ELTON

Medical Device Contextual Vulnerability Justification (ELTON MDCVJ)

Medical Device Development Tool (MDDT) Proposal

Proposal Phase: Universal Tracking Number (UTN) Request

Cover Letter

Date: April 28, 2026

To: U.S. Food and Drug Administration, Center for Devices and Radiological Health (CDRH)

From: ELTON Cyber

Submission Type

MDDT Proposal Phase: Universal Tracking Number (UTN) Request

MDDT Name

ELTON Medical Device Contextual Vulnerability Justification (ELTON MDCVJ)

MDDT Type

Non-Clinical Assessment Model; Other (ELTON MDCVJ is a non-clinical, automated cybersecurity assessment tool that does not map precisely to the Non-clinical Outcome Measurement, Biomarker Test, or Clinical Outcome Assessment categories as defined in the MDDT Qualification Guidance; "Other" is added to avoid ambiguity and support FDA classification.)

Context of Use (COU)

ELTON MDCVJ is intended for the evaluation of cybersecurity vulnerabilities in medical devices and justification of resulting CVSS 4.0 vectors, specifically during premarket submissions of medical devices that meet the definition of a cyber device. As defined under section 524B(c) of the FD&C Act, a "cyber device" is 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. The FDA's "Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submissions" (February 3, 2026, Section VII, pp. 30–36) addresses section 524B of the FD&C Act for cyber devices.

Cyber devices are required to submit premarket review documentation to ensure that cyber devices meet the cybersecurity requirements under section 524B(b). Additionally, when determining the severity of a vulnerability that may affect their device, all medical devices must employ FIRST CVSS v4.0 [Rec# 13-140] by July 4, 2027.

ELTON MDCVJ incorporates and expands on the existing FDA MDDT "Rubric for Applying CVSS to Medical Devices" (Version 0.12.04, September 3, 2019) by modernizing the approach for CVSS 4.0 and increasing the concordance between the reported vulnerability evaluations and the device architecture representations in submission documentation, thereby allowing regulators to rely on ELTON-based CVSS 4.0 ratings with more confidence and less uncertainty. CVSS 4.0 is significantly more complex to compute, and unlike CVSS 3.0, difficult to perform manually for the volume of vulnerabilities in medical devices, such as the totality of SBOM, code scanning, and penetration testing results which can now result in hundreds of vulnerabilities requiring justifiable scores.

ELTON MDCVJ is intended for use by medical device manufacturers during the premarket submission phase of device development to support safety and effectiveness assessments related to cybersecurity. Its outputs (CVSS 4.0 vectors with architecturally traceable justifications) may be used by FDA reviewers to evaluate the severity of vulnerabilities reported in premarket documentation. CVSS ratings are commonly used as inputs to a manufacturer's cybersecurity risk assessment process. The tool is applicable at the design evaluation and premarket submission phases and is not intended to replace the manufacturer's cybersecurity risk assessment or other required risk management activities.

Previous Submission

No. This tool has not been previously submitted to the MDDT Program or to the Drug Development Tool (DDT) Program.

- Details on previous submission: N/A
- MDDT Q-submission / UTN number: N/A

Requestor Information

- **Requestor name:** Jason Sinchak
- **Requestor organization:** ELTON Cyber
- **Mailing address:** 55 S Main St, Suite 350, Naperville, IL 60540
- **Email address:** jsinchak@eltoncyber.com
- **Phone number:** 312-385-9578

MDDT Proposal Package

ELTON is pleased to submit this proposal for the FDA's consideration and feedback. We have followed the MDDT Proposal Submission Content guidance and organized this document so that each section can be traced to the corresponding FDA recommendation.

1. MDDT Description

Element	Response
Description of the MDDT	Medical device manufacturers may use ELTON MDCVJ to score cybersecurity vulnerabilities as input to assessing the safety and effectiveness of the medical device. ELTON MDCVJ is a vulnerability evaluation system designed to assess vulnerabilities reported within the specific scope of the manufacturer-provided premarket review documentation required to meet the cybersecurity requirements under section 524B(c) of the FD&C Act. The system intakes documentation provided during premarket review, such as the cybersecurity architecture views, threat model, cybersecurity risk assessment, cybersecurity risk management report, cybersecurity controls documentation, Software Bill of Materials (SBOM), SBOM vulnerability assessment, and cybersecurity testing reports. The system allows users to further create and edit device architectures and security design directly through a graphical user interface (GUI) and to ensure traceability to premarket submission and quality management documentation. New vulnerabilities enter the evaluation system through sources and reports required by FDA ("Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submissions," February 3, 2026, Section V.C, pp. 25–26, including "fuzz testing," "known vulnerability scanning," "static and dynamic code analysis," and "penetration testing"). When a new vulnerability is linked to components present in the architecture, ELTON MDCVJ automatically produces a device-specific CVSS 4.0 vector. ELTON MDCVJ incorporates architectural

