# FDA Use Case Concept for SCITT

On March 30, 2023 the Food and Drug Administration (FDA) issued updated guidance “Guidance for Industry and Food and Drug Administration Staff” containing requirements for cybersecurity information that Medical Device Manufacturers (MDM) will be expected to submit with applications, described in “Cybersecurity in Medical Devices: Refuse to Accept Policy for Cyber Devices and Related Systems Under Section 524B of the FD&C Act”, “Ensuring Cybersecurity of Devices.” These rules went into effect on March 30, 2023; however, enforcement has been delayed until October 1, 2023, at which time FDA may reject a medical device application that fails to provide the required cybersecurity information.

MDMs are expected to provide the FDA with the following cybersecurity information with an application filed under section 510(k), 513, 515(c), 515(f), or 520(m) for a device that meets the definition of a cyber device. The term ‘cyber device’ means a device that—

(1) includes software validated, installed, or authorized by the sponsor as a device or in a device;

(2) has the ability to connect to the internet; and

(3) contains any such technological characteristics validated, installed, or authorized by the sponsor that could be vulnerable to cybersecurity threats.

## Cybersecurity Information Requirements in Section 524B of the FD&C Act

(1) submit to the Secretary **a plan** to monitor, identify, and address, as appropriate, in a reasonable time, postmarket cybersecurity vulnerabilities and exploits, including coordinated vulnerability disclosure and related procedures;

(2) **design, develop, and maintain processes and procedures to provide a reasonable assurance that the device and related systems are cybersecure, and make available postmarket updates and patches to the device and related systems to address**—

(A) on a reasonably justified regular cycle, known unacceptable vulnerabilities; and

(B) as soon as possible out of cycle, critical vulnerabilities that could cause uncontrolled risks;

(3) **provide to the Secretary a software bill of materials**, including commercial, open-source, and off-the-shelf software components; and

(4) comply with such other requirements as the Secretary may require through regulation to demonstrate reasonable assurance that the device and related systems are cybersecure.

It’s conceivable that documentation describing 3 distinct topics may be provided to the FDA, by a MDM, in order to address these requirements:

1. A plan to monitor, identify, and address post-market cybersecurity vulnerabilities and exploits including coordinated vulnerability disclosure and related procedures
2. Documented processes and procedures to provide reasonable assurance that the device and related systems are cybersecure and make available post-market updates and patches available to end users of the device
3. A software bill of materials (SBOM)

Submitters are expected to [submit acceptance checklists with their submissions that identify the location of supporting information for each Refuse to Accept (RTA) element](https://www.fda.gov/media/83888/download). This includes the new cybersecurity artifacts required under section 524B, identified above.

This document describes one possible use case in which a Supply Chain Integrity, Transparency and Trust (SCITT) Registry, operated by a SCITT Transparency Service provider implements a “registration policy” to maintain trusted statements identifying the location of supporting information required by 524B. This use case will be referred to as the “SCITT FDA Cybersecurity Use Case”, contained in a single [open-source “Vendor Response File” (VRF)](https://energycentral.com/c/pip/advice-software-vendors-prepare-omb-m-22-18-requirements) supplied to a Transparency Service in the payload of a “trusted statement”.

## SCITT FDA Cybersecurity Use Case Description

Purpose: Provide FDA personnel with the location information for section 524 RTA elements provided by an MDM, submitting an application to the FDA. Locations for the following RTA elements will be provided in a single, open-source [“Vendor Response File” (VRF)](https://energycentral.com/c/pip/advice-software-vendors-prepare-omb-m-22-18-requirements) that will be made available to the FDA via a SCITT Transparency Service, using a REST API:

1. The location of a document describing cybersecurity practices currently in use, or planned to be in use, by the MDM submitting an application to FDA (identified by data element CyberSecPolicyURL in the VRF)
2. The location of a document describing processes and procedures to provide reasonable assurance that the device and related systems are cybersecure and make available post-market updates and patches available to end users of the device (identified by data elements SDLCPolicyURL and KnownVulnInfoURL in the VRF)
3. The location of an SBOM document for the product (identified by data element SBOM/URL in the VRF)

[An example open-source Vendor Response File (VRF) is available online](https://raw.githubusercontent.com/rjb4standards/REA-Products/master/jsonvrf.json).

<https://raw.githubusercontent.com/rjb4standards/REA-Products/master/jsonvrf.json>

This use case includes the following activities:

1. Registration of a Vendor Response File (VRF) within a SCITT Transparency Service with an appropriate “Registration Policy” specifying that FDA Vendor Response Files for Section 524B are stored in the registry.
2. The MDM is responsible for filling in the contents of the VRF and submitting the completed VRF to the SCITT Transparency Service
3. The SCITT Transparency Service will issue a receipt to the MDM upon completing the VRF registration, that also includes an URL to access the VRF within the registry
4. The MDM provides the FDA with a link to the registered VRF.
5. The FDA retrieves the VRF from the SCITT Transparency Service using the supplied link
6. After retrieving the VRF, the FDA can now use the VRF data to lookup the location of each 524B artifact listed in the CyberSecPolicyURL, SDLCPolicyURL, KnownVulnInfoURL and SBOM/URL data elements and download each file.
7. The FDA performs its processing steps to validate and process the downloaded data files as part of the application process