VELENTIUM MEDICAL

NAVIGATING CYBERSECURITY DURING FDA ESTAR SUBMISSIONS

SEC-GUIDE-00

Provided by:
VELENTIUM MEDICAL
CYBERSECURITY SERVICES

1.0 Purpose

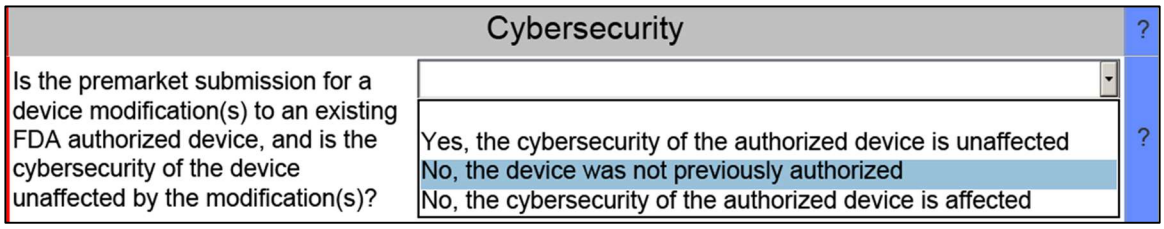
With the introduction of the FDA's Electronic Submission Template (eSTAR), the FDA has established a standardized, structured approach to medical device submissions. This process requires manufacturers to submit well-organized, detailed artifacts that demonstrate the security and risk management measures implemented in their devices. This guide will walk through eSTAR cybersecurity requirements for premarket application (PMA), de novo, and premarket notification 510(k) submissions, as well as device modifications to previously authorized devices.

2.0 Getting Started with eSTAR

eSTAR can be downloaded from the following website: https://www.fda.gov/medical-devices/how-study-and-market-your-device/estar-program. Once downloaded and opened, and a submission type is selected, many non-security prompts must be responded to. The first prompt in eSTAR for cybersecurity addresses whether the sponsored device being submitted has been authorized before or not. Device modifications, such as a letter to file, are now submitted via eSTAR in addition to new submissions. The submission requirements for modifications depend on whether the changes made to the system impact security or not.

ACTION: Select the most appropriate answer from the dropdown menu as shown in the below figure.

- **For new 510(k), de novo, and PMA submissions**, select "No, the device was not previously authorized", and proceed to Section 3.0 of this document for guidance on completing the cybersecurity portion of eSTAR.
- **For previously authorized devices with changes impacting security,** select "No, the cybersecurity of the authorized device is affected", and proceed to Section 3.0 of this document for guidance on completing the cybersecurity portion of eSTAR.
    - Per the FDA Premarket Guidance and eSTAR: "Changes that may impact cybersecurity and may require premarket submission could include changes to authentication or encryption algorithms, new connectivity features, or changing software update process/mechanisms."
- **For previously authorized devices with changes not impacting security**, select "Yes, the cybersecurity of the authorized device is unaffected", and proceed to Section 4.0 of this document for guidance on completing the cybersecurity portion of eSTAR.
    - Per the FDA Premarket Guidance and eSTAR: "Changes unlikely to impact cybersecurity could include changes in materials, sterilization method changes, or a change to an algorithm without change to architecture/software structure/connectivity."



3.0 eSTAR Cybersecurity Requirements for New Submissions and Device Modifications with Changes Impacting Security

This section details the prompts within the Cybersecurity Section of the FDA eSTAR Submission System version 5.6. Table 1 lists the artifacts required to be attached to an eSTAR submission, along with references to sections within the FDA's Premarket Cybersecurity Guidance that cover these artifacts and related processes.

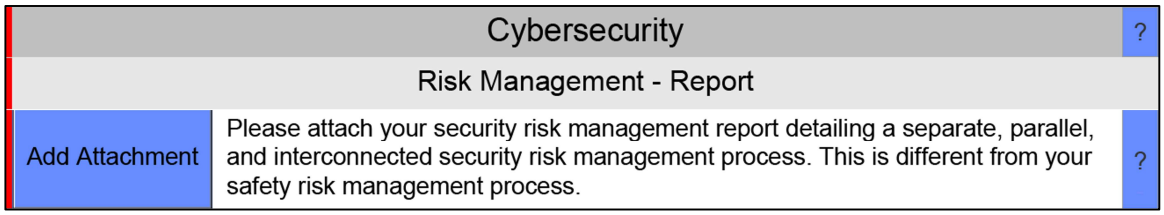
Required Artifacts for eSTAR Submission	FDA Premarket Cybersecurity Guidance Sections	Section of this Document
Security Risk Management Plan	VI.B	3.10
Threat Modeling and Security Architecture Report	V.A.1, V.B.2	3.2
Cybersecurity Risk Assessment Report	V.A.2, V.A.3	3.3
Software Bill of Materials (SBOM)	V.A.4, VI.A	3.4
SBOM Support Report	V.A.4.a	3.4
Software Component Risk Management Report	V.A.4	3.4
Unresolved Anomalies Risk Management Report	V.A.5	3.5
Cybersecurity Metrics Report	V.A.6	3.6
Cybersecurity Control Report	V.B.1	3.7
Cybersecurity Testing Report	V.C	3.8
Cybersecurity Labeling Report	VI.A	3.9
Security Risk Management Report	V.A, VI.B	3.1

