ELTON

WHITEPAPER · FDA TRACEABILITY

Every ELTON Activity, Traced to FDA

The cybersecurity deficiencies FDA reviewers write on real submissions, the activity that answers each one, and where the requirement is written

KEY TAKEAWAYS

- Most of the activities in an ELTON subscription began as an FDA deficiency on a customer's submission. The reviewer wording in this paper comes from cybersecurity submissions ELTON has worked through, and each one is paired with the activity that now answers it before it is asked.
- Five deficiencies account for most of the trouble: pentest findings marked "deferred" are rejected outright; interface V&V has to be test cases per mechanism or a justification; a postmarket vulnerability management plan is required under Section 524B; a pentest that covers a subset of the product fails the SPDF; and a postmarket plan without regular penetration testing draws its own deficiency.
- Behind those five sits a long tail of documentation deficiencies, from the threat model and the four control families to SBOM format, end-of-life components, patch timelines, disclosure and labeling. Each pairs a reviewer request with an artifact ELTON produces from the same digital twin.
- Every activity in a subscription traces to the requirement it evidences: the premarket cybersecurity guidance, Section 524B, the 2016 postmarket guidance, QMSR, and the MDDT-qualified rubric. Section 3 carries the full map.
- Every deficiency traces to the same root. Legacy testing produces findings and advice, with no evidence behind them, and it stops at clearance. A deficiency is prevented by producing the evidence before the reviewer asks for it, and keeping it current.

Executive summary

A point-in-time pentest hands you a PDF of findings and high-level advice. FDA reviewers want the opposite: test cases mapped to threats, prescriptive fixes, proof that each mitigation was tested, and evidence of prior results. Increasingly they also ask how you will keep testing after clearance.

The same gaps recur across premarket review under Section 524B and across postmarket review. No test-case testing for threat mitigations, so a reviewer asks for interface-by-interface verification. Vendor recommendations that are not actionable, which FDA then treats as the fix criteria. A claimed control that was never attacked, and no evidence of prior testing results or a plan to keep testing. Each of those produces a deficiency letter with wording that has become familiar, because ELTON has answered it on more than 1,000 submissions.

That history is where the method comes from. When a reviewer asked a customer for the individual test cases behind a pentest, the test case list became a standing output. When a reviewer rejected a deferred finding and pointed to the vendor's recommendation as the fix, prescriptive remediation written past the pentest report became a standing activity. And the request for a vulnerability management plan, with evidence that it was being followed, is why continuous verification and annual testing became the

program. This paper walks the five deficiencies that matter most, maps every testing activity in a subscription to the FDA requirement it evidences, and then pairs the long tail of documentation deficiencies with the artifact that closes each.

1. Where the method comes from

ELTON's activities were written backwards from FDA feedback. The deficiency wording quoted in this paper was taken from cybersecurity submissions ELTON has worked through, restated plainly, and paired with the artifact that answered it. Each answer that worked became part of every subscription after it, traced to the requirement it evidences, so the next customer's submission already carried it.

