paper. It is not a legal opinion, regulatory certification, cybersecurity audit, privacy assessment, penetration test, or final project design. Always validate current standards, tender requirements, certificate status, field of view, lighting, recording settings, storage, network security, VMS control, system health monitoring, maintenance access, and operator workflow in the target scene before deployment.

Prepared by ACTi Corporation

For Taiwan IoT Cybersecurity Certification projects, confirm product category selection, certificate requirements, security level, recording platform, cybersecurity policy, mounting accessories, and regional availability with your ACTi sales contact or authorized system integrator.

sales@acti.com | www.acti.com