Table 1. Required artifacts for FDA eSTAR 510(k), de novo, and PMA submissions, and for device modifications with changes impacting security

3.1 Security Risk Management Report

The Security Risk Management Report summarizes all security activities performed during the premarket development process and includes cybersecurity traceability, justifications for any residual risks, and deviations from the Security Risk Management Plan.

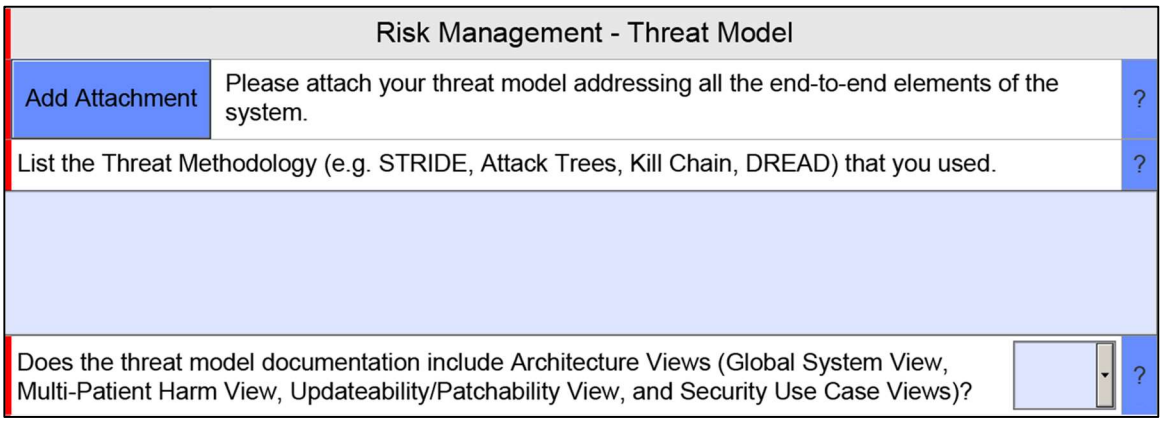
ACTION: Attach the Security Risk Management Report by clicking on "Add Attachment" as shown below.



3.2 Threat Modeling and Security Architecture Report

A Threat Model captures cybersecurity vulnerabilities and the mitigations necessary to control said vulnerabilities. Security Architecture Views similarly summarize and communicate the security mitigations and controls with diagrams and textual descriptions. At Velentium Medical, we include several threat models and architecture views in the Threat Modeling and Security Architecture Report.

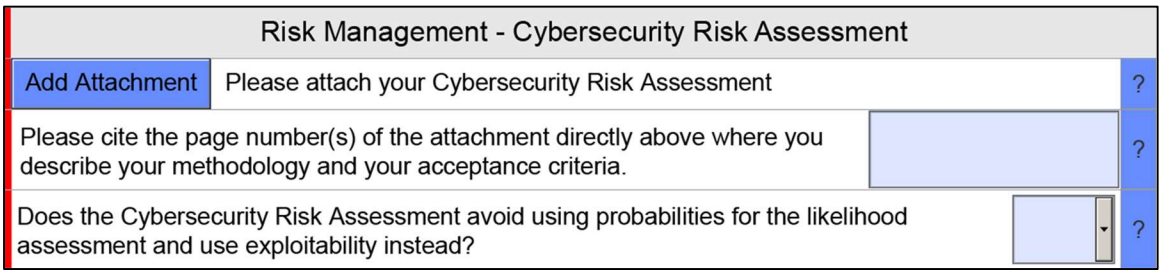
ACTION: Attach the Threat Modeling and Security Architecture Report and describe the methods used for threat modeling in the input field, as shown below. Additionally, indicate whether the security architecture views are included in the threat modeling documentation. If the views are not included in the threat model documentation, an additional section covering the views is contained within the eSTAR dynamic PDF (not shown in this document).



