PHD House, 4th Floor, Ramakrishna Dalmia Wing
4/2, Siri Institutional Area, August Kranti Marg, New Delhi – 110016,
Tel# 9599665859 E-mail: ajafri@mait.com Website: http://www.mait.com

Ref.No.MAIT/PY/2738 May 18, 2023

Shri Krishna Karuturi
DDG (Security Assurance Standards (SAS) Division)
Department of Telecommunications

Subject: MAIT representation on NFV (Network Function Virtualization) ITSAR

Respected Sir,

Greetings from MAIT, India's apex Industry body empowering IT, Telecom & Electronics Hardware sectors!

This bears reference to the India NCCS NFV ITSAR draft that states cybersecurity requirements for NFV products which are sold in India. MAIT would like to humbly request upon several requirements in this proposed NFV ITSAR of the industry.

Below stated are a few concerns of the currently defined ITSAR for the industry:

Interpretation of NCCS NFV ITSAR Draft:

The draft ITSAR introduces a few potentially demanding obligations that are not aligned with Industry Standards and become more granular and prescriptive. The risk in this misalignment with the other global Industry Standards is that these controls are at such a detailed level, manufacturers will have to build customized solutions and services specifically for India in order to comply. This high level of customization could make products and services unique for India, create a trade barrier to enter the India market, complicate supply chain management, and therefore result in products that are much more expensive for India customers than the rest of the world.

Key Concerns:

1. The proposed vulnerability remediation timelines are not aligned with Industry Standards.
    a. Instead of providing specific remediation timelines (e.g., the proposed critical severity remediation timelines requiring immediate patching in 2.9.3 Vulnerability Scanning (page 37) and Chapter 3 PART II requirement 15 (page 87)), ITSAR should require remediation of vulnerabilities based on severity and potential impact. This approach to vulnerability remediation is better aligned with NIST and other global standards.

2. Risk-based evaluation and remediation of vulnerabilities is preferred instead of requiring such products to reach a state of presenting "free from vulnerabilities" specific to top 10 or top 25 named lists, as is defined in 2.3.3, Source code security assurance, and 2.3.4 Known Malware and backdoor Check. This preferred approach would incentivize manufacturers to identify and fix vulnerabilities rather than avoid discovering vulnerabilities until after the software is released.

    a. To better align this requirement with Industry Standards, please refer to NIST Special Publication 800-37 Risk Management Framework for Information Systems and Organizations

3. The accepted encryption methods are not aligned with Industry Standards.

    a. For some controls, NFV ITSAR provides a list of accepted encryption methods, for example, TLS, that is not aligned with Industry Standards and does not include relevant equivalents.
    b. Where example methods are provided in NFV ITSAR, it is recommended to use industry accepted standards.

4. NFV ITSAR does not provide a clear list indicating each clause's required submission/undertakings of assurance, in a single format (specifically, what documents need to be submitted, required content of the document, to whom the document shall be submitted, and by what timeline it is to be submitted).
    a. Required submissions/undertakings of assurance are scattered and vaguely worded in this entire document, and language around these requirements is not consistent throughout this document.

5. Several ambiguous terms (timely manner, continuously apply/monitor/perform, immediate, secure logging, etc.) need to be better defined, clarified or replaced with a definite and technically feasible term.
    a. As interpreted directly, "continuously" and "immediate" are not technically feasible.
    b. These ambiguous terms can be found in Chapter 3 Part 1 Requirement 1, Chapter 3 Part I Requirement 41) Runtime Défense and Monitoring.
    c. Chapter 3 Part I Requirement 25) System Hardening requires that the Platform must support "Secure logging". Secure Loggings needs to be defined to clarify whether it refers to secure log-in (access) or secure event logging (monitoring).

6. NFV ITSAR does not provide details of "accepted measures" and "secure practices".
    a. Some requirements (for example, Chapter 3 Part I Requirement 5 and Chapter 3 Part 3 Requirement 9) refer to accepted "measures" or secure "practices" that need to be followed without referencing any acceptable measures or practices in this document.

We are hopeful that our request on the subject matter would be addressed in a positive manner by your good office.

Warm regards,

Col. AA Jafri, Retd.
Director General

CC: Shri Prashant Pantode, Director (SAS-I), Department of Telecommunications