Element	Response
	attributes, trust relationships, countermeasures, interconnections, and interactions between security-relevant elements commonly part of premarket submissions. Unlike ad-hoc scoring by humans, ELTON MDCVJ produces traceable, standardized, and architecturally justified vectors. Because each CVSS 4.0 vector is computed deterministically from the property graph, the vector for a given vulnerability can only change when the underlying architectural inputs change. Any modification to a CVSS 4.0 vector therefore requires a corresponding, traceable modification to the change-controlled premarket review documentation from which the property graph was derived, ensuring that vulnerability ratings remain aligned with the architecture and threat model on file.
How the tool is intended to support an assessment of safety, effectiveness, or performance to facilitate regulatory decision-making	When used to evaluate vulnerability reports included by a manufacturer in a premarket submission, regulatory decision-makers can accept ELTON MDCVJ outputs with confidence that the vulnerability ratings align with the manufacturer-provided security architecture documentation, without additional review or inspection of the vulnerability evaluation process or unstructured justifications.
Category of the MDDT	Non-Clinical Assessment Model; Other (the tool does not map cleanly to NAM, BT, or COA as defined in Section IV of the MDDT Qualification Guidance; Other is added to support classification and avoid ambiguity).
Is the proposed MDDT a cleared or approved medical device?	No. ELTON MDCVJ is not a cleared or approved medical device.
Has the MDDT been previously submitted to the MDDT Program or the DDT Program?	No. ELTON MDCVJ has not been previously submitted to the MDDT Program or through the Drug Development Tool Program.

Description of how the MDDT achieves the specified output

The ELTON MDCVJ process produces CVSS 4.0 vectors that are explicitly grounded in a device's security architecture documentation, such as cybersecurity architecture views, threat model, cybersecurity risk assessment, cybersecurity risk management report, cybersecurity controls documentation, Software Bill of Materials (SBOM), SBOM vulnerability assessment, and cybersecurity testing reports provided to the FDA during premarket submission. CVSS v4.0 vectors are industry-standard strings that encode the key characteristics of a software vulnerability into a single, machine-readable score. Vectors are a structured fingerprint for a vulnerability in a format standardized by FIRST; they capture factors such as how the vulnerability is exploited (over a network vs. requiring physical access), whether user interaction is needed, and what the potential impact is on confidentiality, integrity, and availability of the affected system. The resulting string, such as "CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N" is decoded into a numeric score (0–10) that lets security teams quickly compare and prioritize vulnerabilities across products, vendors, and time, without relying on subjective judgment. How the factors are selected may be subjective, without a tool such as ELTON MDCVJ.

Rather than treating vulnerabilities in isolation, the system evaluates how a given vulnerability can be reached and its potential downstream safety impacts within a specific device design. The outputs include a CVSS 4.0 rating and explanations of each of the standard CVSS v4.0 metrics in the vector.

At a high level, the system proceeds through the stages in the figure below.

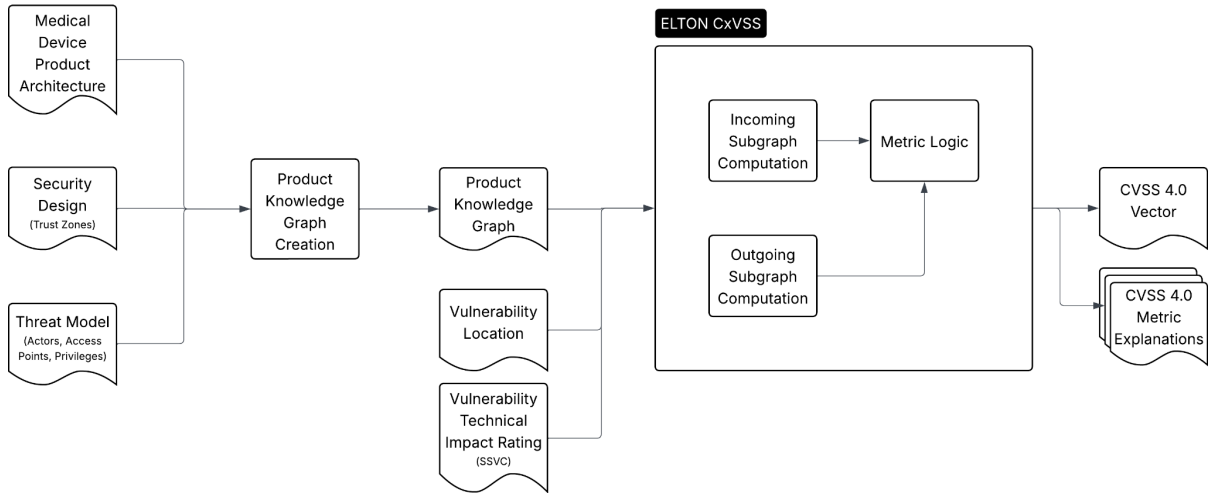

Figure 1. MDCVJ Scoring Pipeline

Stage 1: Ingest Regulatory Architecture Views and Security Context

The MDCVJ process begins by ingesting security artifacts that are already required and commonly included as part of a regulated medical device submission. Primary inputs include the manufacturer-provided premarket review documentation required to meet the cybersecurity requirements under section 524B(c) of the FD&C Act and required by eSTAR.