3.3 Cybersecurity Risk Assessment Report

A Cybersecurity Risk Assessment must be performed on the vulnerabilities (or risks) identified during threat modeling. This assessment includes a pre-mitigation and post-mitigation evaluation based upon exploitability and severity.

ACTION: Attach the Cybersecurity Risk Assessment Report as shown below. Reference the report sections and page numbers where the methods and acceptance criteria are described. Ensure you answer “Yes” to indicate that you have NOT used likelihood for the risk assessment methods.



3.4 Software Bill of Materials (SBOM) and Related Reports

SBOMs contain lists of third-party software components included in the first-party software within the medical device system. Additional reports must also be generated that describe support information for the listed third-party components and an assessment of vulnerabilities affecting the same third-party components.

ACTION: Attach the SBOM file(s) as shown below. These should be in either JSON or XML data structure formats using either the CycloneDX or SPDX specification. Attach the SBOM Support Report for the second attachment option and attach the Software Component Risk Management Report for the third attachment option as shown below. In the input field, describe the operating systems implemented in the system, if applicable.

Risk Management - Software Bill of Materials (SBOM) and Related Information		
Add Attachment	Please attach your Software Bill of Materials (SBOM).	?
Add Attachment	Please attach a document to provide the software level of support and end-of-support date for each software component (e.g. OTS software) identified in the SBOM. For any component where this information was not available, provide a justification.	?
List the supported operating system(s) and associated version(s) your device(s)/system uses. Be aware that if you list any operating systems that are no longer supported (e.g. Windows 7, Mac OS 9) or nearing end of support, this will generally be considered an inaccurate response. Type "N/A" if your device(s) does not use an operating system.		?
Add Attachment	Please attach a safety and security assessment of cybersecurity vulnerabilities in the component software used by the device for all software components in the SBOM and a description of any controls that address the vulnerability.	?

3.5 Unresolved Anomalies Risk Management Report

Following Verification and Validation, any unresolved software bugs in the final release of the system must be assessed for security.

ACTION: Attach the Unresolved Anomalies Risk Management Report as shown below.

Assessment of Unresolved Anomalies		
Add Attachment	Please attach an assessment of any unresolved anomalies for cybersecurity impact. If none exist, attach a document stating that no unresolved anomalies exist.	?

3.6 Cybersecurity Metrics Report

Cybersecurity metrics must be gathered during update and patching events in fielded products, and these metrics must be documented in a Cybersecurity Metrics Report. This report pertains to all products and systems developed by the manufacturer, including devices already on the market. The report must include past metric information if available and applicable, and it must define the metrics that will be gathered for the product being submitted in the future.

ACTION: Attach the Cybersecurity Metrics Report as shown below.

Cybersecurity Metrics		
Add Attachment	Please attach data from monitoring cybersecurity metrics. If metric data are unavailable, please attach a justification.	?

3.7 Cybersecurity Controls Report

A Cybersecurity Controls Report summarizes all security mitigations and controls implemented in the system per Appendix 1 of the FDA's 2023 Premarket Cybersecurity Guidance.

ACTION: Attach the Cybersecurity Controls Report as shown below. Complete the input field with the page numbers of the report where each of the control categories is addressed.

Cybersecurity Controls		
Add Attachment	Please attach information on the security controls categories included in the device.	?
Please cite the page number(s) of the attachment directly above where you addressed the following controls listed in the textbox below (e.g. "A) Authentication Controls: *Page 2*").		?
A) Authentication controls: B) Authorization controls: C) Cryptography controls: D) Code, data, and execution integrity controls: E) Confidentiality controls: F) Event detection and logging controls: G) Resiliency and recovery controls: H) Firmware and software update controls:		

3.8 Cybersecurity Testing Report

All security testing performed must be summarized in a Cybersecurity Testing Report, which will reference all individual testing reports from each discrete testing activity. These additional reports need to be appended and included with the Cybersecurity Testing Report.

ACTION: Attach the Cybersecurity Testing Report as shown below.

Cybersecurity Testing		
Add Attachment	Please attach a document(s) that describes the cybersecurity testing performed and the associated test reports. Cybersecurity testing includes but may not be limited to security requirement testing, threat mitigation testing, vulnerability testing, and penetration testing. If security testing was performed by a third party, please provided the original third party test report and your assessment of any findings. Alternatively, provide a justification for why particular testing was not performed.	?