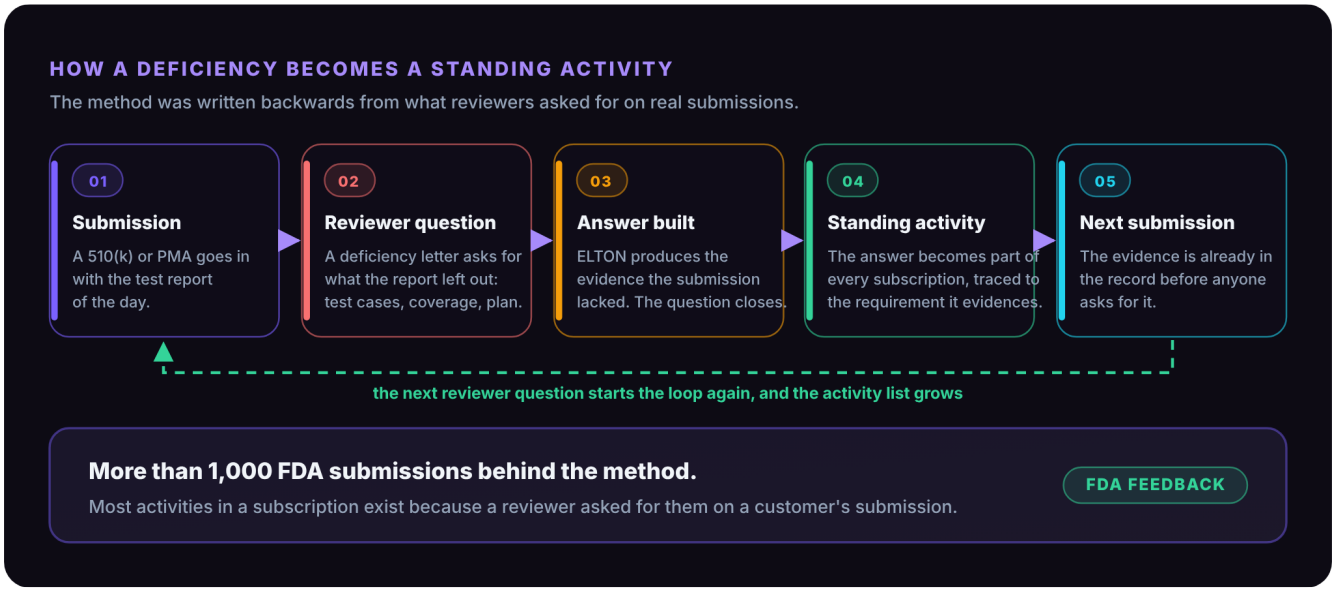


Figure 1. How a deficiency becomes a standing activity. A reviewer question on one customer's submission is answered, the answer becomes an activity in every subscription, and the next submission carries the evidence before anyone asks for it.

The loop has run for 13 years, across more than 1,000 FDA submissions and 10,000 device tests, and the activity list is the residue. Two things follow. The activities are specific to what reviewers actually ask for, which is narrower and more concrete than a reading of the guidance would produce. And the list keeps growing, because reviewers keep asking new questions. The interface-by-interface V&V request in Section 2 arrived in January 2026 and was a standing activity within the quarter.

2. The five deficiencies that matter most

2.1 "Deferred" is not an accepted answer

The most common deficiency ELTON sees: a third-party penetration test report with findings marked "deferred." FDA rejects the deferral outright.

> *"You provided the third-party penetration test report which identifies multiple security findings. You state that these findings are 'deferred.' However, these findings pose a security risk that should be mitigated to ensure patient safety*

> *from device tampering. Adequate authentication, authorization, and code, data, and execution integrity controls are required under Section 524B(b)(2) of the FD&C Act. Please revise these controls based on the concerns in the tables below." What FDA writes*

Read plainly: FDA will not accept a justification for leaving pentest findings unfixed, and a risk assessment that defers them is not enough. Then, on the fix, the Agency points at the pentest vendor's own recommendation:

> *"The Agency concurs with ELTON's feedback to remediate the issue. In your future 510(k) submission, please address this vulnerability as recommended in the penetration test report." What FDA writes*

The trap is that pentest recommendations are high-level and often incomplete, so "fixed per the report" can still be wrong. ELTON generates prescriptive remediation from its own test cases, down to the code fix and past what the pentest report says, so the mitigation holds and the retest proves it. The activity: prescriptive remediation, with exploitability classification deciding what must be fixed now.

2.2 Interface-by-interface test cases, or a justification

The second most common deficiency: verification and validation that does not cover the electronic interfaces, mechanism by mechanism.

> *"The verification and validation testing for the electronic interfaces on the device has not been adequately addressed. For example, you did not provide complete V&V test results for interface-specific security mechanisms, including: (a) USB-C: malware protection, unauthorized device rejection, and data-integrity verification during transfer; (c) Wi-Fi/Bluetooth: verification that wireless capabilities cannot be reactivated through firmware exploitation or physical access. Please provide adequate V&V for the electronic interfaces, or an acceptable justification for the omission." What FDA writes*

Per the verification and validation sections of FDA's guidance on interoperable medical devices, every interface needs evidenced test results, scaled to its risk. Since January 2026 ELTON derives interface-specific test cases from the device's digital twin, executes them at the deepest available tier, and records pass or fail with evidence for each mechanism, so the interface V&V FDA asks for exists as a list of executed test cases. The activities: threat-model-driven test case creation and test case traceability to design.

2.3 A postmarket vulnerability management plan, or a deficiency

FDA increasingly asks how you will keep monitoring the product after it ships. A vulnerability management plan is required under Section 524B.

