



भारत सरकार  
संचार मंत्रालय  
दूरसंचार विभाग  
राष्ट्रीय संचार सुरक्षा केंद्र

Government of India  
Ministry of Communications  
Department of Telecommunications  
National Centre for Communication Security



No. NCCS/SAS/6-1/2024-25/ dated at Bangalore. the 23.04.2026

**OFFICE MEMORANDUM**

Sub: Amendments to OM dated: 2nd January, 2025 regarding Expanding the scope of CSR Testing.

Ref: 1. OM No. NCCS/SAS/6-1/2024-25/ dated at Bengaluru, 2nd January, 2025  
2. OM No. NCCS/SAS/6-1/2024-25/ dated at Bangalore the 27.03.2026

In the above referred OMs, six groups of devices (Group I to VI) are listed by grouping various ITSARs/devices for designating the TSTLs against a group of ITSARs/devices for CSR testing.

In continuation of above referred OMs, the Group IV is hereby modified to include four more ITSARs viz. the revised versions (V2.0.0) of IP Router & Wi-Fi CPE and the newly published ITSARs for Network Next Generation Firewall including IDS & IPS and Layer 2 & Layer 3 LAN Switch. This revised group shall be considered by SLR division for designating the TSTLs against a group of ITSARs/devices for CSR testing. Now, the group IV contains eight ITSARs.

As four more ITSARs are added to group IV, the testing matrix pertaining to Group IV ITSARs listed as Annexure-IV under the OM dated 2<sup>nd</sup> January, 2025 stands modified accordingly. The modified Annexure-IV is enclosed herewith.

This issues with the approval of competent authority.

Director (SAS I)  
O/o Sr.DDG, NCCS,  
Bangalore

Encl: Annexure

Copy for information and necessary action to:

1. DDG (SLR)/ DDG (SC & HQ)
3. All OEMs/Dealers/Importers/applicants- through NCCS website

Copy for kind information to:

1. Member (S), DCC
2. Sr. DDG, TEC
3. DDG(SA), DoT HQ

**ANNEXURE -IV****TESTING MATRIX FOR ROUTER, CPE, CBC, PABX, Firewall and LAN switch**

S No	Clause No in Group IV ITSAR (V2.0.0)	Clause Title	Criterion to be followed for proving capability for TSTL designation for CSR Part of IP Router (V1.0.1 & V2.0.0), Wi-Fi CPE (V1.0.1 & V2.0.0), L2 and (or) L3 LAN Switch, Network Next Generation Firewall including IDS & IPS, CBC and PABX Group IV ITSAR (V2.0.0)
1	2.1.5	Remote Management Standards	Test against 'Wi-Fi CPE (V1.0.1 & V2.0.0)' only
2	2.1.6	Remote login restrictions for privileged users	Test against any one of 'IP Router (V1.0.1 & V2.0.0)', 'Network Next Generation Firewall including IDS & IPS', 'L2 and (or) L3 LAN Switch', 'CBC' and 'PABX' only
3	2.1.7	Authorization Policy	Test against any one of 'IP Router (V1.0.1 & V2.0.0)', 'Network Next Generation Network Next Generation Firewall including IDS & IPS including IDS & IPS', 'L2 and (or) L3 LAN Switch', 'CBC' and 'PABX' only
4	2.1.9	Remote Management Standards for Connected Devices, Additional Features	Test against 'WiFi CPE (V1.0.1)' only
5	2.2.2	Authentication Support - External	Test against any one of 'IP Router (V1.0.1 & V2.0.0)', 'Wi-Fi CPE (V1.0.1)', 'Network Next Generation Network Next Generation Firewall including IDS & IPS', 'L2 and (or) L3 LAN Switch', 'CBC', or 'PABX' only
6	2.2.9	Logout function	Test against any one of 'Network Next Generation Firewall including IDS & IPS', 'L2 and (or) L3 LAN Switch', 'IP Router (V2.0.0)' and 'Wi-Fi CPE (V2.0.0)' only
7	2.2.10.	Storage of Passwords in encrypted form	Test against 'Wi-Fi CPE (V1.0.1)' only
8	2.2.11	Policy regarding consecutive failed login attempts	Test against any one of the four devices 'Network Next Generation Firewall including IDS & IPS', 'L2 and (or) L3 LAN Switch', (V2.0.0 of IP Router and Wi-Fi CPE) only
9	2.2.12	Suspend accounts on non-use	Test against any one of 'IP Router (V2.0.0)', 'Network Next Generation Firewall including IDS & IPS', 'L2 and (or) L3 LAN Switch' only
10	2.3.9.	Restricted reachability of services	Test against any one of 'IP Router (V1.0.1 and V2.0.0)', 'Network Next Generation Firewall including IDS & IPS', 'L2 and (or) L3 LAN Switch', 'Wi-Fi CPE (V1.0.1)', 'CBC', or 'PABX' only