- Cybersecurity Architecture Views (Global System View, Multi-Patient Harm View, Updatability/Patchability View, Security Use Case Views): These views provide the authoritative representation of the device's software architecture and data flows. They are typically expressed as data flow diagrams (DFDs) and capture system components, interfaces, and trust boundaries as reviewed during regulatory submission.
- Software Bill of Materials (SBOM) and Software Support and End-of-Support Documentation: The SBOM provides a structured inventory of software components and dependencies.
- Threat Model, Cybersecurity Risk Assessment, Cybersecurity Risk Management Report, Cybersecurity Controls Documentation (covering Authentication, Authorization, Cryptography, Code/Data/Execution Integrity, Confidentiality, Event Detection and Logging, Resiliency and Recovery, and Firmware/Software Update controls): The device's security design defines trust levels and trust zones across the architecture, establishing the system's security hierarchy. These trust zones describe relative privilege, isolation, and exposure assumptions that are critical to determining exploitability and required privileges. Trust boundary (zones) and security controls or mitigations are commonly found within the eSTAR Risk Management Report.
- Cybersecurity Testing Reports (Security Requirements Testing, Threat Mitigation Testing, Vulnerability Testing, Penetration Testing) and Cybersecurity Vulnerability Assessment of SBOM.

Together, these inputs establish the foundation for contextual vulnerability analysis without requiring new or duplicative documentation.

Stage 2: Transform Inputs into a Structured Property Graph

This transformation is performed automatically by ELTON MDCVJ upon ingestion of the premarket review documentation described in Stage 1; no manual graph construction is required of the user. After automated ingestion, the user may optionally review and edit the graph through the ELTON MDCVJ graphical user interface to correct or extend the representation where the source documentation is incomplete, with every edit logged and traceable back to the underlying documentation.

The documentation is normalized into a property graph with a fixed, well-defined structure that supports automated reasoning between relationships key to cybersecurity. There are two component types, Nodes and Edges, defined as follows:

Nodes (Components)

Each component becomes a node. A component can be any software or hardware element in the product, such as an operating system, software application, process, or software dependency. Nodes carry structured properties, including:

- Trust level (zone and relative level within the system)

- Assets (data with cybersecurity impact in the system, such as sensitive files, configurations, or keys), with confidentiality, integrity, and availability (CIA) requirements expressed as High / Low / None
- Countermeasures that apply (i.e., controls)
- A configurable attribute to denote components that are customer-configurable or optional in different deployment models and whether they are active in the device architecture under review

Edges (Data Flows)

Each data flow becomes a directed edge between components. Edges include:

- Source and destination components
- Source and destination interfaces, including interface type (Network, Adjacent, Local, Physical)
- Configurable attribute to denote interfaces that are optional in different deployment models and whether they are active in the architecture under review

This transformation produces a consistent, machine-readable representation of the device's security architecture that preserves trust boundaries, exposure points, and asset sensitivity. The resultant property graph is traceable to input documentation using tags associated with where each element of the graph was sourced. The property graph is displayed and may be modified as necessary by the manufacturer to ensure the representation aligns with detailed specifications.

Stage 3: Define the Vulnerability Target

A scoring target is the explicit association of a known vulnerability with a concrete architectural component represented in the system's property graph.

The system updates a scoring target whenever a triggering event occurs, including:

- The addition of a new vulnerability:
    - From source documentation, e.g., a penetration testing report or SBOM vulnerability scan
    - Manually by a user addition
    - Automatically via integrated feed of new public CVE data for known software materials assigned to a component
- A user change to the system architecture represented in the system's property graph

For each scoring target, the system evaluates:

A vulnerable component

A component node derived from premarket review documentation and represented in the property graph.

A specific vulnerability on that component

The vulnerability attached directly to a component node as the directly affected target of the vulnerability.

Each vulnerability is represented as a structured object with attributes required for contextual evaluation, including:

- An optional machine-readable Stakeholder-Specific Vulnerability Categorization (SSVC) decision string (per the SSVC standard; CISA/CMU SEI) where available from National Vulnerability Databases. SSVC informs the consequence of successful vulnerability exploitation in isolation (without full context of the device) as it pertains to how it directly affects the component. SSVC is operational context-specific, rather than producing a generic numeric score. Instead of asking "how bad is this vulnerability in the abstract," SSVC asks a series of structured questions: Is it being exploited in the wild? Is the affected system safety-critical? Is it deployed in your environment?
- On-component reachability indicators (exposure indicator) providing context as to whether the vulnerability can be exploited (reached) regardless of trust level of the component it resides on (e.g., unauthenticated remote code execution)

At this stage, the vulnerability is treated as a property of the component itself, independent of any particular attacker entry point or exploit path. This explicit binding ensures that scoring is anchored to the device's documented architecture and that all subsequent analysis operates on a well-defined, unambiguous target. This step establishes the unit of analysis for MDCVJ: a single vulnerability as it exists on a specific component within a specific device design.

