सत्यमेव जयते

भारत सरकार Government of India
संचार मंत्रालय Ministry of Communications
दूरसंचार विभाग Department of Telecommunications
राष्ट्रीय संचार सुरक्षा केंद्र National Centre for Communication Security

Securing Networks

Frequently Asked Questions on Security Testing

Q1) Is source code review mandatory for obtaining security certificate?

NCCS Response: As per the NCCS OM NCCS/HQ/COMSEC/2021-22/III-Part(1) dated 17.02.2025, OEMs have now an option of submitting internal test report i.e. either they can submit source code or submit tool generated Internal test report with no paraphrasing/transposition. This will be accepted till 31.12.2025.

Q2) How can I safeguard my IPR while offering the source code for review?

NCCS Response: OEM can bring the source code on his/her own media. While performing source code analysis, the source code will not be copied to any device in the Telecom Security Testing Lab (TSTL). The code brought by OEM will be tested by connecting their media containing the source code directly to the tool and the test reports are generated in their presence. All intermediate test data will be deleted on completion of test. There will be no manual review of source code avoiding any compromise on intellectual property.

OEMs may enter into Non-Disclosure Agreement with the TSTL chosen by them. OEMs are given an option of getting the source code tested in NCCS Lab.

Q3) What if special environment is needed for security testing of network elements (NEs) or network functions (NFs)?

NCCS Response: TSTLs are designated for testing a given network elements (NEs) /network functions (NFs) only after validating the available infrastructure and capability. The infrastructure available will be general in nature and is sufficient for testing the device it is designated for. However, if the device to be tested from any OEM needs a special environment, such environment will be provided by OEM by bearing the implication of such provision.

Q4) Why should OEM give access to file systems and how to ensure access to sensitive information in DUT are protected while testing?

NCCS Response: As part of testing any DUT, TSTL needs to verify the software components installed with the SBOM supplied by the OEM. It may also be necessary to identify the device by verifying the signature of the software. OEM has a choice to provide access to file system in the manner it is deemed fit by them i.e. either they can share the credentials for accessing file systems with the TSTL for verification by the tester or they can enter the credentials by themselves and allow TSTL to take necessary details from the system.

Digitally signed by
Ashutosh Diwakar
Date: 09-04-2025
18:59:59