SECURITY REQUIREMENTS ADDED

MeitY adds essential security requirements for CCTV cameras under the 2021 registration order

S.O. 1652(E) adds essential security requirements for CCTV Camera at S. No. 41, applying six months after publication, with 30 testing parameters.

S.O. 1652(E), AN ORDER OF THE Ministry of Electronics and Information Technology (IPHW Division) dated April 9, 2024, amends the Electronics and Information Technology Goods (Requirement of Compulsory Registration) Order, 2021 under sub-sections (1) and (2) of section 16 read with sub-section (3) of section 25 of the Bureau of Indian Standards Act, 2016. For CCTV Camera, it adds an entry of column (5), Essential Requirement(s), at S. No. 41 of the Schedule: Essential Requirement(s) for CCTV as per Annexure. The entry prints the Indian Standard as IS 13252: Part 1: 2010.

THE CHANGE

For CCTV Camera, S. No. 41 of the Schedule carries an entry in column (5), Essential Requirement(s): Essential Requirement(s) for CCTV as per Annexure, applying on the expiry of six months from the date of publication of the notification in the Official Gazette.

KEY FACTS

TYPE

Security requirements added

S.O. NUMBER

S.O. 1652(E)

DATED

April 9, 2024

APPLIES FROM

On the expiry of six months from the date of publication of the notification in the Official Gazette (paragraph 3 of S.O. 1652(E)); no date is printed

REFERENCES

S.O. 1652(E)

CG-DL-E-09042024-253632

MeitY adds essential security requirements for CCTV cameras under the 2021 registration order

S.O. 1652(E) · April 9, 2024

S.O. 1652(E), an order of the Ministry of Electronics and Information Technology (IPHW Division) dated April 9, 2024, amends the Electronics and Information Technology Goods (Requirement of Compulsory Registration) Order, 2021 under sub-sections (1) and (2) of section 16 read with sub-section (3) of section 25 of the Bureau of Indian Standards Act, 2016. For CCTV Camera, it adds an entry of column (5), Essential Requirement(s), at S. No. 41 of the Schedule: Essential Requirement(s) for CCTV as per Annexure. The entry prints the Indian Standard as IS 13252: Part 1: 2010.

The order applies to CCTV Camera, for conforming to these essential requirements, on the expiry of six months from the date of publication of the notification in the Official Gazette; it prints no calendar date. As per Scheme II of the BIS Conformity Assessment Regulations, 2018, submission of test reports from BIS recognized labs is a pre-requisite for obtaining a licence to use the Standard Mark.

The Annexure, Essential Requirement(s) for Security of CCTV, names the key areas of testing: exposed network services, device communication protocols, physical access to the device's UART, JTAG, SWD, etc., the ability to extract memory and firmware, firmware update process security, and storage and encryption of data. It lists five brief requirements: physical security, access control, network security, software security and penetration testing.

Its table of Essential Security Requirements sets 30 testing parameters in four categories: Hardware Level Security Parameter (supported by software), 1.1 to 1.9; Software/Firmware, 2.1 to 2.11, with 2.7 printed twice; Secure Process Conformance, 3.1 to 3.5; and Security Conformance at product development stage, 4.1 to 4.4. Two further columns are headed What to be tested and Documents Required.

The order (F.No. W-43/11/2021-IPHW) appears in the Gazette of India, Extraordinary, No. 1569, dated April 9, 2024.

S.O. number	S.O. 1652(E)
Dated	April 9, 2024
Published in the Gazette	April 9, 2024
Gazette ID	CG-DL-E-09042024-253632
File number	W-43/11/2021-IPHW
Type	Security requirements added

Products	CCTV Camera
What it does	For CCTV Camera, S. No. 41 of the Schedule carries an entry in column (5), Essential Requirement(s): Essential Requirement(s) for CCTV as per Annexure, applying on the expiry of six months from the date of publication of the notification in the Official Gazette.
Applies from	On the expiry of six months from the date of publication of the notification in the Official Gazette (paragraph 3 of S.O. 1652(E)); no date is printed
Conditions	• The order applies to CCTV Camera, for conforming to the Essential Requirement(s) in column (5), on the expiry of six months from the date of publication of the notification in the Official Gazette. • As per Scheme II of BIS Conformity Assessment Regulations, 2018, submission of test reports from BIS recognized labs forms a pre-requisite for obtaining a licence to use the Standard Mark. • The Annexure, Essential Requirement(s) for Security of CCTV, sets 30 testing parameters in four categories, numbered 1.1 to 4.4 (2.7 is printed twice), in a table that also has columns headed What to be tested and Documents Required.
Applies to	CCTV Camera, at S. No. 41 of the Schedule (CCTV Cameras/CCTV Recorders, IS 13252: Part 1: 2010).
Issued under	Sub-sections (1) and (2) of section 16 read with sub-section (3) of section 25 of the Bureau of Indian Standards Act, 2016 (11 of 2016)
Signed by	ASHA NANGIA, Group Coordinator & Scientist 'G'

The notification, entry by entry

Entry	Text
S. No. 41: CCTV Camera, column (5) Essential Requirement(s) (added)	Essential Requirement(s) for CCTV as per Annexure
Annexure 1.1: Hardware Level Security Parameter (supported by software)	Verify that application layer debugging interfaces such USB, UART, and other serial variants are disabled or protected by a complex password.
Annexure 1.2: Hardware Level Security Parameter (supported by software)	Verify that cryptographic keys and certificates are unique to each individual device.
Annexure 1.3: Hardware Level Security Parameter (supported by software)	Verify that on-chip debugging interfaces such as JTAG or SWD are disabled or that available protection mechanism is enabled and configured appropriately.