Stage 4: Derive Contextual Subgraphs

Using the property graph and the defined scoring target, the system derives constrained subgraphs that represent the exploitability and impact context of the vulnerability. Initial Access nodes defined in source documentation or elected by the user are used to perform attack-path analysis from a starting point (initial access) to the scoring target (vulnerability). Initial access points represent the attack surface of the device, providing key context for various means by which a target vulnerability may be attempted exploitation or be reachable. Initial access points can include Wi-Fi, Bluetooth, USB ports, user interface screens, and board-level debugging outputs. This process is performed independently for each initial access node defined in the source material documentation (such as the threat model) or manually added in the ELTON MDCVJ user interface, as different entry points carry different exposure, trust, and privilege assumptions.

For a given initial access node, two contextual subgraphs are produced.

Incoming (Pre-Compromise) Subgraph

The incoming subgraph represents the set of feasible architectural paths by which a threat actor can reach the vulnerable component from a specific initial access point. Rather than enumerating all possible paths, the incoming subgraph consists of:

- All nodes and edges reachable forward from the initial access node, subject to traversal constraints, and
- All nodes and edges reachable in reverse from the vulnerable component back toward the initial access node

The intersection of these traversals yields the minimal set of components, interfaces, and data flows that lie on at least one feasible path from the initial access node to the vulnerable component. This corridor captures reachability of the vulnerable component and trust levels traversed prior to exploitation.

Outgoing (Post-Compromise) Subgraph

The outgoing subgraph represents all feasible propagation paths after the vulnerable component is compromised. Starting from the vulnerable component, the system performs constrained forward traversal to identify downstream components and data flows that may be impacted as a result of exploitation. This subgraph defines:

- Downstream components that may be affected
- Opportunities for trust escalation or lateral movement
- Assets that may be exposed beyond the initially compromised component

Both subgraphs are computed using constrained graph traversal rules that respect architectural directionality and trust boundaries. This ensures that only feasible and security-relevant paths are included in the analysis.

By deriving these subgraphs separately for each initial access node, the system preserves attack-scenario-specific context (e.g., an authenticated service technician, an unauthenticated user of the product touchscreen, a threat actor on the local Wi-Fi network, a threat actor with physical access, etc.) and enables consistent evaluation of how different initial access attack-surface entry points affect exploitability and impact on the assets within a medical device for a given vulnerability.

Stage 5: Apply Rule-Based CVSS 4.0 Scoring Logic

For each initial access node defined in the threat model, the derived incoming and outgoing subgraphs and their associated properties are passed to a scoring service that applies deterministic rules in accordance with the FDA MDDT “Rubric for Applying CVSS to Medical Devices” (Version 0.12.04, September 3, 2019), expanded to meet the more complex CVSS 4.0 specification for a given metric. Logic is adapted to operate over explicit architectural paths provided in premarket review documentation rather than subjective questionnaire responses. Each initial access node defines a distinct exploitation scenario for the same vulnerability, resulting in a CVSS 4.0 score for each initial access point.

Each CVSS metric is computed through structured logic to align with the CVSS 4.0 specification and directly reference architectural elements. For example:

- Exploitability metrics are derived from:
    - Entry interfaces and exposure types
    - Trust levels traversed
    - Potential countermeasures
    - Dependency on configurable components or interfaces
    - User interaction attributes of the initial access point
- Impact metrics are derived from:
    - Asset sensitivities on the vulnerable component
    - Asset sensitivities on downstream impacted components
    - Differences between pre- and post-compromise scope

If a given initial access node cannot reach the vulnerable component under the defined traversal constraints, the resulting scenario is considered non-exploitable, and exploitability-related metrics are correspondingly set to reflect no feasible attack path.

Stage 6: Generate Scores and Traceable Explanations

For each vulnerability target and for each initial access point in the device architecture, the system produces:

- A complete CVSS 4.0 vector, score, and severity
- Metric-level explanations that explicitly reference the components, interfaces, trust levels, and assets that influenced each metric, and the attack paths and propagation paths used in the analysis
- References to the source materials supporting elements of the graph employed for the metrics (where a component, interface, trust level, or asset was sourced in documentation)

This results in a set of multiple scores and justifications for a single vulnerability across different initial-access attack surfaces, each corresponding to a different initial-access assumption. For example, how a vulnerability may be rated if exploited from the network versus physically.

To support reporting and decision-making, the system designates a canonical vulnerability score, defined as the highest-severity CVSS score produced across all feasible initial access scenarios. Scores from other scenarios are retained as supporting context and reference, enabling reviewers to understand how different entry points influence risk.

This approach preserves architectural fidelity, avoids overstating exploitability, and maintains a direct, auditable link between the device architecture, threat assumptions, and resulting CVSS scores.

Regulatory Context and Related Guidance

As part of premarket submissions, medical device manufacturers must document design output in terms that allow an adequate evaluation of conformance to design input requirements (21 CFR 820.30(d)) and, as expanded in FDA's "Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submissions" (February 3, 2026, Section V.B.2, pp. 22–24), provide documentation on the security architecture, including "the security context and trust-boundaries of the medical device system in terms of the interfaces, interconnections, and interaction that the medical device system has" (Section V.B.2, p. 22). FDA further "recommends that this architecture information take the form of 'views,' and that these views be provided during premarket submissions to demonstrate safety and effectiveness" (Section V.B.2, pp. 22–24). Manufacturers must also include a plan to assess cybersecurity vulnerabilities (21 U.S.C. § 360n-2(b)(1)).