> *"You provided cybersecurity documentation for the product, but you did not elaborate on how you intend to continuously monitor the product's cybersecurity in the postmarket phase, nor did you provide a vulnerability management plan. A vulnerability management plan is required under Section 524B of the FD&C Act. As referenced in the premarket guidance under Total Product Lifecycle Management (TPLM), the manufacturer is expected to describe how vulnerabilities will be identified, assessed, and remediated across the device's supported lifetime, including monitoring of the SBOM against newly disclosed vulnerabilities and periodic security testing. Please provide a vulnerability management plan and describe your continuous monitoring and disclosure processes." What FDA writes*

What the reviewer is after is evidence that the security program does not end at clearance: a named function, a cadence, and a paper trail that shows monitoring and remediation continuing through the device's supported life. ELTON operates that function as a managed program. It monitors the device's SBOM against new CVEs, re-analyzes exploitability on the current release twin, runs annual penetration testing, and produces the plan itself along with the ongoing evidence that it is being followed, mapped to scope and controls. The activities: continuous vulnerability verification and annual testing, postmarket.

2.4 Evidence of testing across the whole product, with its history

A pentest that covers only part of the device does not satisfy the Secure Product Development Framework. FDA wants complete, historical evidence of how the product was tested and managed during development.

> *"You provided a penetration testing report that contains a subset of findings. Please provide evidence of testing for all in-scope components and any historical testing performed during development, as well as how those vulnerabilities were managed." What FDA writes*

The Agency then asks for all historical testing reports that substantiate comprehensive and complete testing during development. ELTON tests every in-scope component from the digital twin and retains the full history, each test case, result and disposition across releases, so the complete and historical evidence the SPDF requires is already assembled and traceable instead of reconstructed under a deadline. The activities: a digital twin of each release and iterative testing, premarket.

2.5 Regular penetration testing after release

A postmarket plan without recurring testing draws a deficiency of its own. FDA expects testing that keeps pace with the threat landscape.

> *"You provided a postmarket vulnerability management plan that does not include regular penetration testing. Regular third-party penetration testing is recommended to keep pace with evolving threats and to identify new vulnerabilities, alongside validation of reported and SBOM-related issues."*
> *What FDA writes*

ELTON runs penetration testing on every release and at least annually as part of the subscription, validating reported findings and SBOM-derived issues on the real device, so the recurring testing FDA requires is continuous rather than a scramble before the next submission. The activity: annual testing, postmarket.



Figure 2. The five that matter most, and the activity that answers each. Every one of them traces to a section of the statute or the premarket guidance, and every one is a standing part of a subscription.

3. Every ELTON testing activity, traced to FDA

The table maps every activity in a subscription to the requirement it evidences and to where that requirement is written. Section numbers for the premarket guidance follow the current final guidance; the postmarket guidance is FDA's 2016 Postmarket Management of Cybersecurity in Medical Devices; QMSR is 21 CFR Part 820 incorporating ISO 13485:2016.

INCLUDED ACTIVITY	WHAT FDA ASKS FOR, AND WHERE IT IS WRITTEN	WHAT ELTON DELIVERS
Iterative testing, premarket	Cybersecurity testing through development, with the reports in the submission: security requirements testing, threat mitigation testing, vulnerability testing and penetration testing. Premarket guidance, Section V.C Cybersecurity Testing; Section 524B(b)(2), processes that give reasonable assurance the device is cybersecure.	Every premarket release is tested through to final, results land on the digital twin, and the submission-ready report is regenerated on demand.
Annual testing, postmarket	Testing repeated at regular intervals after release, annually in the guidance's own example, as part of the postmarket cybersecurity plan. Premarket guidance, Section V.C and the cybersecurity management plan; Section 524B(b)(1), the plan to monitor, identify and address postmarket vulnerabilities.	The supported release is tested once a year on the real device, and the living report stays current between tests.
Continuous vulnerability verification (exploitability determination)	Monitor for new vulnerabilities after release and assess the exploitability of each one before deciding what it means for the device. Section 524B(b)(1); Postmarket guidance, Section VI.A, assessing the exploitability of the cybersecurity vulnerability.	New CVEs are correlated with the twin and the test results, then verified at the twin, in code or firmware, and on the device, so each one resolves to Affected or Not Affected with evidence.
MDDT-qualified vulnerability severity ratings	An exploitability-based cybersecurity risk assessment, with CVSS applied the way FDA qualified it for medical devices. Premarket guidance, security risk management and cybersecurity risk assessment; Postmarket guidance, Section VI.A (CVSS as an exploitability tool); the Rubric for Applying CVSS to Medical Devices, qualified under the MDDT program (Q171974).	Product-adjusted CVSSv3 and CVSSv4 for every finding through the MDDT-qualified rubric, each rating evidenced against the twin's security profile.
Digital twin of each product release	Security architecture views for the release and an SBOM of commercial, open-source and off-the-shelf components. Premarket guidance, security architecture and third-party software components (SBOM); Section 524B(b)(3).	A twin per release: components, interfaces, data flows, assets, trust boundaries and countermeasures, with software and hardware materials exportable as CycloneDX.
Threat-model-driven test case creation	A threat model that informs the risk assessment and the test plan, so what gets tested follows from how the device can be attacked. Premarket guidance, threat modeling under security risk management; Section V.C, threat mitigation testing.	Test cases are generated from the twin's components and their EMB3D properties, so coverage reads as a list before testing starts.
Test case traceability to design	Traceability from security requirements and design controls to the tests that verified them, kept in the design history file. Premarket guidance, Section V.C and its submission documentation; QMSR, 21 CFR Part 820 incorporating ISO 13485 clauses 7.3.3 and 7.3.6, design inputs and design verification.	Every test case maps to the twin component and the control it exercises, and the matrix exports with the report.