11	2.3.10	Restricting System Boot Source	Test against any one of 'IP Router (V1.0.1 and V2.0.0)', 'Network Next Generation Firewall including IDS & IPS', 'L2 and (or) L3 LAN Switch', 'Wi-Fi CPE (V2.0.0)', 'CBC', or 'PABX' only
12	2.3.11	Avoidance of Unspecified Wireless Access	Test against any one of 'IP Router (V1.0.1 and V2.0.0)', 'PABX', 'Network Next Generation Firewall including IDS & IPS', 'L2 and (or) L3 LAN Switch', or 'CBC' only
13	2.3.12	Feature / Service Activation Policy	Test against 'Wi-Fi CPE (V1.0.1 and V2.0.0)' only
14	2.4.3	No Known Vulnerabilities in System on Chip (SOC) solution	Test against 'Wi-Fi CPE (V1.0.1 and V2.0.0)' only
15	2.5.1	Audit trail storage and protection	Test against any one of 'IP Router (V1.0.1 & V2.0.0)', 'Network Next Generation Firewall including IDS & IPS', 'L2 and (or) L3 LAN Switch', 'CBC', or 'PABX' only
16	2.5.3	Secure Log Export	Test against any one of 'IP Router (V1.0.1 & V2.0.0)', 'Network Next Generation Firewall including IDS & IPS', 'L2 and (or) L3 LAN Switch', 'CBC' or 'PABX' only
17	2.5.4	Logging access to personal data	Test against 'Network Next Generation Firewall including IDS & IPS' only
18	2.5.5	Security audit log:	Test against 'Network Next Generation Firewall including IDS & IPS' only
19	2.5.6	Audit Logs	Test against 'Network Next Generation Firewall including IDS & IPS' only
20	2.5.7	Centralized log Auditing	Test against 'Network Next Generation Firewall including IDS & IPS' only
21	2.6.2	Cryptographic Based Secure Communication on Wi-Fi Access	Test against 'Wi-Fi CPE (V1.0.1)' only
22	2.6.3	Cryptographic Module Security Assurance	Test against any one of 'IP Router (V1.0.1 & V2.0.0)', 'Network Next Generation Firewall including IDS & IPS', 'L2 and (or) L3 LAN Switch', 'CBC' or 'PABX' only
23	2.6.4	Cryptographic Algorithms implementation Security Assurance	Test against any one of 'IP Router (V1.0.1 & V2.0.0)', 'Network Next Generation Firewall including IDS & IPS', 'L2 and (or) L3 LAN Switch', 'CBC', or 'PABX' only
24	2.6.5	Cryptographic Algorithm selection for Wi-Fi Access	Test against 'Wi-Fi CPE (V1.0.1)' only
25	2.6.7	Crypto-Key Protection Mechanism	Test against 'Wi-Fi CPE (V1.0.1 & V2.0.0)' only

