*Note: Update to cover more than just Kaspersky (mention Kaspersky, but don’t limit it to just Kaspersky)*

**Requirement:**

TCBs shall not certify equipment with:

*Cybersecurity and anti-virus software produced or provided by****Kaspersky Lab, Inc.****or any of its successors and assignees, including equipment with integrated Kaspersky Lab, Inc. (or any of its successors and assignees) cybersecurity or anti-virus software. (as of July 23, 2024)*

<https://www.fcc.gov/supplychain/coveredlist>

Note that given the recent examples of applicants bypassing the US agent for service of process requirements, it is clear that any actor who is intentionally including Kaspersky software on their product is not going to volunteer that information to the TCB.

*Note: Add references to KDB 986446 Covered Equipment Guidance V03 Q2a, Q8, and Q32 which discuss not just relying on statements of compliance but actually doing due diligence and documenting an explanation of why the equipment is not covered.*

**Documentation:**

Documentation of compliance is needed, to demonstrate that the presence of Kaspersky was “checked” for. Documentation provides a reviewable objective way of showing that the check was performed and describes what was checked. This also supports ongoing compliance as the marketed product can be compared to what was checked and documented.

Documentation includes both an attestation and documentation of the “check” for the Kaspersky software. The attestation can be treated as a cover letter, and the documentation of the “check” can conceivably be treated as either a test report, if appropriate, or as operational description (therefore allowing confidentiality).

**Evaluation/Review/Decision under 17065 and TCB Roles and Responsibilities:**

As required by both ISO/IEC 17065 and KDB 641163 TCB Roles and Responsibilities, the persons performing the “evaluation” cannot be the same persons that are performing the “review and decision on certification”. Therefore the TCB “reviewer/decision maker” cannot generate the Kaspersky compliance documentation, rather, someone on the “evaluation” side shall provide reviewable documentation to the TCB “reviewer/decision maker”.

**Attestations:**

Use of an attestation declaring explicit compliance with the Kaspersky software covered list requirements is a best practice, but is not sufficient as the sole basis for compliance. Attestations should not include statements about future compliance as certification is a check for compliance at the time of certification and it is the grantee’s responsibility to adhere to the certification requirements and place product on the market that conforms to what was documented in the certification filing. No expiration dates are allowed by the FCC on cover letters.

Potential wordings for attestation:

TCB1: The software to be loaded prior to marketing of the equipment identified above ☐ is / ☐ is not “covered” software manufactured by any entity including predecessors, successors, parents, subsidiaries, or affiliates or any entity which has rebranded or relabeled the software produced by the entity(ies) identified on the “Covered List.”

TCB2: Applicant certifies that the equipment for which authorization is sought does not contain cybersecurity and anti-virus software produced or provided by Kaspersky Lab, Inc. or any of its successors and assignees, including equipment with integrated Kaspersky Lab, Inc. (or any of its successors and assignees) cybersecurity or anti-virus software.

TCB3: Applicant further certifies that no Cybersecurity or anti-virus software produced or provided by **Kaspersky Lab, Inc.** or any of its successors and assignees, including equipment with integrated Kaspersky Lab, Inc. (or any of its successors and assignees) cybersecurity or anti-virus software is installed in the equipment being certified.

**Inherent Compliance:**

TCB1: Require documentation of chipsets, memory, storage capacity, and operating system, as well as ability to connect to the internet or external devices. Approach vectors take two forms, the primary form is presence of Kaspersky software on the product which runs on the product. Therefore if the product is not capable of running the Kaspersky software due to limitations on chipset, memory, storage capacity, and operating system, the device might be deemed inherently compliant. Documentation of chipsets is verifiable since the TCB also obtains internal photos and schematics. The second approach vector is for a product that does not have the capability to run Kaspersky software, but which was the storage capacity to have Kaspersky software embedded on the device, and a means to deliver the Kaspersky software maliciously to connected devices.

TCB2: Questionnaire for review – will be posted on the website as an example – covers inherent compliance

How to handle C2PCs for modules and host devices – for example if host is clearly manufactured by an entity named on the covered list, then an inquiry to the FCC is needed, just like for covered list “red flags”. Also, potential integration instructions requirement for host integrator not to include Kaspersky (not fully supported on the call). Could be a best practice for manufacturers (not a requirement for TCB certification).

**Non-Inherent Compliance:**

If a device is not inherently compliant based on hardware limitations or software controls, it is necessary to check and document compliance in some manner – it is not possible to simply say it is too hard to do so therefore no check is made.

Possible ways to check:

Software scan for Kaspersky software images on product

review of file system, running processes

review of software bill of materials? Might not be acceptable because it is very similar to an attestation

Potential concerns:

Final software build is unlikely to be available at time of certification, we really cannot delay certification until the final software build is available

Counterpoint to potential concerns – by documenting a check as described above, the deployed product at time of certification must conform to the documented certification, i.e., Kaspersky was not present at the time of the check therefore is not allowed to be present when the product is placed on the market. This does not preclude the installation of additional compliant (non-Kaspersky) software.

No lab accreditation/recognition requirement exists for such a check, therefore TCBs could conceivably accept documentation/test reports from any source, however is it acceptable for the manufacturer to be the source, or shall it be a third party? If so, which third parties are acceptable?