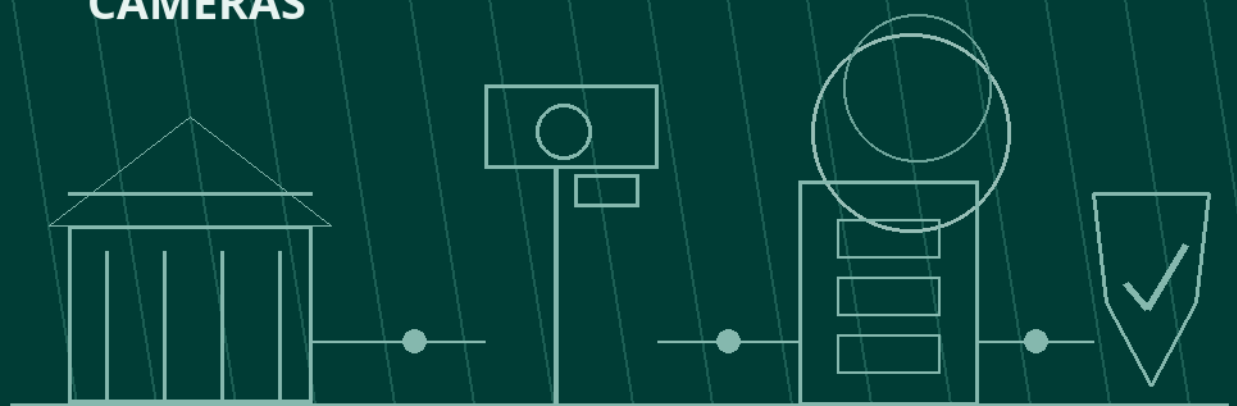


ACTi

Physical Security End-to-End Solution Provider

White Paper | NDAA Compliant Cameras

NDAA COMPLIANT CAMERAS



A practical white paper for specifying NDAA compliant IP camera systems,
secure procurement workflows, and trusted video surveillance deployments

Contents

- 1 Executive Summary
- 2 About ACTi Corporation
- 3 Definition of "NDAA Compliant Cameras"
- 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 NDAA compliant cameras mean in professional physical security projects, why compliance affects camera procurement, and how system integrators, consultants, and end users should specify compliant surveillance systems.

It is written for project teams that need security cameras for government, education, healthcare, utilities, transportation, critical infrastructure, corporate facilities, and other environments where procurement restrictions, cybersecurity expectations, supply-chain traceability, and audit readiness matter.

The document references ACTi public product information for NDAA compliant cameras and official U.S. procurement language related to covered telecommunications and video surveillance equipment. It avoids model-specific naming so the content remains usable even as individual part numbers or product generations change.

Reading guide

Use Sections 3 and 4 to define compliance and technical requirements, Section 5 to map applications, Section 6 to review the system architecture, and Section 7 to align ACTi product categories with project needs.

1. Executive Summary

NDAAs compliant cameras are IP surveillance cameras selected for projects where U.S. procurement restrictions and supply-chain controls must be considered. In practice, the term is most often associated with Section 889 of the FY 2019 National Defense Authorization Act and related Federal Acquisition Regulation clauses covering certain telecommunications and video surveillance equipment or services. [3][4]

ACTi positions its NDAAs compliant camera portfolio as a trusted option for projects that require compliant security cameras, including products using system-on-chip components from suppliers in Taiwan, Japan, or the United States. ACTi public materials state that the portfolio includes more than 150 NDAAs compliant security cameras and a product matrix to support model-by-model procurement verification. [1]

For system integrators, NDAAs compliance should not be treated as a checkbox at the end of a proposal. It affects product sourcing, documentation, tender language, network architecture, secure configuration, firmware maintenance, recording design, and replacement strategy. For consultants and end users, the correct specification should define both compliance expectations and surveillance performance requirements.

Core message

NDAAs compliant camera projects should combine compliant device selection, documented supply-chain review, secure network design, reliable recording, evidence workflow, and lifecycle management. Compliance improves procurement confidence only when the complete surveillance system is specified and maintained correctly.

Key takeaways

- NDAAs compliance is especially important for public-sector, federal-funded, defense, education, utility, transportation, and critical-infrastructure projects.
- Camera selection should be based on both compliance status and application fit: resolution, low-light performance, WDR, optical zoom, analytics, environmental protection, mounting, and recording needs.
- Project teams should confirm compliance documentation, origin requirements, latest product availability, accessory compatibility, and regional procurement requirements before submission.
- The surveillance architecture must include network security, user permissions, time synchronization, VMS/NVR retention, event search, evidence export, and system health monitoring.
- A compliant camera can still fail the project if it is poorly configured, installed with the wrong field of view, recorded at the wrong profile, or maintained without firmware and asset-control discipline.

