PCCP Beyond AI/ML

Reviewer Rejection & Corrective-Action Checklist

For cybersecurity, firmware, SBOM, and hardware-scoped Predetermined Change Control Plans submitted under FDA's December 4, 2024 final guidance and Section 524B.

How to use this checklist. Red-team every draft PCCP against the 20 items below before submission. Each item lists the reviewer's objection, the root cause, and the corrective action. If any item cannot be answered "yes" with a document reference, fix the language before you submit — not after the Additional Information (AI) request.

1. Description of Modifications (DoM)

#	Reviewer objection	Root cause	Corrective action
■	Unbounded language ('as needed', 'as appropriate', 'per current practice')	Reviewer reads as unlimited delegation.	Replace with enumerated modification classes and quantitative bounds (e.g., 'signed firmware releases within features A/B/C on the update channel validated in Section X').
■	Multiple modification classes bundled under one DoM entry	Reviewer cannot assess safety impact per class.	Split DoM into one entry per class: crypto agility, SBOM refresh, firmware OTA, hardware substitution, non-AI algorithm tuning.
■	DoM references SOPs without inlining the bounds	SOP contents are not part of the authorized submission.	Inline the specific parameters (semver ranges, cipher suites, parameter min/max) directly in the DoM.
■	DoM includes changes that expand the attack surface analyzed in the threat model	Changes exceed what the risk file supports.	Move those changes out of the PCCP; route via new submission or supplement.

2. Modification Protocol (MP)

#	Reviewer objection	Root cause	Corrective action
■	Single generic MP covering all modification classes	Reviewer treats as unbounded delegation.	Write one MP per DoM class with class-specific verification methods and pass/fail criteria.
■	No pass/fail acceptance criteria	Reviewer cannot judge when a change is authorized to ship.	Add explicit numeric or boolean criteria per test (KAT vector results, interoperability matrix, regression suite pass).

#	Reviewer objection	Root cause	Corrective action
■	No rollback / abort criteria	Field safety net is undefined.	State exactly when a modification is pulled back, what happens to fielded units, and who authorizes the rollback.
■	Validation approach not tied to the security risk file / threat model	Reviewer cannot trace protocol to analyzed hazards.	Cross-reference each MP test to the specific threat model entry or IEC 81001-5-1 activity it validates.
■	No change-log / record requirements per executed modification	Postmarket inspectors have nothing to audit.	Require an executed record per modification: test results, refreshed SBOM/VEX, threat model delta, PCCP change log entry.

3. Impact Assessment (IA)

#	Reviewer objection	Root cause	Corrective action
■	Narrative paragraph without per-class analysis	Reviewer sees policy, not analysis.	Restructure IA as a table: modification class x (safety, effectiveness, cybersecurity, usability) impact + mitigation.
■	IA does not cite the threat model or security risk file	Impact claims are unsupported.	Cite the specific threat model IDs and risk file sections that bound each modification class.
■	IA does not address benefit-risk of the pre-authorization itself	Reviewer questions why a PCCP vs case-by-case.	Add a paragraph on why pre-authorization is safer and faster than per-instance letter-to-file for this cadence.

4. Section 524B Postmarket Interlock

#	Reviewer objection	Root cause	Corrective action
■	Postmarket cybersecurity plan does not name the PCCP as the closure mechanism	Two disconnected workstreams.	Add explicit reference from the postmarket plan to the PCCP by document name and section.
■	PCCP does not reference the postmarket monitoring / vulnerability handling process	PCCP appears to bypass 524B(b)(2)(B).	Add cross-reference from PCCP into the postmarket plan and the SBOM/VEX workflow.
■	SBOM/VEX workflow does not route in-scope findings into the PCCP	No operational path from vulnerability to fix.	Document the routing rule in the postmarket plan: in-scope --> PCCP MP execution; out-of-scope --> CAPA.
■	Cybersecurity management plan does not tie both documents into the QMSR	QMS integration missing.	Update the cybersecurity management plan to name the PCCP, postmarket plan, and CAPA as one loop.

5. eSTAR Placement & Cross-References

#	Reviewer objection	Root cause	Corrective action
■	PCCP attached without cross-references from cybersecurity content	Reviewer cannot locate the linkage.	Reference the PCCP by attachment name from the cybersecurity management plan, threat model summary, and postmarket plan.
■	Impact Assessment does not cite threat model IDs	Boundaries unclear.	Add explicit threat model ID citations per modification class.
■	No version control on the PCCP itself	Change history invisible.	Add a version table on the PCCP first page with revision, date, author, summary of change.
■	Missing statement that modifications outside PCCP scope still trigger letter-to-file or new submission	Reviewer suspects scope creep.	Add a bounding statement explicitly reserving out-of-scope modifications for existing change-control pathways.

Governing References

- FDA, *Predetermined Change Control Plans for Medical Devices* — final guidance, December 4, 2024.
- FDA, *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions* — final guidance, February 3, 2026.
- FD&C Act Section 524B(b)(2)(B) — postmarket cybersecurity plan requirement.
- AAMI TIR57:2016/(R)2023 — Principles for medical device security risk management.
- AAMI SW96:2023 — Security risk management for medical device software.
- IEC 81001-5-1:2021 — Security activities in the product lifecycle.
- ISO 14971:2019 — Application of risk management to medical devices.

Reviewer Red-Team: Final 5 Questions Before Submission

1. Can every DoM entry be answered with a bounded numeric or enumerated specification?
2. Does each MP have explicit pass/fail criteria and a rollback rule?
3. Does the postmarket cybersecurity plan name the PCCP by document reference?
4. Does the SBOM/VEX workflow route in-scope findings into the PCCP and out-of-scope findings into CAPA?
5. If a reviewer read only the PCCP and the postmarket plan, would they see one loop or two disconnected documents?