



One Distribution Center Circle, Suite 1  
Littleton, MA 01460  
Tel: +1 978 486 8880  
Email: [certification@bureauveritas.com](mailto:certification@bureauveritas.com)  
Website: <https://www.cps.bureauveritas.com/>

# Software Due Diligence Questionnaire

| Reason for Amendment                                                                                                                                                                                                                                         | Revision History |     | Approved Date |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|-----|---------------|
|                                                                                                                                                                                                                                                              | From             | To  |               |
| Initial Release                                                                                                                                                                                                                                              | Initial          | 1.0 | Jan-03-2025   |
| Updated header and footer information.<br>Replaced specific references to Kaspersky with generic FCC Covered List Entity.<br>Added place for justification of inherently compliant devices.<br>Added question related to software installed on host devices. | 1.0              | 2.0 | Jan-08-2025   |
|                                                                                                                                                                                                                                                              |                  |     |               |
|                                                                                                                                                                                                                                                              |                  |     |               |
|                                                                                                                                                                                                                                                              |                  |     |               |
|                                                                                                                                                                                                                                                              |                  |     |               |

Dear Applicants,

I am writing to inform you of an important update regarding the FCC's equipment authorization process. On July 23, 2024, the Federal Communications Commission (FCC) added Kaspersky Lab to the Covered List, designating them, and other related entities, as entities that pose an unacceptable risk to the national security of the United States.

In response to this development, the FCC has issued Public Notice DA-24-886A1 on September 3, 2024, providing guidance on the FCC's new requirements for all Applicants seeking equipment authorization.

Specifically, as outlined in Question 2a of KDB 946446 D01, Bureau Veritas is now requiring all Applicants to complete a Software Due Diligence Questionnaire as part of our internal due diligence process. This questionnaire is designed to ensure that the equipment being certified does not contain any software or software components from entities that have been added to the Covered List, such as Kaspersky Lab.

It is important to note that this questionnaire will not be included in the submission package to the FCC, but will be retained in Bureau Veritas' records associated with your FCC Application. By implementing this new requirement, Bureau Veritas aims to strengthen the security and integrity of the equipment authorization process, protecting the national security interests of the United States.

We encourage all Applicants to carefully review the Public Notice and complete the Software Due Diligence Questionnaire as part of your application process. If you have any questions or require further assistance, please do not hesitate to contact us.

Sincerely,  
Ryan McGann  
TCB Program Manager  
Bureau Veritas Consumer Products Services, Inc.

## Software Due Diligence Questionnaire

in respect of the equipment identified below with regards to software capabilities for

**FCC ID: 2BSNSNCLS**

| <b>Declaration</b>                  |                                                                                                                                                                                              |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/>            | Product hardware <u>does not</u> have the capability to install or operate software by any manufacturer, end-user, or third party. (Provide justification below. Questionnaire not required) |
| <input type="checkbox"/>            | Product hardware has the capability to install software by the equipment manufacturer only at the time of manufacturing and not updatable at any later time.                                 |
| <input checked="" type="checkbox"/> | Product hardware has the capability to install or operate software by:<br>(select all that apply)                                                                                            |
| <input checked="" type="checkbox"/> | the equipment manufacturer                                                                                                                                                                   |
| <input checked="" type="checkbox"/> | Another entity in the supply chain                                                                                                                                                           |
| <input checked="" type="checkbox"/> | End-users or other third parties                                                                                                                                                             |