3.9 Cybersecurity Labeling

Manufacturers must communicate specific cybersecurity information to end users in the product labeling and Instructions for Use (IFU).

ACTION: Attach the IFU containing cybersecurity content and communications for users within the IFU as shown below (this section in eSTAR is covered much earlier in the eSTAR dynamic PDF than the other cybersecurity sections and prompts).

Package Insert / Instructions for Use		
Add Attachment	Please attach copies of the User Instructions, Inserts, Directions for Use and/or Instructions for Use that are intended for use with your device. This includes instructions that may be downloaded or viewed on a website.	?

ACTION: Provide the page numbers of typical labeling attachments (IFU) where the FDA's 14 requirements are addressed into the text below as shown below.

Cybersecurity Labeling	
Please specifically cite the attachment(s) and page number(s) where cybersecurity information is documented in the labeling, as specified in the help text to the right for all the recommended elements. If there is separate cybersecurity labeling, attach this in the labeling section above.	?

3.10 Security Risk Management Plan

Although mentioned last, the Security Risk Management Plan (SRMP) should be the first document generated and maintained as part of a secure development process. The SRMP summarizes all plans and procedures for premarket and post-market activities, as well as the security goals for the project, the secure product development framework used for the system with references to QMS and governance structures, roles and responsibilities, and much more.

ACTION: Attach the Security Risk Management Plan in the prompt shown below. In the input fields, cite the page numbers within the plan where the FDA's requirements specified in the help text are addressed (click the "?" symbol to the right for the help text).

Cybersecurity Management Plan		
Add Attachment	Please attach a Cybersecurity Management Plan.	?
Please cite the page number(s) of the attachment directly above where you include the information specified in the help text to the right for all the recommended elements.		?
Please cite the page number(s) of the attachment directly above where you include a description of and justification for the time-lines to make patches on a regular cycle and out of cycle.		?

4.0 eSTAR Cybersecurity Requirements for Device Modifications with Changes Not Impacting Security

This section details the prompts within the Cybersecurity Section of the FDA eSTAR Submission System version 5.6 for device modification submissions that do not impact cybersecurity. Table 2 lists the artifacts required to be attached to an eSTAR submission for these scenarios.

Required Artifacts for eSTAR Submission	FDA Premarket Cybersecurity Guidance Sections	Section of this Document
Security Risk Management Plan	VI.B	0
Software Bill of Materials (SBOM)	V.A.4, VI.A	4.1
SBOM Support Report	V.A.4.a	4.1
Software Component Risk Management Report	V.A.4	4.1
Uncontrolled Risk Report	VII.D.2	4.2
Uncontrolled Risk Remediation Report	VII.D.2	4.2

Table 2. Required artifacts for FDA eSTAR device modification submissions with changes not impacting security

4.1 Software Bill of Materials (SBOM) and Related Reports

SBOMs contain lists of third-party software components included in the first-party software within the medical device system. Additional reports must also be generated that describe support information for the listed third-party components and an assessment of vulnerabilities affecting the same third-party components.

ACTION: Attach the SBOM file(s) in the first prompt shown below. These should be in either JSON or XML data structure formats using either the CycloneDX or SPDX specification. Attach the SBOM Support Report for the second attachment option and attach the Software Component Risk Management Report for the third attachment option. In the input field, describe the operating systems implemented in the system, if applicable.

Risk Management - Software Bill of Materials (SBOM) and Related Information		
Add Attachment	Please attach your Software Bill of Materials (SBOM).	?
Add Attachment	Please attach a document to provide the software level of support and end-of-support date for each software component (e.g. OTS software) identified in the SBOM. For any component where this information was not available, provide a justification.	?
List the supported operating system(s) and associated version(s) your device(s)/system uses. Be aware that if you list any operating systems that are no longer supported (e.g. Windows 7, Mac OS 9) or nearing end of support, this will generally be considered an inaccurate response. Type "N/A" if your device(s) does not use an operating system.		?
Add Attachment	Please attach a safety and security assessment of cybersecurity vulnerabilities in the component software used by the device for all software components in the SBOM and a description of any controls that address the vulnerability.	?

4.2 Vulnerabilities with Uncontrolled Risk Documentation

Per the FDA's 2016 Postmarket Cybersecurity Guidance, critical or catastrophic vulnerabilities are those that could cause permanent impairment or life-threatening injury or that could cause patient death, respectively. Uncontrolled risks arise from vulnerabilities that are critical in severity of patient harm and medium or high in exploitability, or uncontrolled risks arise from vulnerabilities that are catastrophic in severity of patient harm. Present uncontrolled risks must be documented in the Uncontrolled Risk Report, and the Uncontrolled Risk Remediation Report must detail any such vulnerabilities that no longer exist due to being mitigated since the previous authorization of the system.

