Essential Requirements Generic Pre-Test Application Form

We request that a separate application is filled out for each product for which tests are being undertaken.

Only columns that are highlighted in grey are mandatory. If left blank, the default values in the “Instructions” column will be used for conducting the tests.

Fill only those sections which are applicable for the product variant under test

Section:1

Administrative Information	**Instructions**	**To be filled by the Customer**
Tested For Company & Address of the Company	Company name who is submitting the Project	
OEM Name & Address	Manufacturer Name and Address	
Date of application	Date of Sample Submission	
Administrative and Technical Contacts	Support contact in case of the Issues/Bugs found in the SW/FW	
E-Mail		
Phone		
Intermediary Company Name		
Requested Test Start Date		
Requested Completion Date		

Section 2:

Device Information	Instructions	To be filled by the Customer
Brand/Vendor Name		
Product Name/ Model Number		
Product / Device description	Detailed description of the Device	
Serial Number of the Device		
Software/Firmware Major and Minor Versions	Major and Minor versions of the software / firmware	
Information on series of product	Include list of all models in family	
Kernel Version		
Environment for OS/Protocol Stack used	Complete if Target is OS/Protocol Stack	
Interface used for Testing	Ethernet/WiFi Interface	
Product Classification	Applicable ER name	
Region / Country Name		
Version of test spec. and scenarios	Complete only if specific tests need to be performed else approved versions below will be used	
Test Specification	ER Number Applicable	
Decision Rule for reporting Statement of conformity	As Per Standard/Not Applicable	

Note:

1) All the above fields are mandatory
2) If provided details are not matching against the DUT, then Lab will update the actual test details and not the details given in pre-test form
3) Kindly provide the GUI/CLI commands to perform all requested test parameters & Configuration guide.
4) Kindly Provide the Compatible SFP's to test Optical Ethernet Interface test Parameters (FE/1GE/10GE/25GE/40GE/50GE/100GE, as applicable)

Product Variant: <Please Fill Product Type >

Test case description	Test case Specification	Remarks	The GUI/CLI commands to perform the test parameters.

Name of the authorized signatory:

Date:

S.l No	Requirement No.	Documentation / Software files and other information, requirements from the OEM	Instructions	OEM's Response	Remarks
1.	1.1, 1.3, 1.7, 1.8, 1.9	Schematic diagram, Datasheet of device and the SoC being used in the device.	The customer should provide the Schematic diagram, Datasheet of the device and SoC being used.	☐ Available and Provided ☐ Not Available ☐ Other (please see remarks)	
2.	1.1, 1.3	Documentation related to ports/interfaces enabled in the production devices and the related access control mechanism for protection of the same.	A detailed list of all the ports and interfaces enabled on the production devices, such as USB, Ethernet, and serial ports. The specific access control mechanisms employed to protect these interfaces, including firewalls, access control lists (ACLs), and authentication methods like passwords or key-based systems. (Also refer S.No 1)	☐ Available and Provided ☐ Not Available ☐ Other (please see remarks)	
3.	Section 1 & 4	System Security Engineering Manual (or Technical Construction File (TCF)) which focuses on implementation mechanisms should be provided.	The TCF shall define contexts to ensure the security of a system, which is based on achieving a complete understanding of security objectives, security concerns, protection needs, and security		

			requirements. This shall be evaluated using the artifacts requested in the Essential Requirements. Hardware and software architecture of the device.		
4.	1.1, 1.3	Process flow of the Manufacturing/Provisioning of the device	A detailed outline of the process flow for manufacturing and provisioning the device. This includes the stages of component procurement, assembly, initial testing, firmware installation, and quality assurance. Details on the provisioning steps, such as configuring device settings, installing necessary software, and performing final inspections before shipping. Information on any automated systems or tools used in the process, and the roles and responsibilities of personnel involved at each stage.	☐ Available and Provided ☐ Not Available ☐ Other (please see remarks)	
5.	1.2, 1.5	List of all keys and certificates being used in the device	A catalog of all keys and certificates	☐ Available and Provided	