Manufacturers must also demonstrate the effectiveness of design controls "beyond standard software verification and validation activities to demonstrate the effectiveness of the controls in the proper security context" (Section V.C, pp. 25–26), resulting in the inclusion of vulnerabilities discovered in the device during design and development through activities such as "closed-box testing of known vulnerability scanning," "software composition analysis," "static and dynamic code analysis," and "penetration testing."

The current state of the art of vulnerability rating is manual and subjective, based on opinion or, at best, in accordance with the FDA MDDT "Rubric for Applying CVSS to Medical Devices" (Version 0.12.04, September 3, 2019), with no traceability to documentation submitted during premarket review. The existing MDDT covers only CVSS 3.0 and is not contextual to medical device documentation. No current FDA guidance exists for adopting CVSS 4.0. CVSS 4.0 is significantly different from the CVSS 3.0 specification in that it introduces multiple new metrics, redefines existing metrics, and introduces new underlying math for how quantitative scores are computed. While some logic from CVSS 3.0 can be re-used, a new approach is needed to properly calculate CVSS 4.0. The new metrics are difficult to compute manually because they require whole-device context. For example, CVSS 4.0 introduces the Attack Requirements (AT) metric, which evaluates whether additional requirements must be met along a particular attack path (initial-access point) prior to the vulnerability being exploited; this type of analysis is difficult to perform manually with accuracy and is extremely time-consuming for a single vulnerability, and not scalable to the hundreds reported within regulatory premarket review documentation. Additionally, CVSS 4.0 expands the existing CVSS 3.0 metrics for Confidentiality, Integrity, and Availability (which pertain to the directly impacted component of a vulnerability) with an additional, more complex, Subsequent Confidentiality, Integrity, and Availability impact metric that evaluates how the vulnerability can affect downstream assets in the system. Determining subsequent impact requires a knowledge graph to determine how the privileges and assets immediately compromised by a vulnerability may be re-used by a threat actor to gain further access to the system and compromise additional assets.

ELTON MDCVJ provides traceability for CVSS 4.0 decisions that resulted in a particular metric based on the evidence submitted by medical device manufacturers in premarket submissions.

2. Context of Use (COU)

ELTON MDCVJ is intended for the evaluation of cybersecurity vulnerabilities in medical devices and justification of resulting CVSS 4.0 vectors, specifically during premarket submissions of medical devices that meet the definition of a cyber device. As defined under section 524B(c) of the FD&C Act, a “cyber device” is 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. The FDA’s “Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submissions” (February 3, 2026, Section VII, pp. 30–36) addresses section 524B of the FD&C Act for cyber devices.

Cyber devices are required to submit premarket review documentation to ensure that cyber devices meet the cybersecurity requirements under section 524B(b). Additionally, when determining the severity of a vulnerability that may affect their device, all medical devices must employ FIRST CVSS v4.0 [Rec# 13-140] by July 4, 2027.

ELTON MDCVJ incorporates and expands on the existing FDA MDDT “Rubric for Applying CVSS to Medical Devices” (Version 0.12.04, September 3, 2019) by modernizing the approach for CVSS 4.0 and increasing the concordance between the reported vulnerability evaluations and the device architecture representations in submission documentation, thereby allowing regulators to rely on ELTON-based CVSS 4.0 ratings with more confidence and less uncertainty. CVSS 4.0 is significantly more complex to compute, and unlike CVSS 3.0, difficult to perform manually for the volume of vulnerabilities in medical devices, such as the totality of SBOM, code scanning, and penetration testing results which can now result in hundreds of vulnerabilities requiring justifiable scores.

ELTON MDCVJ is intended for use by medical device manufacturers during the premarket submission phase of device development to support safety and effectiveness assessments related to cybersecurity. Its outputs (CVSS 4.0 vectors with architecturally traceable justifications) may be used by FDA reviewers to evaluate the severity of vulnerabilities reported in premarket documentation. CVSS ratings are commonly used as inputs to a manufacturer’s cybersecurity risk assessment process. The tool is applicable at the design evaluation and premarket submission phases and is not intended to replace the manufacturer’s cybersecurity risk assessment or other required risk management activities.

3. Performance Criteria

ELTON MDCVJ is intended to achieve accuracy comparable to, or exceeding, expert human assessment, while improving rating consistency and reducing assessment time relative to manual expert evaluation. Specifically, ELTON MDCVJ is designed to achieve the following performance characteristics:

Performance Criterion	Acceptance Threshold	Justification / Explanation
Accuracy	Accuracy comparable to, or exceeding, expert human assessment.	Because no objective ground truth exists for vulnerability severity, accuracy is defined as the reasonableness of the CVSS vector for decision-making. Reasonableness is evaluated based on the extent to which the ELTON MDCVJ output: • Aligns with expert judgment when experts are provided with equivalent architectural and threat context; and • More appropriately reflects the specific security architecture documentation and use conditions than a context-independent CVSS vector (e.g., NVD). Accuracy will be evaluated by comparing expert assessments, with interrater agreement in the CVSS severity category and vector.
Consistency	For a given input knowledge graph, ELTON MDCVJ produces a deterministic CVSS 4.0 vector, score, and justification. Consistency is evaluated by re-executing ELTON MDCVJ on version-controlled knowledge graphs and confirming that the emitted CVSS 4.0	Ensures repeatable and auditable vulnerability assessments across diverse reported vulnerability sources, such as those required by FDA (“Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submissions,” February 3, 2026, Section V.C, pp. 25–26, including “fuzz testing,” “known vulnerability scanning,” “static and dynamic code analysis,” and “penetration testing”).

