ujiyari

UPSC & STATE PCS CURRENT AFFAIRS · UJIYARI.COM

DAILY CURRENT AFFAIRS

India's CCTV Certification Mandate — Digital Security, Chinese Hardware Risk, and Atmanirbhar Surveillance

1 April 2026

CURATED & WRITTEN BY

Bharat Choudhary

UPSC Educator & Content Creator

linkedin.com/in/epicbharat

India's CCTV Certification Mandate — Digital Security, Chinese Hardware Risk, and Atmanirbhar Surveillance

1 April 2026 · 5 min read · 3 tags

On this Page

WHY IN NEWS

From April 1, 2026, India's mandatory certification regime for internet-connected CCTV cameras came into force under MeitY's Essential Requirements (ER) norms, effectively banning uncertified devices and particularly targeting Chinese brands — Hikvision, Dahua, and TP-Link — that have not obtained BIS/STQC certification, citing national security risks.

THE POLICY — WHAT CHANGED

Two-Year Compliance Window Now Closed

In April 2024, the **Ministry of Electronics and Information Technology (MeitY)** notified **Essential Requirements (ER) norms** for internet-connected (IP-based) CCTV cameras — giving manufacturers a 24-month window to certify their products. From April 1, 2026:

- **All new sales** of IP-connected CCTV cameras must use certified models
- Certification is through **STQC** (Standardisation Testing and Quality Certification Directorate) under BIS's regime
- Manufacturers must **declare country of origin of the System-on-Chip (SoC)** — the central processing unit of the camera
- Devices must be tested at accredited labs for cybersecurity vulnerabilities (including backdoor access, unencrypted data transmission, firmware update mechanisms)

As of April 1, 2026: 507 camera models are certified for sale in India.

Why the SoC Declaration Matters

The SoC is the most critical component in a smart CCTV camera — it controls:

- Video encoding/compression (H.264, H.265)
- Motion detection and AI analytics
- Network connectivity (Wi-Fi, Ethernet, 4G)
- Remote access and cloud streaming
- Firmware update mechanisms

The risk: A SoC with a backdoor — either by design (government-mandated in Chinese companies' national security laws) or through supply chain compromise — can allow unauthorised access to a camera's live feed, stored footage, or network traffic. This is not hypothetical: US intelligence agencies have documented such capabilities in Chinese surveillance hardware.

WHY CHINESE BRANDS ARE BLOCKED

Hikvision and Dahua — The Global Ban Wave

Hikvision (Hangzhou Hikvision Digital Technology Co.) and **Dahua** (Zhejiang Dahua Technology Co.) are the world's two largest CCTV manufacturers, both state-owned (Chinese government holds 41.86% of Hikvision).

Bans/restrictions globally:

- **USA (2022):** FCC banned Hikvision and Dahua equipment on national security grounds under the Secure and Trusted Communications Networks Act
- **UK (2022):** Banned Hikvision and Dahua from UK government buildings; private sector guidance issued
- **Australia (2023):** Government buildings banned Chinese-made cameras
- **India (April 2026):** BIS/STQC certification requirement; Chinese brands refused certification

China's National Intelligence Law (2017): Requires all Chinese companies and citizens to "support, assist, and cooperate with state intelligence work" — creating a legal obligation for Chinese manufacturers to facilitate government access to their devices' data.

TP-Link — The Router/IoT Security Concern

TP-Link is predominantly a Wi-Fi router and smart home devices company. Its CCTV products are lower-end but widely distributed. The concern: TP-Link routers have been documented in multiple US government reports as having been compromised for Chinese state-sponsored cyber operations. India's ban extends this security logic to TP-Link's camera products.

THE MARKET TRANSFORMATION

Domestic Surge

The policy's two-year window (2024-2026) accelerated India's domestic CCTV industry dramatically:

YEAR	DOMESTIC MARKET SHARE
2020	~20%
2022	~45%
Early 2026	**>80%**

Key domestic players:

- **CP Plus** (Aditya Infotech Ltd, Delhi): India's largest — was already manufacturing in India; expanded rapidly
- **Bosch Security Systems India**
- **Honeywell India** (now Resideo)
- **Godrej Security Solutions**
- **Zicom Electronic Security Systems**

International compliant brands: Axis Communications (Sweden), Avigilon (Motorola Solutions, USA) — both certify and do not use Chinese SoCs.

The ₹7,000 Crore Opportunity

India's CCTV market was ~₹7,000 crore/year (2024). With 130+ million cameras installed (3rd largest market globally) and ongoing Smart City Mission, Safe City projects, and residential boom driving new installations — the banned Chinese brands' market share (~₹5,000 crore equivalent) is being captured by domestic and Western manufacturers.