INCLUDED ACTIVITY	WHAT FDA ASKS FOR, AND WHERE IT IS WRITTEN	WHAT ELTON DELIVERS
Vulnerability traceability to test cases	Findings tied to the tests that produced them, including a security assessment of unresolved anomalies. Premarket guidance, Section V.C test reports and the security assessment of unresolved anomalies.	Every finding links to its test case, its evidence and its component, so a reviewer can walk from the vulnerability back to the test.
Exploitability classification: directly exploitable, conditionally exploitable, weakness	Decide whether the risk is controlled or uncontrolled from exploitability and severity of patient harm, and separate known unacceptable vulnerabilities from critical ones. Postmarket guidance, Sections VI and VII, controlled and uncontrolled risk; Section 524B(b)(2)(A) and (B).	Three verdicts on every finding, and a VEX-aligned disposition with CISA-defined justifications for everything dismissed.
Prescriptive remediation	Updates and patches on a regular cycle for known unacceptable vulnerabilities, out of cycle for critical ones, with corrective and preventive action under the quality system. Section 524B(b)(2)(A) and (B); Postmarket guidance, Section VII Remediating and Reporting; QMSR, ISO 13485 clauses 8.5.2 and 8.5.3.	One fix per root cause, tied to the chain it closes, written for the developer who ships it and tracked to Fixed in a later release.
Mitigation prioritization	Risk-based remediation: what to fix first, on what timeline, by the risk it carries to patients. Postmarket guidance, Section VII; Section 524B(b)(2).	Root causes ranked by the exploitable chains they close, with mean time to triage and mean time to remediation tracked across the program.

ELTON meets FDA premarket (Section 524B) and postmarket cybersecurity vulnerability testing and management requirements. The rubric is FDA-qualified under the MDDT program; the ratings and dispositions are ELTON's, evidenced against your product.

4. The documentation deficiencies

Beyond the five above, a long list of documentation deficiencies recurs. Each pairs a reviewer request with what ELTON produces from the same digital twin. The first group concerns the controls FDA expects you to prove.

FDA ASKS	ELTON PRODUCES
Threat modeling: your device is a cyber device under 524B(c) but you did not provide threat modeling. Provide a model assessing assets, threats, vulnerabilities and controls, with a justified methodology (STRIDE, attack trees, kill chain), all end-to-end elements, and architecture or sequence diagrams.	A digital twin built from the SBOM, vulnerabilities and architecture, with threat modeling layered on it: exploitable-path analysis, vulnerability chaining, and mitigations with traceability across assets and controls.
Authorization controls: you reference privilege levels but do not describe them or how permissions are granted and controlled. Define each role's privileges and the authentication tied to each level.	Testing identifies weaknesses in privilege boundaries and links findings back to roles and controls, creating traceable evidence of compliance.