Annexure 1.4: Hardware Level Security Parameter (supported by software)	Verify that trusted execution is implemented and enabled, if available on the device SoC or CPU.
Annexure 1.5: Hardware Level Security Parameter (supported by software)	Verify that sensitive data, private keys and certificates are stored securely in a Secure Element, TPM, TEE (Trusted Execution Environment), or protected using strong cryptography.
Annexure 1.6: Hardware Level Security Parameter (supported by software)	Verify the presence of tamper resistance and/or tamper detection features.
Annexure 1.7: Hardware Level Security Parameter (supported by software)	Verify that any available Intellectual Property protection technologies provided by the chip manufacturer are enabled.
Annexure 1.8: Hardware Level Security Parameter (supported by software)	Verify the device validates the boot image signature before loading.
Annexure 1.9: Hardware Level Security Parameter (supported by software)	Verify usage of cryptographically secure pseudo-random number generator on embedded device (e.g., using chip-provided random number generators).
Annexure 2.1: Software/Firmware	Verify that memory protection controls such as ASLR and DEP are enabled by the embedded/IoT operating system, if applicable.
Annexure 2.2: Software/Firmware	Verify that the firmware apps protect data-in-transit using transport layer security.
Annexure 2.3: Software/Firmware	Verify that the firmware apps validate the digital signature of server connections.
Annexure 2.4: Software/Firmware	Verify that any use of banned C functions are replaced with the appropriate safe equivalent functions.
Annexure 2.5: Software/Firmware	Verify that each firmware maintains a software bill of materials cataloging third party components, versioning, and published vulnerabilities.
Annexure 2.6: Software/Firmware	Verify all code including third-party binaries, libraries, frameworks are reviewed for hardcoded credentials (backdoors).
Annexure 2.7: Software/Firmware	Verify that the firmware apps pin the digital signature to a trusted server(s).
Annexure 2.7: Software/Firmware	Verify security controls are in place to hinder firmware reverse engineering (e.g.removal of verbose debugging symbols).
Annexure 2.8: Software/Firmware	Verify that the firmware update process is not vulnerable to time-of-check vs time-of-use attacks.
Annexure 2.9: Software/Firmware	Verify the device uses code signing and validates firmware upgrade files before installing.

Annexure 2.10: Software/Firmware	Verify that the device cannot be downgraded to old versions (anti-rollback) of valid firmware.
Annexure 2.11: Software/Firmware	Verify that firmware can perform automatic firmware updates upon a predefined schedule.
Annexure 3.1: Secure Process Conformance	Verify that wireless communications are mutually authenticated.
Annexure 3.2: Secure Process Conformance	Verify that wireless communications are sent over an encrypted channel.
Annexure 3.3: Secure Process Conformance	Verify that whether trusted sources are being used for sourcing the components of the device i.e. trusted supply chain through a managed Bill of materials for critical hardware components (related to security functions like SoC) is in use.
Annexure 3.4: Secure Process Conformance	Supply chain risk identification, assessment, prioritization, and mitigation shall be conducted. Supply chain risk/business continuity planning policy documents, playbooks reflecting how to handle supply chain disruption, post-incident summary documents need to be submitted and demonstrate the same.
Annexure 3.5: Secure Process Conformance	Verify the no proprietary network protocols are being used in the device. If yes, then complete implementation details and the source code for the same shall be provided.
Annexure 4.1: Security Conformance at product development stage	Design and architecture details till the PCBA and SoC level to be provided to aid in counterfeit mitigation and malware detection.
Annexure 4.2: Security Conformance at product development stage	Threat mitigation strategies for tainted and counterfeit products shall be implemented as part of product development.
Annexure 4.3: Security Conformance at product development stage	One or more up-to-date malware detection tools shall be deployed as part of the code acceptance and development processes. Malware detection techniques shall be used before final packaging and delivery (e.g., scanning finished products and components for malware using one or more up-to-date malware detection tools).
Annexure 4.4: Security Conformance at product development stage	Supply chain risk identification, assessment, prioritization, and mitigation shall be conducted.

The notification (PDF, 742 KB)

Gazette of India, CG-DL-E-09042024-253632, published April 9, 2024.

Checked against the official copy on October 27, 2026.

IndusDesk

hello@indusdesk.com · +91 11 4141 3939

9th Floor, Hemkunt House, Rajendra Place, New Delhi, Delhi 110008, India

Read online: indusdesk.com/meity/tracker/adds-essential-security-requirements-for-cctv-cameras-253632/