KHAITAN &CO ADVOCATES SINCE 1911

UPDATE

ERGO

Analysing developments impacting business

SHARPER WATCH: MEITY INTRODUCES ENHANCED SECURITY REQUIREMENTS FOR CCTV SYSTEMS

30 April 2024

On 9 April 2024, the Ministry of Electronics and Information Technology (MEITY) amended the Electronics and Information Technology Goods (Requirement of Compulsory Registration) Order, 2021 (CRO 2021). Under the amendment, MEITY has mandated certain 'essential security requirements' for Closed-Circuit Television (CCTV) cameras (CRO Amendment). The CRO Amendment will be effective from 9 October 2024, giving manufacturers of CCTV cameras six months to conform to the requirements under the CRO Amendment.

Reportedly, around 90% out of more than two million CCTV cameras installed and used across India in 2023 were manufactured by Chinese companies. This includes CCTV cameras used in government institutions and establishments as well as public spaces in India, which could expose sensitive data to security threats. Countries such as the USA, the UK and Australia have taken steps over the past few years to prohibit the use of surveillance products manufactured by Chinese companies on grounds of national security.

The CRO Amendment underpins India's own effort to secure its infrastructures against potential foreign surveillance facilitated by compromised surveillance technology by enforcing strict standards for security and enhancing the overall integrity of surveillance systems.

Key Provisions of the CRO Amendment

The sale of CCTV cameras in India is permitted only if such CCTV cameras carry a standard mark issued by the Bureau of Indian Standards (BIS). For the grant of license to use such standard mark issued by the BIS, all manufacturers of CCTV cameras in India are required to adhere to:

a) the 'essential security requirements' provided under the CRO Amendment; and

b) the relevant Indian Standard as provided under the CRO 2021.

Applicants for the BIS standard mark are required to submit test reports from a lab recognized by the BIS, evidencing adherence to the above.

The 'essential security requirements' under the CRO Amendment include the following:

a) ***Hardware Level Security Parameters***: The CRO Amendment prescribes several testing parameters such verification of protection of debugging interfaces with a password,

uniqueness of cryptographic keys and certificates, presence of tamper resistance/detection features, etc.

b) ***Software / Firmware***: This category requires testing of memory protection controls, protection of data-in-transit, validation of digital signature of server connections, verification of code for back-doors, verification that firmware apps pin the digital signature to trusted servers, etc.

c) ***Secure Process Conformance***: This category of tests requires verification of sources of components of the device, supply chain risk identification, verification of non-proprietary network protocols, mutual authentication of wireless communications, etc.

d) ***Security Conformance at Product Development Stage***: Under this category, design and architecture documents have to be provided, threat mitigation strategies are required to be implemented and malware detection tools have to be deployed. Supply chain risk identification, an exercise stipulated in the previous category, is also a requirement under this category.

Conclusion

MEITY had previously issued a notification dated 6 March 2024 (PPO 2024) in furtherance of the Public Procurement (Preference to Make in India) Order, 2017, encouraging preference to procurement of locally manufactured CCTV cameras by government entities which also set out the essential security requirements which are now included under the CRO Amendment.

The PPO 2024 was followed by an advisory issued by MEITY on 11 March 2024 to government ministries and departments, prescribing guidelines to be followed for procurement of CCTV systems, such as blacklisting of CCTV brands with history of security failures, ideal network security practices, etc.

In this context, the CRO Amendment seeks to further enhance cybersecurity measures amid the growing dependency on digital surveillance and as a response to rising concerns around escalating cyber threats and vulnerabilities in the security of CCTV systems in India.

- *Tanu Banerjee (Partner); Ishan Johri (Principal Associate); Heema Shirvaikar (Senior Associate) and Vaibhav Laddha (Associate)*

For any queries please contact: editors@khaitanco.com