Procurement principle

Do not specify NDAAs compliant cameras only by a marketing label. Specify compliance evidence, intended use, system architecture, cybersecurity controls, recording policy, retention, documentation, replacement rules, and operator workflow 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 security-industry experience 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 includes IP cameras, recording platforms, video management, access control, central management, system health management, AI-enabled video technologies, mobile operation, and third-party system integration. [5]

This broader ecosystem matters for NDAAs compliant camera projects. Procurement teams may begin with the camera, but the project succeeds only when the full system can maintain trusted device selection, secure communication, reliable recording, event investigation, multi-site operation, and documented support throughout the lifecycle.

Why ACTi is relevant to NDAAs compliant camera projects

ACTi strength	Project relevance
NDAAs compliant camera portfolio	ACTi public materials describe more than 150 NDAAs compliant cameras and a product matrix that can help integrators verify project fit before procurement. [1]
End-to-end security system scope	Cameras can be planned together with NVR/VMS, CMS, analytics, access control, mobile operation, and system health management instead of being treated as isolated endpoints.
Video as a foundation	ACTi emphasizes video-based security technologies; for compliance-sensitive projects, reliable video evidence must be captured, protected, searched, exported, and retained.
Project and documentation fit	System integrators can align compliant camera categories, application requirements, compliance notes, accessory needs, and lifecycle support with tender and audit expectations.

3. Definition of "NDAA Compliant Cameras"

An NDAA compliant camera is a security camera selected and documented so it can be used in projects where procurement rules restrict certain covered telecommunications or video surveillance equipment and services. In U.S. federal procurement language, covered equipment restrictions are implemented through Section 889 and related FAR provisions. [3][4]

For surveillance projects, the phrase usually refers to cameras that avoid prohibited sources and components covered by the rules, and that can be supported with reasonable compliance evidence during tender, award, deployment, and audit review. Compliance should be validated against the latest manufacturer documentation and project-specific procurement requirements.

ACTi describes its NDAA compliant camera portfolio as using SoC components from trusted suppliers in Taiwan, Japan, or the United States, and states that its NDAA product matrix helps integrators verify model-by-model compliance before procurement. [1]

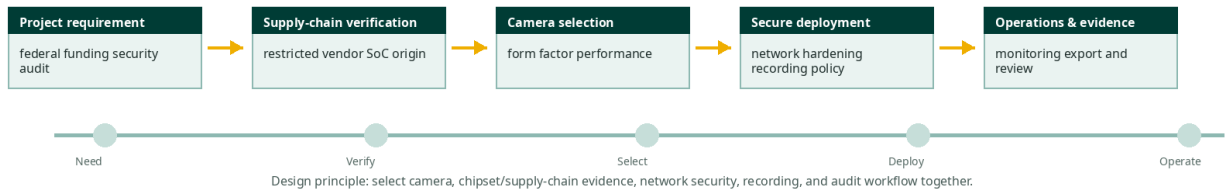
NDAA compliant cameras vs. related concepts

Term	Meaning	Common misunderstanding
NDAA compliant camera	IP surveillance camera selected for projects that require compliance with applicable procurement restrictions and supply-chain expectations.	It is not the same as a complete legal opinion; project documentation and buyer-side representations may still be required.
Covered telecommunications equipment	Regulated equipment or services identified by Section 889 and FAR clauses when used as a substantial or essential component or as critical technology. [3]	The restriction is broader than camera hardware alone; services, systems, components, and contractor use may matter.
Supply-chain verification	Review of manufacturer, chipset, origin, declarations, and product matrix information to support procurement decisions.	A one-time check is not enough if products change, substitutions occur, or project requirements require a specific origin.
Cybersecurity hardening	Secure account control, encrypted management, network segmentation, firmware policy, and remote-access control.	NDAA compliance does not automatically mean the device is securely deployed.
Procurement documentation	Tender notes, manufacturer statements, product matrix, asset list, and records supporting audit and acceptance.	Compliance value can be lost if the project cannot prove what was installed and maintained.

Visual concept

How NDA compliant cameras reduce procurement and deployment risk

From requirement review to auditable surveillance operation



Design note

NDA compliant cameras create value when compliance review is tied to practical system design. The complete chain must be planned: tender requirement, supply-chain verification, camera form factor, field of view, PoE/network path, cybersecurity policy, recording, VMS/NVR search, evidence export, firmware maintenance, and replacement control.

Practical deployment interpretation

In a school, courthouse, airport, utility site, public transit facility, hospital, warehouse, office, or critical infrastructure environment, the system may face procurement audits, cyber review, high retention requirements, difficult lighting, harsh weather, remote monitoring, and future replacement needs. The design should therefore protect both compliance confidence and operational evidence value.