| <b>Questionnaire</b>                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Please provide a detailed description of the cybersecurity and anti-virus software components integrated into the equipment for which you are seeking authorization. Specifically, address whether any of these components are produced or provided by an entity on the FCC's Covered List, or any of its subsidiaries and affiliates. |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| A:                                                                                                                                                                                                                                                                                                                                     | <p>The Firmware installed at the manufacturer includes:</p> <ol style="list-style-type: none"> <li>1. An immutable bootloader from Nordic Semiconductor ASA</li> <li>2. A version of MCUBoot from Nordic Semiconductor ASA</li> <li>3. The main firmware</li> </ol> <p>The immutable bootloader checks a digital signature of MCUBoot and will only run that firmware if it is signed using a private key.</p> <p>The MCUBoot checks the digital signature of the main firmware and will only flash the main firmware if it is signed using a private key.</p> <p>While running the firmware is protected using Trusted Firmware-M (TF-M), which implements the Secure Processing Environment (SPE) for the Arm microcontroller. This implementation also comes from Nordic Semiconductor ASA.</p> <p>Teledyne maintains the code signing keys on their private network with limited access control.</p> <p>None of these components comes from an entity on the FCC's Covered List or any of their subsidiaries and affiliates.</p> |
| Explain the measures you have taken to ensure that the equipment does not include any FCC Covered List cybersecurity or anti-virus software.                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| A:                                                                                                                                                                                                                                                                                                                                     | Teledyne has reviewed the FCC Covered List and compared that with the development tools and code to make sure that none of the components are sourced from any of the entities or any of their known subsidiaries or affiliates.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Describe in detail the authentication protocols that are in place to ensure that the source of the software is valid. Describe in detail how the software is protected against modification and any encryption methods used to support the use of legitimate software.                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

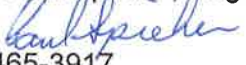


|                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A:                                                                                                                                                                                                                                                | Source code is managed using a private Bitbucket repository. Only authorized developers have access. The third-party SDK and components are only pulled once from their official repos. There is no automatic updating in the development process. The compiled code is signed using a private key generated and stored by Teledyne. |
| Describe the process you have in place to continuously monitor for and remove any FCC Covered List cybersecurity or anti-virus software that may be inadvertently integrated into the equipment during the manufacturing or supply chain process. |                                                                                                                                                                                                                                                                                                                                      |
| A:                                                                                                                                                                                                                                                | There is no anti-virus integration in the product. Cybersecurity is handled using digitally signed binaries. There is no automatic inclusion of components in the binary build system. Components used are checked against the FCC Covered List before being implemented. The List is also checked before release of the binary.     |
| Describe how any software updates will be obtained, downloaded, validated and installed. For software that is accessed through manufacturer's website or device's management system, describe the different levels of security as appropriate.    |                                                                                                                                                                                                                                                                                                                                      |
| A:                                                                                                                                                                                                                                                | Device firmware updates will be signed by Teledyne, the manufacturer and only that signed firmware is allowed to update the device. Software updates to the firmware build system are protected by Teledyne I.T.'s controls including antivirus from Palo Alto Networks.                                                             |

#### Questionnaire

|                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| For radio equipment that requires software installation onto third party or host equipment, what controls are in place to ensure installed software is compliant with the U.S. requirements?                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| A:                                                                                                                                                                                                                                       | The equipment does not <i>require</i> software installation. There is software available that can communicate with the device and this software will be compliant with Teledyne I.T. standards. Controls include 2-factor authentication to both development workstations as well as code repositories. A limited whitelist of approved software development tools. A blacklist of sites with known vulnerabilities or known to distribute malicious code. |
| Explain if any third parties have the capability to operate a U.S.-sold device on any other regulatory domain, or in any manner that may allow the device to operate in violation of the device's authorization if activated in the U.S. |                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| A:                                                                                                                                                                                                                                       | There are no restrictions on where the device can be used. There is no way to operate the device in violation of the device's authorization. There is no device "activation" other than turning it on.                                                                                                                                                                                                                                                     |
| Is the country code factory set? Can it be changed in the UI? If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.?                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| A:                                                                                                                                                                                                                                       | The device has no notion of country code. The device is designed to operate within the constraints of the U.S. Authorization. Other country constraints have been considered, but they are not in opposition to the U.S. rules.                                                                                                                                                                                                                            |
| What are the default parameters when the device is restarted?                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| A:                                                                                                                                                                                                                                       | The device starts up with Bluetooth advertising and if configured to do so, with the radar sensing level. Startup parameters such as duty cycle and information to be collected can be configured by the user as the default. None of these settings will allow the device to violate the constraints of the U.S. Authorization.                                                                                                                           |

Name / Title: Paul Spieker, Regulatory Compliance Manager

Signature: 

Phone: 402-465-3917

Email: paul.spieker@teledyne.com

Date: December 22, 2025