Guidance on supply chain security aspects covered in the Essential Requirements (attached) released by MeitY.

Security of CCTV cameras is very important. There is a risk of leakage of sensitive video footage/ image to the unauthorized personnel if the CCTV cameras are insecure. Government of India vide the Gazette Notification dated 07/03/2024[1] has published Essential Security Requirements to be adhered to by all CCTV cameras being procured by the Government. The following sections (Given at Sr. No. 3 and 4 in Annexure A of the Notification) have been reproduced from the Essential Requirements (ERs) of this notification which are to be complied by CCTV cameras. These are related to:

- Ensuring the components are from trusted source
- Supply-Chain
- counterfeit mitigation and malware detection
- Threat mitigation strategies for tainted and counterfeit products

Against each of these following ERs, 'Guidance to the Test Lab has been provided for conducting assessment.

3.3 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.

Documents Required: Bill of materials for critical hardware components (related to security functions like SoC).

Guidance to Test Lab:

- *Verify the security critical components in the CCTV camera. The security critical components (i.e. components impacting the security compliance as per the ERs listed in Annexure A of the above document) are SoC, Firmware, PCBA, Network Interface Card (NIC) and Physical Interfaces (e.g. USB, UART, and other serial variants, JTAG or SWD available in CCTV).*
- *Verify PCBA with respect of design for its correct implementation. Vendor has to provide design document, layout diagram, and X-Ray images of PCBA to accomplish this activity.*
- *Verify physical interfaces and NIC for vulnerabilities like unauthorized access and data manipulation. Verify USB, UART, JTAG, and SWD interfaces by conducting security assessments to confirm strict access controls and to ensure there is no unintended data flows.*
- *Verify The bill of materials and invoices in respect of SoC and firmware. If any of these components are being developed in house, then no invoice for such component is needed.*

[1] the Gazette of India CG-DL-E-08032024-252738 Extraordinary PART II—Section 3—Sub-section (ii) No. 1062 NEW DELHI, THURSDAY, MARCH 7, 2024

- *Verify that the SOC and firmware are not sourced from Land Border Sharing Countries. This needs verification via invoices, technical literature, and other supporting documents provided by the client.*
- *Verify the traceability of SoC and firmware from procurement through to integration into the final product.*

3.4 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.

Documents Required: Vendor shall submit the following:

- Supply chain risk identification, assessment, prioritization and mitigation documents.
- Supply chain risk/business continuity planning policy documents,
- Playbooks reflecting how to handle supply chain disruption
- Post-incident summary documents.

Guidance to Test Lab:

- *Verify that the Supply chain risk identification, assessment, prioritization and mitigation of risks pertaining to these components have been conducted by the vendor. The Vendor must ensure that all invoices of SoC and firmware are available. Verify any of the SoC and firmware are not from land Border Sharing Countries.*
- *Verify that the supply chain risk/business continuity planning policy documents have been prepared by the vendor. Verify that the Playbooks reflecting how to handle supply chain disruption is available with Vendor. Verify that the post-incident summary documents are available for the incidents related to Supply Chain.*

3.5 Verify the no proprietary network protocols are being used in the device. If yes, then complete implementation details and the source code

Documents Required: Vendor shall submit the following:

- Document mentioning implementation details and the source code specific to proprietary protocols

Guidance to Test Lab:

- *Verify the presence of proprietary network protocols by analyzing network traffic with tools like Wireshark, Nmap, inspecting device configurations, consulting vendor documentation, interviewing administrators, and using packet inspection tools. Contact vendors for clarification and ensure compliance with network standards.*
- *Verify the source code (in case proprietary network protocols are implemented) to ensure that there is no malicious code.*

4.1 Design and architecture details till the PCBA and SoC level to be provided to aid in counterfeit mitigation and malware detection.

Documents Required: Design and architecture documents till the PCBA and SoC level.

Guidance to Test Lab:

- *Verify that the SOC and firmware are not sourced from Land Border Sharing Countries. This needs verification via invoices, technical literature, and other supporting documents provided by the client.*
- *Verify The bill of materials and invoices in respect of SoC and firmware. If any of these components are being developed in house, then no invoice for such component is needed.*
- *Verify physical interfaces and NIC for vulnerabilities like unauthorized access and data manipulation. Verify USB, UART, JTAG, and SWD interfaces by conducting security assessments to confirm strict access controls and to ensure there is no unintended data flows.*
- *Verify PCBA with respect of design for its correct implementation. Vendor has to provide design document, layout diagram, and X-Ray images of PCBA to accomplish this activity.*
- *Verify that the Vendor has anti-virus solution and shall ensure the firmware is free from malware before provisioning it to CCTV.*

4.2 Threat mitigation strategies for tainted and counterfeit products shall be implemented as part of product development.

Documents Required: Process and method artifacts need to be submitted and demonstrate the same.

Guidance to Test Lab

- *Verify that the SoC and firmware are not from a Land Border Sharing Country and are as per the required specifications.*
- *Verify PCBA with respect of design for its correct implementation. Vendor has to provide design document, layout diagram, and X-Ray images of PCBA to accomplish this activity.*
- *Verify physical interfaces and NIC for vulnerabilities like unauthorized access and data manipulation. Verify USB, UART, JTAG, and SWD interfaces by conducting security assessments to confirm strict access controls and to ensure there is no unintended data flows.*
- *Verify that the vendor has up-to-date anti-virus solution and shall ensure the firmware is free from malware before provisioning it to CCTV.*
- *Verify existence of acceptance criteria and measures to detect counterfeit or malicious components through physical inspections, anti-malware scanning, or testing.*
- *Verify use of malware analysis tools before final packaging and delivery.*

4.3 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 upto-date malware detection tools).

Documents Required: List of components that have been identified as requiring tracking targets of tainting/ counterfeiting, CM tool. Quality assurance process needs to be submitted and demonstrate the same.

Guidance to Test Lab

- *Verify that the vendor has up-to-date malware detection tools and shall ensure the firmware is free from malware before provisioning it to CCTV.*
- *Verify that the secure configuration is implemented during provisioning of CCTV.*

4.4 Supply chain risk identification, assessment, prioritization, and mitigation shall be conducted.

Documents Required: 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.

Guidance to Test Lab:

- *Verify that the Supply chain risk identification, assessment, prioritization and mitigation of risks pertaining to these components have been conducted by the vendor.*
- *Verify that the supply chain risk/business continuity planning policy documents have been prepared by the vendor. Verify that the Playbooks reflecting how to handle supply chain disruption is available with Vendor. Verify that the post-incident summary documents are available for the incidents related to Supply Chain.*