4. Core Technical Concepts

NDAA compliant camera selection should begin with the procurement requirement and the security objective. The goal is to provide compliant sourcing, useful video, reliable recording, secure network operation, and defensible documentation at the required site, lighting condition, distance, and retention policy. The following concepts help teams avoid under-designed specifications.

Concept	Practical meaning
Compliance scope	Identify whether the project is federal, state, municipal, grant-funded, defense-related, critical infrastructure, or private-sector with customer-imposed NDAA language.
Supply-chain and SoC review	Confirm manufacturer documentation, chipset origin requirements, product matrix status, and whether the project requires additional origin assurance.
Camera performance	Resolution, WDR, low-light support, IR distance, optical zoom, frame rate, compression, lens type, and analytics must match the application rather than only the compliance label.
Form factor and environment	Bullet, dome, turret, PTZ, fisheye, multi-imager, box, thermal, anti-corrosion, or explosion-protected form factors should fit weather, vandalism, mounting, and coverage needs.
Network and cybersecurity	PoE budget, VLANs, HTTPS/TLS, account control, password policy, firmware policy, time synchronization, firewall rules, and remote access protect system integrity.
Recording and evidence	NVR/VMS compatibility, bit rate, retention period, synchronized time, event search, playback, export, chain-of-custody process, and audit trail determine evidence usability.
Documentation and lifecycle	Asset inventory, installed location, serial records, firmware version, replacement approval, support path, and decommissioning controls support ongoing compliance.

Specification interpretation

A camera with compliant sourcing can still fail the project if the wrong lens is selected, image quality is insufficient, the network is insecure, the recorder uses an unsuitable profile, retention is too short, or the installed asset list cannot be reconciled during an audit. Conversely, a well-integrated system can improve compliance readiness, cybersecurity, evidence handling, and operational efficiency at the same time.

Capability matrix

NDAACompliance requirement to system capability matrix

Translate procurement requirements into deployable camera, network, recording, and documentation controls.

Project requirement	What can go wrong	Capabilities to specify	Operational output
Federal or grant-funded procurement	Non-compliant equipment blocks award or audit acceptance	NDAACompliant camera list, SoC origin, vendor documentation	Defensible procurement
Sensitive facility surveillance	Untrusted device increases cyber and supply-chain risk	Trusted chipset, secure firmware policy, HTTPS, user control	Risk-reduced deployment
Lifecycle and replacement planning	One device change breaks compliance status	Asset inventory, firmware tracking, approved substitutes	Sustainable compliance
Evidence and incident review	Compliant camera still fails if recording is incomplete	NVR/VMS retention, time sync, search, export, audit trail	Searchable evidence

How to use this matrix

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

For tender writing, define the project type first. Then specify the NDAACompliant camera categories, required origin assurance, product matrix confirmation, video performance, cybersecurity baseline, recording platform, evidence export process, replacement rules, and documentation package.

5. High-Value Applications

NDAAs compliant cameras are most valuable where security performance, procurement restrictions, and audit confidence overlap. ACTi public materials identify NDAAs compliance as a mainstream requirement and describe a broad compliant camera portfolio for security projects. [1][2]

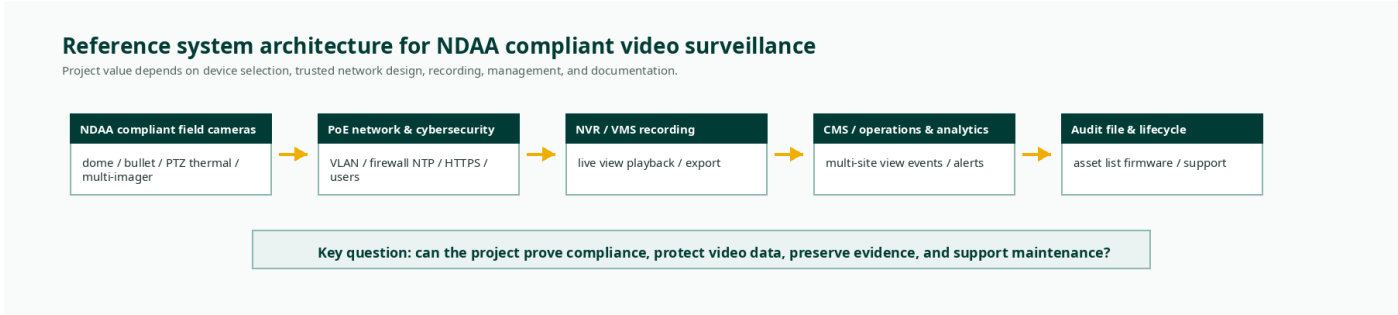
Application	Operational value	Typical locations
Government and public facilities	Support compliant procurement, visitor and perimeter monitoring, incident review, and long-term evidence retention.	City halls, courthouses, administrative buildings, public service centers
Schools and campuses	Align camera procurement with public funding, safety policies, and searchable video evidence for incidents.	School entrances, hallways, parking areas, dormitories, campuses
Utilities and critical infrastructure	Improve supply-chain confidence while monitoring restricted zones, perimeter risk, and operational assets.	Power facilities, water plants, substations, data centers, control rooms
Transportation and airports	Support surveillance for high-traffic areas, restricted access points, and compliance-sensitive infrastructure.	Stations, terminals, depots, platforms, parking, service areas
Healthcare facilities	Provide compliant surveillance for public areas, staff-only spaces, pharmacy or lab access, and incident investigations.	Hospitals, clinics, laboratories, care facilities
Corporate and defense contractors	Meet customer-imposed procurement language while supporting security operations and evidence workflows.	Offices, warehouses, manufacturing sites, R&D labs, secure rooms