Performance Criterion	Acceptance Threshold	Justification / Explanation
	vectors, scores, and metric-level justifications are identical across runs (see Consistency Study under Section 4, Qualification Plan).	
Efficiency	For a given medical device software version, ELTON MDCVJ produces vulnerability scores more efficiently than manual expert assessment processes.	Manufacturers are required to include cybersecurity vulnerability information for hundreds of vulnerabilities as part of applicable premarket submissions which are then reviewed by the FDA. One key source, under §524B(b)(2) of the Federal Food, Drug, and Cosmetic Act, is the Software Bill of Materials (SBOM), while §524B(b)(1) requires manufacturers to identify all known vulnerabilities associated with the device and hundreds of its software components. Efficiency is included as a characterized performance attribute for the benefit of FDA as it reduces the need to challenge a high volume of ratings provided by a manufacturer. Tool users (medical device manufacturers) realize efficiency in creating the ratings, encouraging a higher volume of vulnerability disclosure

4. Qualification Plan

The following qualification plan describes the evidence-generation strategy to demonstrate that ELTON MDCVJ reliably and accurately meets the performance criteria defined above. The plan addresses each performance criterion through structured study protocols with predefined endpoints, metrics, and acceptance criteria. The performance criteria being addressed are:

- Accuracy: ELTON MDCVJ produces CVSS 4.0 vectors that are at least as accurate as expert human assessment and more accurate than context-independent public vulnerability ratings.
- Directionality of Error: In cases of disagreement, ELTON MDCVJ produces ratings that are more conservative (higher severity) rather than less conservative.
- Consistency: ELTON MDCVJ produces deterministic, reproducible outputs for identical inputs.
- Efficiency: ELTON MDCVJ reduces the time and level of specialized expertise required relative to manual expert assessment.

Research Questions

1. Accuracy

- a. Does ELTON MDCVJ produce CVSS 4.0 vectors that are considered reasonable by expert raters when provided with equivalent security documentation available during premarket review?
- b. Does ELTON MDCVJ produce results that are more accurate, based on expert judgment, than context-independent vulnerability ratings from public sources, such as the National Vulnerability Database (NVD)?
- c. When ELTON MDCVJ results differ from expert assessments, are the differences systematically more or less severe?
- d. When differences occur, do expert re-reviews support the ELTON MDCVJ output as reasonable for decision-making?
- e. To what extent are observed disagreements attributable to differences in the premarket review documentation provided to ELTON MDCVJ versus the documentation context available to expert raters?

2. Consistency

- a. For a given input (i.e., knowledge graph), does the tool produce a deterministic output?

3. Efficiency

- a. Is the total time required to generate or review CVSS assessments using ELTON MDCVJ less than the time required for manual expert vulnerability assessment of each vulnerability reported in a premarket submission?
- b. Is the level of expertise needed to review vulnerabilities in medical devices reduced?

Proposed Study Designs

Accuracy Study

Design

- Retrospective, blinded comparative agreement study.
- Vulnerabilities are sourced from the National Vulnerability Database (NVD) for known software bill of materials (SBOM) components in the target devices. The context-independent CVSS 4.0 ratings published by NVD serve as the baseline comparator.

Comparators:

- Context-independent public CVSS 4.0 rating for vulnerabilities from NVD (https://nvd.nist.gov/vuln/search).
- ELTON MDCVJ CVSS 4.0 submission-context vulnerability rating (automated ratings with context).
- Expert human CVSS 4.0 vulnerability rating produced by independent third-party assessors who scores vulnerabilities using the FIRST CVSS 4.0 calculator with access to the same premarket review documentation provided to ELTON MDCVJ. The expert human must satisfy the following minimum qualifications: (i) hold at least one current, recognized professional cybersecurity credential (e.g., CISSP, OSCP, GPEN, or CEH); (ii) have a minimum of five years of hands-on experience testing for cybersecurity vulnerabilities in medical devices; (iii) have proficiency with FIRST CVSS 4.0 scoring.