26	2.6.9	Protection against Copy of Data	Test against any one of 'CBC', (V1.0.1 & V2.0.0 of IP Router and Wi-Fi CPE), 'Network Next Generation Firewall including IDS & IPS', LAN Switch' only
27	2.6.10.	Protection against Data Exfiltration - Overt Channel	Test against any of 'CBC', 'Network Next Generation Firewall including IDS & IPS', '(V1 & V2 of IP Router or Wi-Fi CPE)', 'L2 and (or) L3 LAN Switch' only
28	2.6.11	Protection against Data Exfiltration - Covert Channel	Test against 'CBC', 'Network Next Generation Firewall including IDS & IPS', 'IP Router (V2.0.0)', 'L2 and (or) L3 LAN Switch', or 'Wi-Fi CPE (V1.0.1 & V2.0.0)' only
29	2.7.1	Traffic Filtering - Network Level	Test against 'IP Router (V1.0.1 & V2.0.0)', 'Network Next Generation Firewall including IDS & IPS', or 'L2 and (or) L3 LAN Switch', or 'Wi-Fi CPE (V1.0.1 & V2.0.0)' only
30	2.7.2	Traffic Separation	Test against 'IP Router (V1.0.1 & V2.0.0)', 'Network Next Generation Firewall including IDS & IPS', or 'L2 and (or) L3 LAN Switch', 'CBC', 'PABX' or 'Wi-Fi CPE (V2.0.0)' only
31	2.7.3	Traffic Protection - Anti-Spoofing	Test against any of 'IP Router (V1.0.1 & V2.0.0)', 'Network Next Generation Firewall including IDS & IPS', 'L2 and (or) L3 LAN Switch', 'Wi-Fi CPE (V2.0.0)', or 'CBC' only
32	2.8.2	Filtering IP Options	Test against any one of 'IP Router (V1.0.1 & V2.0.0)', 'Wi-Fi CPE (V1.0.1 & V2.0.0)', 'Network Next Generation Firewall including IDS & IPS', 'L2 and (or) L3 LAN Switch' or 'CBC' only
33	2.8.3	Network Level and application level DDoS	Test against any one of 'IP Router (V1.0.1 & V2.0.0)', 'Network Next Generation Firewall including IDS & IPS', 'L2 and (or) L3 LAN Switch', 'Wi-Fi CPE (V2.0.0)', 'CBC', or 'PABX' only
34	2.8.4	Interfaces Robustness Requirements	Test against any one of 'IP Router (V2.0.0)', 'Network Next Generation Firewall including IDS & IPS', or 'L2 and (or) L3 LAN Switch' only
35	2.9.4	SSID Scanning	Test on 'Wi-Fi CPE (V1.0.1)' only
36	2.10.2	Growing Content Handling	Test against any one of 'CBC', 'PABX', 'IP Router (V1.0.1 & V2.0.0)', 'Network Next Generation Firewall including IDS & IPS', 'L2 and (or) L3 LAN Switch', or 'Wi-Fi CPE (V2.0.0)' only
37	2.10.6	Protection from buffer overflows	Test against any one of 'CBC', 'PABX', 'IP Router (V2.0.0)', 'Network Next Generation Firewall including IDS & IPS', 'L2 and (or) L3 LAN Switch', or 'Wi-Fi CPE(V1 & V2)' only
38	2.10.8	No automatic launch of removable media	Test against any one of 'CBC', 'PABX', 'IP Router (V1.0.1 & V2.0.0)', 'Network Next Generation Firewall including IDS & IPS', 'L2