FDA ASKS	ELTON PRODUCES
Confidentiality controls: you reference TLS/SSH and asymmetric encryption but do not detail them or where they are implemented; some TLS/SSH versions are insecure. Describe the controls and justify the algorithms.	Outdated cryptographic libraries and configurations flagged, implementation confirmed by testing, and results tied back to scope and confidentiality controls.
Integrity controls: you reference TLS, SSH and checksums but do not describe how integrity is enforced; non-cryptographic checksums are not integrity controls. Describe and justify the integrity controls.	Confirmation of whether integrity protection is cryptographic and effective, with findings linked directly to the integrity controls in scope.
Device hardening: USB and external ports are enabled but you did not describe default hardening. Remove default passwords, disable unused services, restrict interfaces, and provide hardening measures and testing.	Exposed interfaces, default accounts and unused functionality tested, with results linked to the system architecture and controls for FDA-ready traceability.
Event detection and incident response: your device relies on networking but you did not provide detection, response and recovery. Describe the incident response plan and provide testing of its effectiveness.	A managed product security operations function: when a vulnerability hits a release, the manufacturer is alerted to act and notify affected customers, which is the detection, response and recovery the reviewer asks to see.
Antivirus and malware protection: your OS supports antivirus and anti-malware. Detail the protections implemented, or justify why they are unnecessary.	Unsupported or unprotected OS components highlighted, with test results confirming mitigation and linking back to system-level controls.

The second group concerns testing rigor, the SBOM and the full device lifecycle. ELTON produces each as a traceable artifact.

FDA ASKS	ELTON PRODUCES
Cybersecurity testing: your testing documentation is a summary rather than a full report. Provide tester independence and expertise, scope, duration, methods, results, findings and observations.	Penetration testing, fuzzing, and static and dynamic analysis in premarket and annual evaluations, with methodology, scope and results documented and each finding traceable to risks and controls.
Cybersecurity controls documentation: your risk-to-control traceability table lacked control details. Provide documentation on the controls implemented.	Controls substantiated by linking vulnerabilities and test results to control objectives, with test cases mapped, for full traceability.
End-of-life software components: your SBOM lists components past their end-of-support date. Provide assurance of continued maintenance or upgrade to supported versions.	SBOM components monitored against lifecycle data, end-of-life vulnerabilities flagged, and risk impacts shown tied to scope.
Updateability and patchability: you marked these inapplicable with only a high-level justification. Provide a detailed justification or the views.	Patchability findings tied to vulnerabilities and controls, mapped to scope, to support the required documentation.

FDA ASKS	ELTON PRODUCES
Expanded threat model detail: your threat model did not identify device risks and mitigations, hostile-network assumptions, supply-chain or interoperability risks, or all end-to-end elements.	The twin's outputs expanded to include hostile assumptions, supply-chain risks and interoperability findings, each mapped to scope and controls.
SBOM format: your SBOM could not be opened or was not machine-readable. Provide CycloneDX consistent with the NTIA minimum elements.	Software and hardware materials ingested into a living, validated CycloneDX SBOM, with findings traceable to SBOM entries, vulnerabilities and scope.
Cybersecurity risk management report: your report lacked a separate security risk assessment and the outcomes of threat modeling, SBOM, vulnerability and anomaly reviews, with no cross-document traceability.	Findings integrated into a cybersecurity FMEA summarizing vulnerabilities, risks and mitigations, with full traceability to scope and controls.
Software description: you did not provide a comprehensive software or firmware description.	SBOM-based findings aligned with the software description, with traceability back to testing and scope.
Software bug and patch: you identified a bug and proposed a patch but omitted documentation of the bug, the patch and regression testing.	Remediation and regression evidence captured, with new test results evidencing closure, linked to scope and controls.
Continued support: you did not detail how you will monitor and address vulnerabilities post-deployment, including end-of-life planning.	SBOMs monitored for new vulnerabilities, with traceable outputs showing the evolving risk posture.
Coordinated vulnerability disclosure: you did not provide adequate CVD information or how users are notified of critical vulnerabilities.	Vulnerability findings traceable to disclosure workflows, so FDA can see how risks are identified and communicated.
Patch release timelines: you did not provide patch release timelines, including for critical updates. Justify patch cycles and critical handling.	Vulnerabilities prioritized by exploitability and severity, with findings linked to patchability controls to justify timelines.
Labeling: you did not provide cybersecurity labeling: interfaces, update instructions, antivirus requirements, incident-response guidance, SBOM information and infrastructure dependencies.	The activities that inform customers of product impact, automated, with the appropriate responsibilities carried from manufacturer to customer.