Sample Characteristics:

- 6 medical devices
- 3 manufacturers
- 5 vulnerabilities per device
- 2 expert third-party raters per vulnerability

Process:

1. Independent third-party cybersecurity experts (e.g., penetration testers with medical device experience) independently score each vulnerability in CVSS 4.0 using the FIRST CVSS 4.0 calculator, with access to the same premarket review documentation provided to ELTON MDCVJ.
2. ELTON MDCVJ generates CVSS 4.0 vectors using knowledge graphs derived from the same manufacturer-authored premarket review documentation that is provided to the expert raters — specifically the cybersecurity architecture views, threat model, cybersecurity risk assessment, cybersecurity risk management report, cybersecurity controls documentation, SBOM, SBOM vulnerability assessment, and cybersecurity testing reports. The knowledge graphs are produced automatically by ELTON MDCVJ from that documentation; no study-specific or ELTON-authored

documentation is introduced. This documentation is authored by the device manufacturer as part of the premarket submission for public NVD vulnerabilities.

3. Disagreements between ELTON MDCVJ and expert ratings are identified and subjected to a structured adjudication process. Expert raters are provided with the ELTON MDCVJ justifications and supporting premarket review documentation to perform an informed re-review. The re-review is performed by the same two expert raters per vulnerability described under Comparators above (no separate panel is introduced), and meeting the same qualifications. During the initial scoring phase, raters are blinded to ELTON MDCVJ output and to manufacturer identity. During the re-review phase, raters are unblinded to the ELTON MDCVJ vector and justification strictly for the purpose of adjudicating disagreements, and each rater documents whether the re-review leads them to revise their initial score.
4. Disagreements are categorized using the following taxonomy:
    - **Expert Revision upon Re-review.** Upon structured re-review with access to ELTON MDCVJ CVSS 4.0 justifications and the same premarket documentation used by ELTON MDCVJ, the expert determines that their initial assessment was incorrect or incomplete and revises the CVSS 4.0 score to align within 0.1 of the ELTON MDCVJ output.
    - **Greater MDCVJ Score.** ELTON MDCVJ assigns a higher severity rating than the expert assessment, reflecting a more conservative (safe) interpretation of CVSS 4.0 metrics derived from the premarket review documentation.
    - **Lower Conservative MDCVJ Score.** ELTON MDCVJ assigns a lower severity rating than the expert assessment, reflecting a less conservative (safe) interpretation of CVSS 4.0 metrics derived from the premarket review documentation.
    - **Incomplete or Insufficient Documentation.** The premarket review documentation lacks sufficient detail, fidelity, or clarity for either the ELTON MDCVJ knowledge graph or the expert assessment to fully capture the architectural elements, trust relationships, or operational constraints relevant to the vulnerability.
    - **Residual Expert Disagreement.** After structured re-review, experts maintain a different assessment that cannot be attributed to the categories above, reflecting inherent subjectivity in contextual vulnerability assessment.

Endpoints:

Category	Research Question	Endpoint	Metric	Acceptance
Agreement with Context-	1a	Raw agreement between ELTON MDCVJ and	% agreement	>90% within 0.1 rating

Category	Research Question	Endpoint	Metric	Acceptance
Aware Expert Opinion		industry-standard third-party expert rating		
More Accurate than Context-Independent Sources	1b	Expert opinion agreement that ELTON MDCVJ is more accurate than context-independent CVSS vectors (e.g., NVD)	% of expert assessments confirming ELTON MDCVJ is more accurate than context-independent sources	>90% agree
Directionality of Disagreement	1c	Distribution of ELTON MDCVJ disagreements with expert opinion by severity direction (more severe or less severe)	% by direction	Diagnostic
Expert Revision Upon Re-Review	1d	Proportion of disagreement cases in which expert re-review supports the ELTON MDCVJ output as reasonable for regulatory decision-making	% disagreement cases support ELTON MDCVJ as reasonable	>90%
Disagreement Attribution	1e	Categorization of disagreements using the predefined taxonomy	% by category	Diagnostic

Consistency Study

Design:

- Repeated execution of ELTON MDCVJ on fixed, version-controlled knowledge graphs across multiple runs and environments.

Endpoints:

Category	Research Question	Endpoint	Metric	Acceptance
Determinism	2a	ELTON MDCVJ scores are identical across repeated executions for identical inputs	% identical	100%

Efficiency Study *(reported for tool-user and agency reviewer benefit)*

Design:

- Time study using the same experts participating in the accuracy study.

Comparators:

- Manual expert vulnerability assessment time
- ELTON MDCVJ workflow time (requiring less expert review)

Endpoints:

Category	Research Question	Endpoint	Metric	Acceptance
Review Time Reduction	3a	ELTON MDCVJ total time per vulnerability	Mean time per vulnerability	Statistically significant reduction ($p < 0.05$)
Expertise Required	3b	ELTON MDCVJ provides vulnerability ratings with reduced third-party expert opinion review	Mean total expert opinion time required for entire vulnerability assessment workflow	Statistically significant reduction ($p < 0.05$)

5. Assessment of Advantages and Limitations

Advantages

Improved Traceability. Manufacturers are required to submit security architecture documentation, threat modeling artifacts, and vulnerability reports derived from multiple testing activities as part of a premarket submission. However, the vulnerability ratings provided, expressed using CVSS, are often not traceable to the security architecture documentation included in the submission. Under existing practice, individual vulnerabilities are first assigned a CVSS rating and subsequently used as inputs to the cybersecurity risk assessment included in the submission, yet there is no verifiable linkage between the assigned rating and the underlying architectural, threat, or control information. These ratings are derived from manual expert judgment without documented traceability. Traceability is required by FDA ("Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submissions," February 3, 2026, Sections V.A, V.A.1–V.A.6, V.B.1, V.B.2, V.C, VI.A).

