Covered List Software Best Practices

Introduction and background

A Telecommunications Certification Body (TCB) designated by the Federal Communications Commission (FCC) represents the U.S. government when it evaluates and approves equipment subject to certification under FCC Rules and Regulations.

On November 25, 2022, the FCC released FCC 22-84, a Report and Order, Order, and Further Notice of Proposed Rulemaking on "Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program." [1] In the Report and Order portion of FCC 22-84, the Commission adopted new FCC requirements to protect the nation's networks and supply chains from certain equipment ("covered" equipment) that poses an unacceptable risk to national security or the safety of U.S. persons. On July 23, 2024, the FCC added the following new item to the covered list:

*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.*

Additional items may be added to the covered list at a later date.

Given the addition of "cybersecurity and anti-virus software" to the covered list, it became necessary for TCBs to evaluate compliance with this requirement prior to certifying equipment. While the FCC does provide a knowledge database (KDB) publication that discusses the covered list, KDB 986446 "Covered Equipment Guidance" [2], the guidance contained therein does not provide methods for evaluating compliance with the requirement to prohibit certification of devices including "cybersecurity and anti-virus software" produced or provided by the entity named on the covered list (covered list software). After discussion with the FCC, the TCB Council has been encouraged to develop best practices for evaluating compliance with this requirement.

While the initial entry to the covered list is specifically related to Kaspersky Lab, Inc. and any of its successors or assignees, future covered list software entries might be added, and this document is intended to serve as a best practice for any covered list software evaluations.

The framework for evaluation involves not just relying on statements of compliance such as an attestation, but also performing "appropriate and sufficient due diligence" to establish a basis for compliance, and then documenting how the equipment is not "covered" under the software items on the covered list. FCC KDB 986446 "Covered Equipment Guidance" [2] Q2a, Q8, and Q32 discuss these concepts.

TCB Evaluation/Review/Decision process requirements

As required by both ISO/IEC 17065 [3] and KDB 641163 “TCB Roles and Responsibilities” [4], 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 covered list software compliance documentation. The reviewable documentation supporting compliance with the covered list shall originate from the “evaluation” portion of the certification process and shall be provided to the TCB “reviewer/decision maker” for review and acceptance. Further information on the terms “evaluation”, “reviewer”, and “decision maker” can be found in the cited documents (see [3], [4]).

Certification documentation

Documentation provides a reviewable and objective mechanism for establishing compliance and demonstrating that the TCB applied due diligence. The supplied documentation can be compared by the TCB reviewer/decision maker for consistency with other exhibits such as the schematics, block diagram, internal photos, and operational description. It also establishes a record of how compliance was determined, which can be compared to the marketed device at a later date and which can be included in the certification documentation.

The documentation should include an attestation of compliance with the covered list software requirements and also documentation of how compliance was established. It is recommended that both documents are uploaded to the FCC website as part of the certification documentation package. The attestation can be treated as a cover letter exhibit, and the documentation of the basis for compliance can be treated as an operational description exhibit which can be held confidential.

Attestations

Use of an attestation declaring explicit compliance with the covered list software requirements is a best practice, but the FCC has stated that it 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 the device is certified and it is the grantee’s responsibility to adhere to the certification requirements and place devices on the market that conform to what was documented in the certification filing. No expiration dates are allowed by the FCC on such attestation statements.

Some examples of potential language that could be used in an attestation of compliance with the covered list software requirements are given below. Note that at the time of publication of this best practice document, the only software related entry on the covered list was Kaspersky Lab, Inc., therefore some of the examples mention it explicitly. In the future, if more entries are added to the covered list that relate to software, more general attestation language might be appropriate.

Example #1:

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."

Example #2:

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.

Example #3:

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.*

Documentation related to establishing inherent compliance

It is possible that a device subject to certification is not capable of storing or running covered list software, therefore documentation of why the device is not capable of storing or running the software can be used as a basis for establishing compliance. This is the concept of "inherent compliance".

There are two ways that covered list software might operate. The first is that the covered list software can run on the device being certified. The second is that the covered list software can be stored on the device being certified, and installed or run at some time in the future on a connected device. Therefore establishment of inherent compliance relates to documenting that the device does not have the capability to run or to store the covered list software, and whether the device is capable of connecting to the internet or another device.