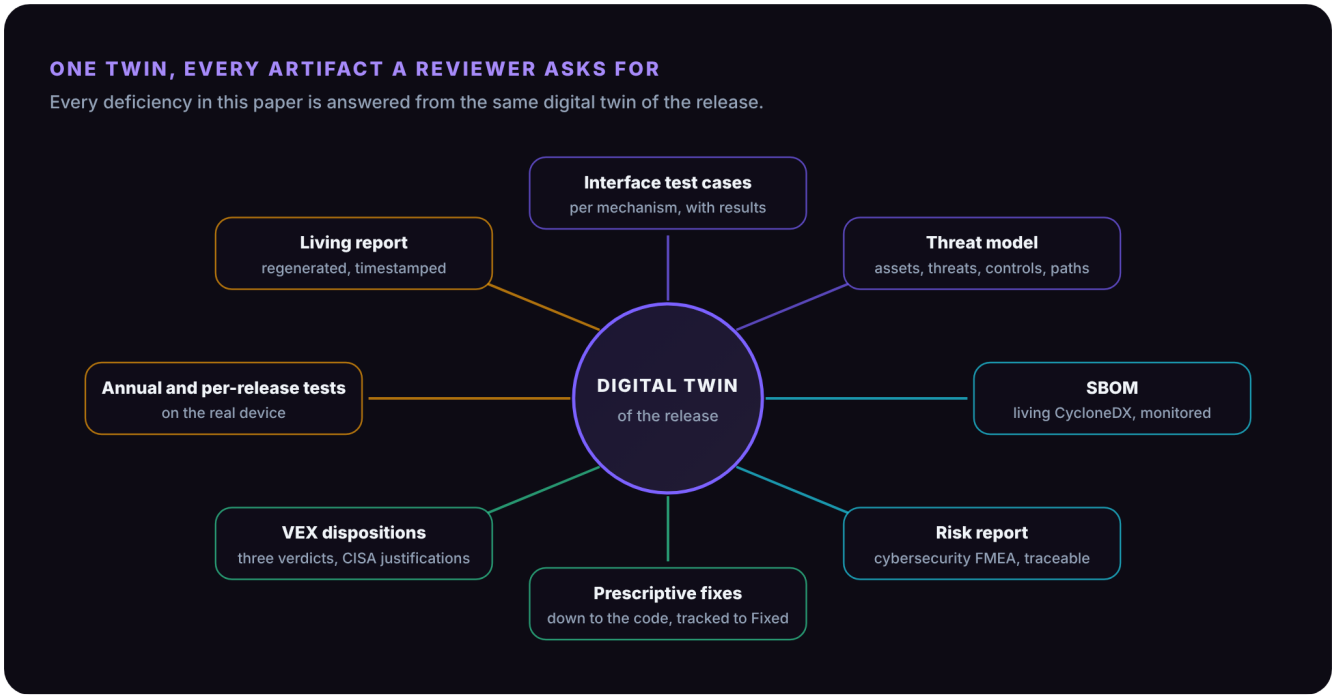


Figure 3. One twin, every artifact a reviewer asks for. Every artifact in this paper is derived from one digital twin of the release, so they stay consistent with each other and with the device.

5. One platform, every deficiency

Every deficiency in this paper traces back to the same root. Legacy testing produces findings and advice, with no evidence behind them, and it stops at clearance.

From a single digital twin, ELTON derives interface-by-interface test cases, executes them at the deepest available tier, generates prescriptive remediation down to the code fix, and layers the threat model, SBOM and risk report on top, with traceability from CVE to determination that FDA and EU reviewers can follow. It runs as a continuous managed program, so the pentest, the test cases, the threat model, the SBOM and the remediation stay current together.

A deficiency is prevented by producing the evidence before the reviewer asks for it, and the subscription has it on record the day the submission goes in.

FDA, Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submissions, final guidance, Docket FDA-2021-D-1158, Sections V and V.C. FDA, Postmarket Management of Cybersecurity in Medical Devices, final guidance, December 2016, Sections VI and VII. Section 524B of the Federal Food, Drug, and Cosmetic Act. QMSR, 21 CFR Part 820 incorporating ISO 13485:2016. The Rubric for Applying CVSS to Medical Devices, MDDT-qualified (Q171974). ELTON, eltoncyber.com/fda-deficiency-explainer and eltoncyber.com/fda-deficiency-guide. Reviewer wording in quotation marks is reproduced from FDA deficiency letters on submissions ELTON has worked through, with product identifiers removed.

About ELTON. ELTON is the exploitability management platform for medical devices, delivered as a managed program. ELTON builds a digital twin of each device, runs the pipeline across firmware, protocols, and real hardware every release, verifies which findings are exploitable on the device, and evidences every finding and every dismissal for regulatory review. ELTON meets FDA premarket (Section 524B) and postmarket cybersecurity vulnerability testing and management requirements. Talk to us at **eltoncyber.com**.