		ecosystem	utilized within the device ecosystem. This should encompass details of encryption keys, authentication keys, SSL/TLS certificates, code-signing certificates, and any other cryptographic keys. Information on the purpose of each key or certificate, the issuing authority, expiration dates, and the methods for secure storage and management. (Please also refer Note 1)	☐ Not Available ☐ Other (please see remarks)	
6.	1.2, 1.5, 1.8	Key management life cycle (purpose, generation, storage, destruction/zeroization, validity, key changeover/rotation)	A description of the key management lifecycle, covering the following aspects: the purpose of each key, the procedures for key generation, the secure storage methods employed, and the protocols for key destruction or zeroization. Details on the validity period of keys, the process for key changeover or rotation, and the mechanisms in place to ensure the secure	☐ Available and Provided ☐ Not Available ☐ Other (please see remarks)	

			transition of keys. (Please also refer Note 1)		
7.	1.4	User manual/ Technical specifications of the device	A user manual and technical specifications for the device. This should include easy-to-follow instructions for setup and operation, a list of features, troubleshooting tips, and maintenance guidelines. (Please also refer Note 1)	☐ Available and Provided ☐ Not Available ☐ Other (please see remarks)	
8.	1.4	Code snippets of the TEE API call, wherever applicable	The source code that demonstrates TEE API calls, applicable for devices where TEE, SE, or TPM is available and enabled. This includes examples of initializing the TEE, performing cryptographic operations, and securely storing keys using TEE APIs. These snippets should illustrate proper integration and usage of the secure environment to ensure cryptographic functions are correctly handled through	☐ Available and Provided ☐ Not Available ☐ Other (please see remarks)	

			TEE/SE/TPM APIs. (Please also refer Note 1)		
9.	1.5	List of all the sensitive data with their intended usage and secure storage mechanism(s)as implemented along with secure configurations to be enabled in the device.	An inventory of sensitive data with details on their intended usage and the secure storage mechanisms implemented. Information on how each type of sensitive data is accessed, processed, and stored securely within the device, along with configurations such as encryption standards, access control policies, mechanisms, and network segmentation to safeguard sensitive data from unauthorized access or breaches. (Please also refer Note 1)	☐ Available and Provided ☐ Not Available ☐ Other (please see remarks)	
10	1.6	Measures available in the device to prevent software tampering.	Measures available in the device to prevent software tampering include secure boot mechanisms, code signing for trusted software updates, runtime integrity checks, access controls, and encryption of sensitive data.	☐ Available and Provided ☐ Not Available ☐ Other (please see remarks)	

11	1.6	Measures available in the device to prevent hardware tampering	Measures available in the device to prevent hardware tampering encompass physical security features like tamper-evident seals, secure hardware modules (e.g., Trusted Platform Module or TPM), intrusion detection sensors, secure boot mechanisms, and robust enclosure designs. These safeguards are designed to detect and deter unauthorized access or modifications to the device's hardware components, ensuring its integrity and reliability.	☐ Available and Provided ☐ Not Available ☐ Other (please see remarks)	
12	1.7	Documentation regarding the Intellectual Property protection technologies provided by the chip manufacturer which have been enabled. In case, no Intellectual Property protection technologies are being provided by the chip manufacturer, then a declaration stating the same.	Documentation regarding the Intellectual Property protection technologies provided by the chip manufacturer that have been enabled. If no Intellectual Property protection technologies are provided by the	☐ Available and Provided ☐ Not Available ☐ Other (please see remarks)	