ACTION: Attach the Uncontrolled Risk Report in the first prompt and the Uncontrolled Risk Remediation Report in the second prompt shown below.

Vulnerabilities with Uncontrolled Risk		?
Add Attachment	Please attach a document(s) with a description of whether there are currently any critical vulnerabilities that could cause uncontrolled risks.	
Add Attachment	Please attach a document(s) with a description of whether any vulnerabilities with uncontrolled risk were remediated in the device since the last authorization. If so, describe how the remediation was performed following the recommendations in FDA guidance "Postmarket Management of Cybersecurity in Medical Devices."	

4.3 Security Risk Management Plan

Although mentioned last, the Security Risk Management Plan (SRMP) should be the first document generated and maintained as part of a secure development process. The SRMP summarizes all plans and procedures for premarket and post-market activities, as well as the security goals for the project, the secure product development framework used for the system with references to QMS and governance structures, roles and responsibilities, and much more.

ACTION: Attach the Security Risk Management Plan in the prompt shown below. In the input fields, cite the page numbers within the plan where the FDA's requirements specified in the help text are addressed (click the "?" symbol to the right for the help text).

Cybersecurity Management Plan		
Add Attachment	Please attach a Cybersecurity Management Plan.	?
Please cite the page number(s) of the attachment directly above where you include the information specified in the help text to the right for all the recommended elements.		?
Please cite the page number(s) of the attachment directly above where you include a description of and justification for the time-lines to make patches on a regular cycle and out of cycle.		?

5.0 Optional PreSTAR Submissions for Investigational Device Exemptions

Investigational Device Exemptions (IDEs) and pre-submissions can be submitted or requested using the FDA's Early Submission Requests eSTAR (PreSTAR). For IDEs, this is currently voluntary. However, it is important for awareness of the pending release of an updated PreSTAR document and future requirements to submit IDE submissions or pre-submission requests via PreSTAR.

Per *Appendix 3. Submission Documentation for Investigational Device Exemptions* and *Appendix 4. General Premarket Submission Documentation Elements and Scaling with Risk* of the FDA's Premarket Cybersecurity Guidance, IDE submissions require a subset of the typical eSTAR submission requirements, including:

- Security Architecture Views and Security Use Case Views (included in the Threat Modeling and Security Architecture Report; see Section X)
- Machine-readable Software Bill of Materials (see Section X)
- Cybersecurity Labeling (see Section X)

Additionally, cybersecurity risk information must be included in the informed consent form for trial participants.

To document architecture views, to communicate security content in the product labeling and IFU, and to determine what cybersecurity risks are present and must be included in the consent form, threat modeling and risk assessment are often also recommended as design practices for IDE submissions and clinical trials. Designing a system right once is much easier than redesigning the system after a trial prior to commercialization.

6.0 Next Steps

The FDA's eSTAR submission process now requires structured and discrete cybersecurity documentation, with numerous artifacts necessary for compliance for both new submissions and device modifications. To accomplish this, medical device manufacturers must generate and provide several cybersecurity-related artifacts created during the Premarket phase.

Velentium Medical offers a comprehensive suite of templates, resources, and expert guidance to support your eSTAR submission. Our structured approach ensures that all required artifacts align with FDA expectations, reducing the complexity of compliance while strengthening the security posture of your medical device. By leveraging Velentium Medical's cybersecurity templates and resources, manufacturers can confidently navigate the eSTAR submission process, ensuring completeness, accuracy, and regulatory adherence.

See also Velentium Medical's *SEC-GUIDE-07 Total Product Life Cycle Security for Medical Devices* for more information on our Total Product Life Cycle Security process that details the activities and phases leading to the generation of the submission artifacts detailed in this guide.

Contact us and learn more at www.VelentiumMedical.com/EmbeddedCybersecurity.

7.0 Revision History

This guide has been revised as described below:

- Version 0: Initial Release
- Version 1: Updates corresponding to release of FDA eSTAR v5.5
- Version 2: Updates corresponding to release of FDA 2025 Premarket Cybersecurity Guidance, eSTAR v5.6, and PreSTAR v1.4

8.0 Appendix A: FDA eSTAR Mind Map

The graphic below shows the twelve FDA eSTAR artifacts and their required contents for successful premarket PMA, de novo, 510(k), and device modification submissions to the US FDA.