# FDA Cybersecurity Label

Use Case

Demonstrates Registration of a Trusted Location (URL)

# FDA Final Cybersecurity Guidelines

- Medical Device Manufacturers MUST satisfy FDA Final Guidelines described here: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions
- FDA requires several artifacts including SBOM and Cybersecurity Label
- These artifacts can be easily shared via a SCITT Trust Registry (Transparency Service)

# FDA Cybersecurity Label Requirements

## VI. Cybersecurity Transparency

Cybersecurity transparency is critical to ensure safe and effective use and integration of devices and systems.[48] This transparency can be conveyed through both device labeling and the establishment of manufacturer vulnerability management plans. However, different types of users (e.g., manufacturers, servicers, patients) will have different abilities to take on a mitigation role, and the need for actions to ensure continued cybersecurity should be appropriate for the type of user. Manufacturers of cyber devices should consider the recommendations in this section as they "design, develop, and maintain processes and procedures to provide a reasonable assurance that the device and related systems are cybersecure . . ." (section 524B(b)(2) of the FD&C Act; see Section VII.C.2).

### A. Labeling Recommendations for Devices with Cybersecurity Risks

# Continued

For devices with cybersecurity risks, informing users of relevant security information may be an effective way to comply with labeling requirements relating to such risks. FDA also believes that informing users of security information through labeling may be an important part of design and development activities to help mitigate cybersecurity risks and help ensure the continued safety and effectiveness of the device. Therefore, when drafting labeling for inclusion in a premarket submission, a manufacturer should consider all applicable labeling requirements and how informing users through labeling may be an effective way to manage cybersecurity risks and/or to ensure the safe and effective use of the device. Any risks transferred to the user should be detailed and considered for inclusion as tasks during usability testing (e.g., human factors testing)[49] to ensure that the type of user has the capability to take appropriate actions to manage those risks.

The recommendations below aim to communicate to users the relevant device security information that may enable their own ongoing security posture, thereby helping ensure a device remains safe and effective throughout its lifecycle. The depth of detail, the exact location in the

# Registering a Trusted Location (URL)

- Using FDA Cybersecurity Label as use case
- Can be used to verify that URLs are registered as trustworthy
- Mapping of APIURL -> SCITT Registered Location
- Most useful to check for “trusted API’s” before use (avoids typosquatting)
  - If ResolveSignedStatementChecker(APIURL)
    - Execute APIURL

# MDM Registration of Cybersecurity Label URL