			chip manufacturer, a declaration stating this is required.		
13	1.8	Technical specifications of the device regarding secure boot (should consist of keys involved and their management life cycle, signature validation process and any other secure mechanisms if implemented.)	Details on the device's secure boot technical specifications, including the management life cycle of keys used, covering their generation, storage, rotation, and destruction. The process for signature validation to verify firmware integrity and authenticity during the boot process, ensuring only trusted code is executed. Also, any other secure mechanisms implemented, such as hardware root of trust, firmware integrity checks, and rollback prevention.	☐ Available and Provided ☐ Not Available ☐ Other (please see remarks)	
14	1.9	Documentation regarding the random generators (either hardware based, or software based or both) being used in the device with their intended usage. In case, hardware based random number generators are being used, vendors shall submit the technical specifications of the device regarding random generators. In case, software based random number generators are being used, vendors shall	Documentation regarding the random generators used in the device, specifying whether they are hardware-based, software-based, or both, along with their intended usage. If hardware-based random number	☐ Available and Provided ☐ Not Available ☐ Other (please see remarks)	

		provide the libraries being used for the same.	generators are employed, vendors must submit the technical specifications of the device regarding these random generators. If software-based random number generators are utilized, vendors should provide details of the libraries used. (Please also refer Note 1)		
15	2.1	Declaration of the memory protection controls available and enabled in the device.	Documentation related to memory protection controls in the device includes details on implemented features such as hardware-based encryption, access control policies during secure boot, memory partitioning, and security techniques like randomizing memory layout and preventing unauthorized code execution. These measures collectively ensure data security by protecting against unauthorized access and	☐ Available and Provided ☐ Not Available ☐ Other (please see remarks)	

			keeping sensitive information safe from malicious attacks.		
16	2.2	Specifications and documentation related to the configurations available in the applications and firmware related to transport layer security.	Specifications and documentation regarding configurations in applications and firmware for transport layer security (TLS), including details on supported TLS versions, cipher suites, certificate management, and implemented secure communication protocols.	☐ Available and Provided ☐ Not Available ☐ Other (please see remarks)	
17	2.3, 2.7a	Document mentioning the use-cases when the device establishes server connections with the external world, with detailed information about the security measures in place while validating the digital signatures of the server connections.	A document outlining the use-cases where the device establishes server connections with the external world, detailing the security measures implemented for validating the digital signatures of these server connections. (Please also refer Note 1)	☐ Available and Provided ☐ Not Available ☐ Other (please see remarks)	
18	2.4, 2.6	Firmware binaries for code review.	The firmware binary file of the CCTV should be provided by the vendor to perform code review. (Please also refer Note 1)	☐ Available and Provided ☐ Not Available ☐ Other (please see remarks)	
19	2.4, 2.6	Internal code review reports	The reports regarding the	☐ Available and	

			internally performed code review by the vendor should be submitted. (Please also refer Note 1)	Provided ☐ Not Available ☐ Other (please see remarks)	
20	2.5	Documentation for information on software bill of materials, including third- party components and versions.	The SBOM (Software Bill of Materials) file should be provided, detailing all third-party components used in the software, along with their respective versions.	☐ Available and Provided ☐ Not Available ☐ Other (please see remarks)	
21	2.5, 2.11	Organization process and policies for the following: • Addressing and patching any identified vulnerabilities in third-party components. • Informing the customers about the security issues or vulnerabilities and providing security updates and patches for the same.	Documentations regarding the organization's approach to handling vulnerabilities in third-party components and the process for deploying patches and updates to mitigate risks and ensure the security of systems. Additionally, policies that are in place to inform customers about identified vulnerabilities and provide timely security updates and patches, ensuring they are kept informed, and their systems remain secure.	☐ Available and Provided ☐ Not Available ☐ Other (please see remarks)	