Improved Consistency and Reproducibility. Unlike manual expert assessments, ELTON MDCVJ generates deterministic outputs for a given input knowledge graph, improving reproducibility and reducing inter-expert variability in vulnerability scoring. Under current practices, the assignment of CVSS ratings allows for considerable subjectivity among experts, so the same vulnerability may receive different ratings depending on the assessor.

Context-Specific Accuracy. ELTON MDCVJ accounts for architectural, trust, and threat context, providing more precise vulnerability assessments than generic, context-independent CVSS scores (e.g., initial public NVD ratings). This ensures assessments reflect device-specific safety and security control effectiveness considerations relevant for premarket evaluation. Manufacturers are required to provide security architecture documentation in premarket submission that describe "security domains, the placement of security-relevant elements within the security domains, the interconnections and trust relationships between the security-relevant elements, and the behavior and interactions between the security-relevant elements" (FDA, "Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submissions," February 3, 2026, Appendix 5, p. 57). However, the submitted security architecture and threat modeling documentation is not currently used in the assessment of vulnerability severity ratings in a manner that provides objective, reviewable, or disputable evidence. As a result, reviewers are unable to independently evaluate or challenge the assigned ratings using the documentation under review, limiting the ability to assess whether the severity determinations are appropriately justified in the context of the device's design and cybersecurity controls.

Alignment with Existing Risk Management Guidance. As part of premarket submission, manufacturers are required to submit a Security Risk Management Report (FDA, "Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submissions," February 3, 2026, Section V.A, p. 10) which specifies the need to provide "traceability between the threat model,

cybersecurity risk assessment, SBOM, and testing documentation." The tool supports a structured approach to meeting this expectation by ensuring that vulnerability ratings within testing documentation are traceable to the underlying security documentation, thereby complementing and strengthening the manufacturer's overall cybersecurity risk management activities through complete traceability.

Alignment with Existing Worst-Case Premarket Cybersecurity Risk Assessment Guidance. As part of a premarket submission, manufacturers are required to execute "security risk assessment processes focused on exploitability, or the ability to exploit vulnerabilities present within a device and/or system" (FDA, "Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submissions," February 3, 2026, Section V.A, p. 10). More specifically, "premarket assessment of exploitability of a cybersecurity risk may be different from the exploitability assessment of a vulnerability discovered postmarket. In these instances, a premarket exploitability assessment could either assume a worst-case assessment" (Section V.A.2, p. 13). The tool supports an approach in which vulnerabilities are rated such that each CVSS metric is traceable to supporting documentation included in the premarket submission, including the device's security architecture and threat model, thereby enabling a worst-case assessment based on the manufacturer's documented representations. This approach minimizes reliance on undocumented expert judgment in favor of conservative, evidence-based severity determinations, resulting in vulnerability ratings that reflect the highest plausible CVSS scores and provide a clear and defensible depiction of residual cybersecurity risk and its potential impact on device safety and effectiveness.

Operationalization of FDA-Requested Security Architecture and Threat Model Documentation. As part of a premarket submission, manufacturers are required to provide Security Architecture Views, such as "global system, multi-patient harm, updatability and patchability, and security use case views" (FDA, "Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submissions," February 3, 2026, Section V.B.2, pp. 22–24) and Threat Modeling (Section V.A.1, p. 12) documentation. The tool employs the submitted documentation as structured inputs to generate a knowledge graph that is subsequently used to rationalize CVSS metric selections for vulnerabilities included in the premarket submission. A key justification for the inclusion of Security Architecture Views in premarket submissions is articulated in the guidance, which states: "If corrective and preventive actions are identified, these views can be used to help identify impacted functionality and solutions that address the risks." The tool operationalizes this guidance by enabling these architectural views to be directly used in the process of vulnerability rating. As a result, the security architecture documentation provided to the FDA as part of the premarket submission can be relied upon as having been actively utilized in the derivation and justification of vulnerability severity ratings during premarket review.

Limitations

Incomplete Submission Documentation. ELTON MDCVJ requires a detailed, standardized representation of the device architecture, including components, interfaces, and trust relationships. The documentation currently required by FDA for premarket submission of cyber devices provides the level of detail needed. In the event that documentation detail is low, ELTON MDCVJ will result in more severe ratings due to the lack of security detail and design information, preventing a situation where low-resolution documentation results in lower ratings from ELTON MDCVJ.

Scope of Use. The tool is not intended to replace cybersecurity risk assessments, in which additional non-technical cybersecurity mitigations and safety impacts are evaluated. ELTON MDCVJ provides accurate and efficient vulnerability ratings prior to those vulnerability ratings being employed in a cybersecurity risk assessment, resulting in more accurate cybersecurity risk assessment input. ELTON MDCVJ should be used as part of a broader cybersecurity risk management strategy rather than as a standalone determinant of safety or effectiveness.