THE BROADER DIGITAL SECURITY ARCHITECTURE

MeitY's Hardware Security Push

The CCTV mandate is part of a broader MeitY push for supply-chain security in critical infrastructure hardware:

- **Telecom Equipment (2022):** Trusted Telecom Portal — only telecom equipment from approved vendors can be deployed in Indian networks (effectively banned Huawei and ZTE from 5G rollout)
- **CCTV (2026):** This mandate
- **Smart Meters:** BIS certification requirements for IoT-enabled electricity meters
- **Routers (proposed):** BIS certification for home and enterprise routers is under discussion

Safe City Mission

India's **Safe City Mission** — a component of the Nirbhaya Fund — has deployed hundreds of thousands of surveillance cameras in 8 cities (Delhi, Mumbai, Kolkata, Chennai, Bengaluru, Hyderabad, Ahmedabad, Lucknow). The surveillance infrastructure of these cities was dominated by Hikvision/Dahua equipment. Replacement and new procurement must now use certified alternatives — driving government tender activity worth thousands of crore.

UPSC RELEVANCE

STQC; BIS; MeitY; Essential Requirements (ER) norms (April 2024); 507 certified models; SoC; Hikvision; Dahua; TP-Link; Safe City Mission; China's National Intelligence Law 2017.

MAINS GS-3 (INTERNAL SECURITY + S&T):

"Cybersecurity risks in surveillance infrastructure — evaluate India's response to Chinese CCTV hardware dominance and the effectiveness of the BIS/STQC certification framework."

MAINS GS-2:

"Digital sovereignty and hardware security — how should India balance economic openness with national security in technology procurement?"

INTERVIEW:

"India bans Chinese CCTV cameras on security grounds but imports critical components for its defence hardware from China. Isn't this contradictory?"

📌 FACTS CORNER — KNOWLEDGEPEDIA

CCTV CERTIFICATION MANDATE:

Effective: April 1, 2026

Nodal ministry: MeitY

Certification body: STQC (Standardisation Testing and Quality Certification Directorate)

Framework: BIS mandatory certification + Essential Requirements (ER) norms (notified April 2024)

Certified models (April 2026): 507

Compliance window: 24 months (April 2024 – March 2026)

Key requirement: SoC country-of-origin declaration; cybersecurity testing

BLOCKED BRANDS:

Hikvision: Hangzhou Hikvision Digital Technology; state-owned (41.86% Chinese govt); world's largest CCTV maker

Dahua: Zhejiang Dahua Technology; world's 2nd largest

TP-Link: Wi-Fi/IoT devices; CCTV range blocked

GLOBAL BANS ON CHINESE SURVEILLANCE TECH:

USA (2022): FCC banned Hikvision + Dahua; NDAA 2019 banned federal procurement

UK (2022): Government buildings banned; private sector guidance

Australia (2023): Government buildings banned

India (April 2026): BIS/STQC certification requirement

INDIA'S CCTV MARKET:

Market size: ~₹7,000 crore/year (2024)

Installed base: 130+ million cameras — 3rd largest globally

Domestic market share: >80% (April 2026); was ~20% in 2020

Key domestic player: CP Plus (Aditya Infotech, Delhi)

BROADER MEITY HARDWARE SECURITY:

Trusted Telecom Portal (2022): blocks Huawei/ZTE from Indian 5G networks

CCTV ER norms (2024/2026): this mandate

IT Act 2000 + DPDPA 2023: data protection framework

OTHER RELEVANT FACTS:

China's National Intelligence Law (2017): obliges Chinese companies to assist state intelligence — legal basis for backdoor risk

SoC (System-on-Chip): integrates CPU, GPU, network, storage controller on one chip

STQC: under MeitY; 20+ test/calibration labs; also certifies IT products under TEC/BIS schemes

Safe City Mission (Nirbhaya Fund): 8 cities; CCTV surveillance + emergency response integration

Huawei Telecoms ban: India did not formally ban Huawei for 5G but used Trusted Telecom Portal to exclude them

Sources: MeitY , PIB , GKToday , InsightsIAS

← PREVIOUS ARTICLE
Artemis II — First Crewed Lunar Mission in 53 Years and...

NEXT ARTICLE →
Kaynes OSAT Plant — India's Semiconductor Indigenisation...

RELATED EDITORIALS

BUSINESS STANDARD
Corporate Laws Amendment Bill, 2026 — Rationalising India's Business Regulation Architecture
1 Apr

INDIAN EXPRESS
Digital Sovereignty Begins at the Hardware Layer — India's CCTV Mandate and What Comes Next
1 Apr

DOWN TO EARTH
Rethinking E20 — India's Ethanol Mandate, Climate Trade-offs, and the Food-Fuel Tension
1 Apr

INDIAN EXPRESS
India's Semiconductor Moment — From Design Strength to Fab Reality
1 Apr

CURATED & WRITTEN BY

Bharat Choudhary

UPSC Educator & Content Creator

linkedin.com/in/epicbharat

📖 Read Full Article on Ujiyari →

https://ujiyari.com/daily/2026/04/01/cctv-ban-india-stqc-bis-digital-security/