22	2.5	Configuration management system and related policies for maintaining firmware and third-party binaries, libraries and frameworks along with the patches/fixes issued to the devices.	The configuration management system to oversee the upkeep of firmware, third-party binaries, libraries, and frameworks, along with the management of patches and fixes issued to devices. This includes version control, change management processes, and automated deployment strategies to ensure timely and secure updates. Policies also include procedures for testing patches before deployment, monitoring vulnerabilities, and ensuring compatibility across all deployed devices. (Please also refer Note 1)	☐ Available and Provided ☐ Not Available ☐ Other (please see remarks)	
23	2.7b	Documentation regarding the security controls in place to hinder firmware reverse engineering.	Documentation outlining the comprehensive security controls in place to deter firmware reverse engineering attempts. These measures include encryption of critical code and data, obfuscation techniques,	☐ Available and Provided ☐ Not Available ☐ Other (please see remarks)	

			secure boot mechanisms, and access controls. Additionally, continuous monitoring and updates to security protocols ensure robust protection against unauthorized access and manipulation of firmware.		
24	2.8	Measures implemented in the device to make it resistant to time-of-check vs. time-of- use attacks.	The document outlining how the device resists time-of-check vs. time-of-use (TOCTOU) attacks should explain how it checks and uses resources or data at the same time to prevent inconsistencies. This includes using secure coding practices to minimize errors and enforcing strict access controls to prevent unauthorized changes between checks and uses.	☐ Available and Provided ☐ Not Available ☐ Other (please see remarks)	
25	2.9, 2.10	The process of achieving secure firmware upgrade which should consist of keys involved and their management life cycle, signature validation process and any other secure mechanisms if implemented. The signed and unsigned image with the version higher than the one being tested.	The document describing the process of achieving a secure firmware upgrade should outline how keys are managed throughout their lifecycle, including their generation,	☐ Available and Provided ☐ Not Available ☐ Other (please see remarks)	

			secure storage, rotation, and eventual destruction. It should also detail the validation of signatures during the upgrade process to ensure the integrity and authenticity of the firmware. Additionally, any implemented secure mechanisms, such as secure boot processes and encryption methods, should be explained to protect the firmware update from unauthorized access or modification.		
26	2.11	Modes of updates available i.e. automatic, manual or both.	-	☐ Available and Provided ☐ Not Available ☐ Other (please see remarks)	
27	2.11	Organizational process and policies regarding the issuing of updates to the devices.	-	☐ Available and Provided ☐ Not Available ☐ Other (please see remarks)	
28	3.1	The documentation regarding the process of mutual authentication as implemented in the device when wireless communications are initiated. In case, the device	-	☐ Available and Provided ☐ Not Available	

		does not support wireless communications, the vendor shall provide a declaration for the same.		☐ Other (please see remarks)	
29	3.2	The documentation regarding the security implemented in the device to prevent tampering of the data being sent through wireless mode of communication. In case, the device does not support wireless communications, the vendor shall provide a declaration for the same.	-	☐ Available and Provided ☐ Not Available ☐ Other (please see remarks)	
30	3.3	Vendor shall submit Bill of materials for critical hardware components (related to security functions like SoC).	The customer shall provide bill of materials along with the origin of the material and end-to-end supply chain. The critical hardware components shall at least cover SoC, memory, flash and TPM.	☐ Available and Provided ☐ Not Available ☐ Other (please see remarks)	
31	3.4	Supply chain risk identification, assessment, prioritization, and mitigation documents.	The customer shall provide full risk assessment report related to supply chain.	☐ Available and Provided ☐ Not Available ☐ Other (please see remarks)	
32	3.4, 4.4	Supply chain risk/business continuity planning policy documents, playbooks reflecting how to handle supply chain disruption, post-incident summary documents.	-	☐ Available and Provided ☐ Not Available ☐ Other (please see remarks)	
33	3.5	Document for Network protocols used in the device.	-	☐ Available and Provided ☐ Not Available	

				☐ Other (please see remarks)	
34	4.1	Design and architecture documents till the PCBA and SoC level.	-	☐ Available and Provided ☐ Not Available ☐ Other (please see remarks)	

Note:

1. The customer shall provide suitable arrangements for code review e.g. through remote access, visit to the laboratory.
2. Any relevant documents / information available on the customer's website may also be utilized for evaluation of compliance with the confirmation from customer.
3. The customer shall provide all necessary permissions / elevated access along with the required debugging tools for accessing the system.