Value by stakeholder

Stakeholder	Main benefit
System integrator	Stronger differentiation when proposals connect compliant camera categories, secure architecture, recording, documentation, and lifecycle support.
Consultant	Clearer specification language for compliance scope, device verification, network controls, evidence retention, and audit documents.
Security manager / operator	Reliable live view, event search, playback, export, and operational confidence without replacing security workflow with a procurement-only view.
Procurement team	A more defensible buying decision based on compliance evidence, application fit, support risk, lifecycle cost, and replacement control.

6. System Architecture

NDAAs compliant camera 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, system health monitoring, compliance documentation, and maintenance workflow.



7. ACTi Product Portfolio Overview

ACTi positions its NDAA compliant camera portfolio around broad surveillance needs, including high-resolution cameras, PTZ cameras, multi-imager cameras, hemispheric cameras, anti-corrosion cameras, explosion-protected cameras, and models with analytics capabilities. ACTi public materials state that the portfolio includes more than 150 NDAA compliant cameras, resolution up to 20MP, optical zoom up to 40x, IR distance up to 250 meters, and analytics including people and vehicle detection, classification, and recognition. [1]

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 compliant sourcing are required.	Entrances, corridors, parking areas, perimeters, offices, retail, schools
PTZ and high-zoom cameras	Large-area monitoring where operators need optical zoom, directional control, and long-distance visual 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 compliant camera category, indoor/outdoor installation, lens, resolution, WDR, low-light, IR, zoom, frame rate, and analytics needs.
- Required origin assurance, compliance statement, product matrix status, procurement documentation, and any government or 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, compliance 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 NDAA compliant cameras, secure surveillance procurement, system architecture, cybersecurity, evidence management, and project planning.

Core topic keywords

NDAA compliant cameras, NDAA camera, NDAA security camera, NDAA IP camera, compliant video surveillance, compliant CCTV, secure camera procurement, trusted surveillance camera, supply-chain verified camera, Section 889 camera

Regulatory and procurement keywords

NDAA Section 889, FAR 52.204-25, FAR 52.204-24, covered telecommunications equipment, covered video surveillance equipment, federal procurement, grant-funded security project, supplier verification, compliance documentation, audit readiness

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

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

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

Cybersecurity and reliability keywords

HTTPS, TLS, VLAN, firewall, password policy, account management, time synchronization, secure firmware, remote access control, device hardening, network segmentation, uptime planning, lifecycle maintenance

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 an NDAA compliant camera, when do I need NDAA compliant cameras, what does Section 889 mean for security cameras, how to specify NDAA compliant cameras, how to verify camera compliance, which camera SoC origins are acceptable, how to document NDAA camera procurement, how to design a compliant surveillance system, how to replace non-compliant cameras, how to integrate NDAA 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 compliance audit

Source notes

Ref.	Source
[1]	ACTi Corporation, "NDAA Compliant Cameras," official product category page. Accessed: June 30, 2026.
[2]	ACTi Corporation, "Specially Certified Cameras," official product category page. Accessed: June 30, 2026.
[3]	Federal Acquisition Regulation, FAR 52.204-25, "Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment." Accessed: June 30, 2026.
[4]	Federal Acquisition Regulation, FAR 52.204-24, "Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment." Accessed: June 30, 2026.
[5]	ACTi Corporation, "About ACTi," official corporate page. Accessed: June 30, 2026.

Revision note

This document is a marketing and technical education white paper. It is not legal advice, a regulatory certification, a procurement representation, a cybersecurity audit, a privacy assessment, or a final project design. Always validate current procurement clauses, customer requirements, compliance documents, 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 NDAA compliant camera projects, confirm product category selection, compliance requirements, supply-chain documentation, recording platform, cybersecurity policy, mounting accessories, and regional availability with your ACTi sales contact or authorized system integrator.

sales@acti.com | www.acti.com