Establishing whether a device can run, install or deliver covered list software can be based on many factors, including but not limited to: the chipset(s), memory, storage capacity, and operating system, as well as whether the device can connect to the internet or another device. Therefore a document which details this information can be used as a certification exhibit. While it is generally expected that the document is supplied by the grantee, it can also originate from the test lab or TCB evaluation personnel. Additional considerations related to inherent compliance that can be documented include software authentication protocols, protection against modification, encryption methods, and controls on how software updates will be obtained, downloaded, validated, and installed. See KDB 594280 [5] for examples of content that could be included in an inherent compliance document.

Documentation for when a device is not inherently compliant

If a device is not inherently compliant based on hardware limitations or software controls, as described above, it is necessary to perform "appropriate and sufficient due diligence" to establish a basis for compliance, which can be documented in the filing.

When it is possible for a device to run, store, or deliver covered list software, there are several possible ways to check for compliance with the covered list. These include, but are not limited to such activities as scanning for the covered list software images on a device, reviewing the device file system and running processes, or reviewing a software bill of materials. Due to the nature of the certification process, some of these methods might not be practicable. For example, many devices are certified well before final software is available, so it would not be possible to scan for software images or evaluate the file system and processes without introducing undue barriers to market entry. Another complicating factor is that there is no laboratory accreditation or recognition requirement for a software scan or other type of software evaluation, so it is difficult to determine which entities are approved to perform a software evaluation. Further, if a grantee is intentionally installing covered list software, they are not likely to provide a test sample that includes it for the software check.

For the reasons elucidated above, the recommendation of the TCB community is that for devices which are not inherently compliant, covered list software compliance can be based on a Software Bill of Materials (SBoM). Since devices placed on the market must conform to what was certified, use of an SBoM provides a way to determine compliance that can be compared to devices placed on the market, but does not preclude the installation of additional software that is not on the covered list. An SBoM is also more practical for the grantee to generate than providing a device with a final software environment for evaluation and testing. The SBoM content can be limited to the scope of covered list software (e.g. antivirus and cybersecurity software).

Successors and assignees

There is no definitive or official list approved by the FCC of the successors or assignees of entities named on the covered list. In the absence of such an official list, there are some unofficial resources that might help identify successors and assignees to entities named on the covered list, such as the Bureau of Industry and Security (BIS) entity list. Other resources may be available as well.

BIS entity list landing page: https://www.bis.gov/entity-list

Direct link to the BIS entity list in 15CFR: https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-744/appendix-Supplement%20No.%204%20to%20Part%20744

Modules and host devices

When certifying a radio module, a TCB is not certifying the potential host devices for the module, which are not usually known at the time of certification. In some cases the host is known at the time of certification, such as host specific limited modular approvals, however only the module is the subject of certification. Therefore, documentation used to establish compliance of a radio module with the covered list software requirements does not need to include compliance of the host device(s), regardless of whether it is a host specific limited modular approval or not. As described in KDB 996369 [6], host product manufacturers are responsible for all additional equipment authorization and testing for technical requirements not covered by the module grant. However, when a TCB has observed evidence that a host product potentially does not comply with the covered list, it is recommended that the TCB submit a KDB inquiry to the FCC to determine the next steps.

Grantees may elect to provide module integration instructions that address compliance with the covered list requirements, however such instructions are not a certification requirement.

Bibliography:

The following bibliographical references were used in the drafting of this guidance document. The versions used were the most current at the time of publication of this document. Entities applying this best practice should consider the implications of the latest editions of any document listed below.

[1] FCC 22-84 Report and Order, Order, and Further Notice of Proposed Rulemaking on “Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program.”

[2] KDB 986446 D01 V03 “Covered Equipment Guidance”

[3] ISO/IEC 17065:2012 “Conformity assessment – Requirements for bodies certifying products, processes and services”

[4] KDB 641163 D01 V04r02 “TCB Roles and Responsibilities”

[5] KDB 594280 D02 V01r03 “U-NII Device Security”

[6] KDB 996369 D04 V02 “Modular Transmitter Integration Guide”