			and (or) L3 LAN Switch', or 'Wi-Fi CPE(V2.0.0)' only
39	2.10.9	File-system Authorization privileges	Test against any one of 'CBC', 'IP Router (V2.0.0)', 'Network Next Generation Firewall including IDS & IPS', 'L2 and (or) L3 LAN Switch', 'PABX', or 'Wi-Fi CPE(V2.0.0)' only
40	2.10.10.	Restrictions on running Scripts / Batch-processes	Test against any one of 'CBC', 'IP Router (V2.0.0)', 'Network Next Generation Firewall including IDS & IPS', 'L2 and (or) L3 LAN Switch', or 'Wi-Fi CPE (V2.0.0)' only
41	2.10.11	SYN Flood Prevention	Test against any one of 'IP Router (V2.0.0)', 'Network Next Generation Firewall including IDS & IPS', 'L2 and (or) L3 LAN Switch' and 'Wi-Fi CPE (V2.0.0)' only
42	2.10.12	Restrictions on Soft-Restart	Test against any one of 'CBC', 'IP Router (V2.0.0)', 'Network Next Generation Firewall including IDS & IPS', 'L2 and (or) L3 LAN Switch', or 'Wi-Fi CPE (V2.0.0)' only
43	2.11.3	HTTP User sessions	Test against any one of 'IP Router (V1.0.1 & V2.0.0)', 'L2 and (or) L3 LAN Switch', or 'Wi-Fi CPE (V1.0.1 & V2.0.0)', 'Network Next Generation Firewall including IDS & IPS' only
44	2.11.7	No compiler, interpreter, or shell via CGI or other server- side scripting	Test against any one of 'IP Router (V1.0.1 & V2.0.0)', 'Wi-Fi CPE (V1.0.1 & V2.0.0)', 'Network Next Generation Firewall including IDS & IPS', 'CBC', or 'PABX' only
45	2.11.14	No system privileges	Test against any of 'CBC', 'Network Next Generation Firewall including IDS & IPS', 'IP Router (V1.0.1 & V2.0.0)', 'L2 and (or) L3 LAN Switch', 'PABX', 'Wi-Fi CPE (V2.0.0)' only
46	2.11.15	Access rights for web server configuration	Test against any of 'CBC', 'Network Next Generation Firewall including IDS & IPS', 'IP Router (V1.0.1 & V2.0.0)', 'L2 and (or) L3 LAN Switch', 'PABX', 'Wi-Fi CPE (V2.0.0)' only
47	2.11.16	Minimized file type mappings	Test against any of 'CBC', 'Network Next Generation Firewall including IDS & IPS', 'IP Router (V1.0.1 & V2.0.0)', 'L2 and (or) L3 LAN Switch', 'PABX', 'Wi-Fi CPE (V2.0.0)' only
48	2.11.17	Restricted file access	Test against any of 'CBC', 'Network Next Generation Firewall including IDS & IPS', 'IP Router (V1.0.1 & V2.0.0)', 'L2 and (or) L3 LAN Switch', 'PABX', 'Wi-Fi CPE (V2.0.0)' only
49	2.11.18	Execute rights exclusive for CGI/Scripting directory	Test against any of 'CBC', 'IP Router (V1.0.1 & V2.0.0)', 'L2 and (or) L3 LAN Switch', 'PABX', 'Wi-Fi CPE (V2.0.0)' only
50	2.12.3	Secure System Software Revocation	Test against any of 'CBC', 'Network Next Generation Firewall including IDS & IPS', 'IP Router (V1.0.1 & V2.0.0)', 'L2 and (or) L3 LAN Switch', 'PABX', 'Wi-Fi CPE (V2.0.0)' only

51	2.12.4	Software Integrity Check – Installation	Test against any of 'CBC', 'Network Next Generation Firewall including IDS & IPS', 'IP Router (V1.0.1 & V2.0.0)', 'L2 and (or) L3 LAN Switch', 'PABX', 'Wi-Fi CPE (V1.0.1)' only
52	2.12.6	Unused Physical Interfaces Disabling	Test against 'IP Router (V1.0.1)', 'Wi-Fi CPE (V1.0.1)' only
53	2.12.7	Unused Physical and Logical Interfaces Disabling	Test against any one of 'Wi-Fi CPE (V1.0.1)', 'CBC', 'IP Router (V2.0.0)', 'Network Next Generation Firewall including IDS & IPS', 'L2 and (or) L3 LAN Switch', or 'PABX' only
54	2.12.9	Security Algorithm Modification	Test against 'L2 and (or) L3 LAN Switch', 'IP Router (V1.0.1 & V2.0.0)', 'CBC' or 'PABX' only
55	2.12.10.	Management Interface Isolation	Test against 'PABX' only
56	2.12.11.	External Alert Generation	Test against 'PABX' only
57	2.12.12	Secure VPN connection	Test against 'PABX' only
58	2.12.13	Control Plane Traffic Protection	Test against 'Network Next Generation Firewall including IDS & IPS', or 'IP Router (V1.0.1)' only

Note: The remaining CSR clauses are same in all the eight ITSARs. They can be tested against any of the network devices viz. IP Router (V1.0.1 & V2.0.0), Wi-Fi CPE (V1.0.1 & V2.0.0), L2 and (or) L3 LAN Switch, Network Next Generation Firewall including IDS & IPS, CBC and PABX.