MEDICAL DEVICE CYBERSECURITY & REGULATORY ENGINEERING

Securing the future *of connected medicine.*

ATOM is an independent cybersecurity and engineering advisory firm specializing in medical device cyber testing, risk management, Secure Product Development Frameworks (SPDF), and regulatory premarket clearance for cyber devices.

LIFECYCLE CYBERSECURITY FOR CONNECTED DEVICES

- **510(k), De Novo & PMA clearance**
- **Class I, II & III connected devices**
- **Section 524B of the FD&C Act**
- **Secure Product Development Frameworks**

FROM ARCHITECTURE TO SUBMISSION

Cybersecurity That Keeps Clearance Moving

It's our job to help manufacturers move through 510(k), De Novo, and PMA clearance without cybersecurity becoming the reason for an RTA, unnecessary engineering rework, or prolonged rounds of interactive questions.

With Section 524B of the FD&C Act and FDA cybersecurity guidance establishing specific cybersecurity expectations for cyber devices, security must be addressed throughout product design, testing, submission, and postmarket support.

ATOM works alongside your engineering, regulatory, and quality teams to address those requirements, from early architecture and threat modeling through verification, penetration testing, and submission-ready documentation.

PROVEN FDA EXPERIENCE

ATOM has guided dozens of medical devices through FDA clearance and provides lifecycle cybersecurity engineering for Class I, Class II, and Class III connected devices.

Schedule your free consultation.

Email **info@theatomgroup.com**

INTEGRATED WITH YOUR SPDF

Built to Fit Into Your Quality System

ATOM integrates directly into your SPDF. We can help develop, review, or test the cybersecurity elements required under Section 524B, whether you are designing a new device, preparing an existing product for submission, or strengthening your manufacturing and postmarket controls.

Postmarket Monitoring & Patching Plans

Comprehensive procedures for coordinated vulnerability disclosure (CVD), CISA Known Exploited Vulnerabilities (KEV) tracking, and defined regular vs. out-of-cycle critical patch deployment timelines.

Reasonable Assurance of Cybersecurity

Design, verification, and validation evidence demonstrating that security controls address reasonably foreseeable misuse and intentional exploitation.

Software Bill of Materials (SBOM)

Machine-readable SBOMs incorporating NTIA baseline attributes, component supportability information, and vulnerability assessments.

SUBMISSION-READY CYBERSECURITY DOCUMENTATION

Documentation Without the Scramble

ATOM develops submission-ready cybersecurity documentation tailored to the device and its risk profile.

Traceable Threat Modeling & Threat Analysis based in requirements

Threat modeling during early design or post-hoc validation using recognized methodologies, including STRIDE and MITRE ATT&CK for ICS/Healthcare.

Submission-Ready Cybersecurity Documentation and Reporting

Controlled documentation designed for inclusion in your quality system and regulatory submission, with supporting documentation maintained throughout the product lifecycle.

Cybersecurity Risk Assessment

Unlike traditional ISO 14971 safety risk assessments that calculate probabilistic harm, ATOM's Cybersecurity Risk Assessment uses a non-probabilistic, exploitability-driven methodology. We evaluate the technical feasibility of exploitation, evaluate pre- and post-mitigation residual risks, establish clear acceptance criteria, and bridge security risks into your ISO 14971 safety risk files when exploitation could lead to direct or indirect patient harm.

Master Traceability Matrix

ATOM works with you to build an end-to-end Cybersecurity Traceability Matrix mapping every security requirement to its corresponding Threat Model entry, Risk Assessment line item, Architecture View element, SBOM component, and Verification/Validation (V&V) Test Execution Record.

TESTED UNDER ADVERSARIAL CONDITIONS

Penetration Testing for Connected Medical Devices

ATOM's ethical hackers and software engineers test medical devices in controlled environments to evaluate whether cybersecurity controls operate as intended under adversarial conditions. From standardized testing, to custom hardware testing modules, no job is too complex. Our team has been part of dozens of successful submissions across some of the largest names in medical device manufacturing today. In the ever changing landscape of cyber requirements, its critical to have a cyber partner that knows how to successfully clear devices.

Hardware & Debug Port Testing

UART & Serial Interface Probing

Testing for interactive shell access, root privilege escalation, and unauthenticated bootloader access.

JTAG / SWD Boundary Scan Testing

Testing debug interfaces to verify they are cryptographically locked or physically disabled in production hardware.

Firmware Extraction & Readout Protection

Testing internal flash memory protections against unauthorized extraction through physical interfaces.

Wireless & RF Testing

Bluetooth & BLE Security

Assessment of pairing mechanisms, key exchange, custom GATT services, spoofing, and relay attacks.

Custom RF & Sub-GHz Testing

Analysis of proprietary wireless protocols for replay vulnerabilities, missing cryptographic nonces, and unencrypted telemetry.

Magnetic Inductive & NFC Testing

Validation of short-range signal-of-intent mechanisms used in implantable device programming.

RF Interference & Resiliency

Testing against RF jamming, packet corruption, excessive band noise, and denial-of-service conditions to evaluate the continued availability of critical clinical functions.

System-Level Penetration Testing & Fuzzing

INDEPENDENT THIRD-PARTY TESTING

ATOM provides independent third-party penetration testing with reporting designed to support FDA submission requirements, including tester independence, methodology, duration, and findings.

Black Box & White Box Testing

Testing from both an external attacker perspective and a privileged position with access to source code and system information.

Protocol & Binary Fuzzing

Malformed, unexpected, and high-rate inputs introduced through ports, wireless channels, and API endpoints to evaluate system stability and memory safety.

Vulnerability Chaining

Testing whether multiple lower-level implementation weaknesses can be combined to escalate privileges or bypass safety controls.

Static & Dynamic Code Analysis

Analysis for hardcoded credentials, insecure cryptographic implementations, buffer overflows, and Common Weakness Enumeration (CWE) patterns.

ACROSS THE PRODUCT LIFECYCLE

Working Alongside Your Teams

Architecture & Threat Modeling
Security addressed from early design

→

Verification & Pen Testing
Controls tested as intended

→

Submission Documentation
Ready for 510(k), De Novo & PMA

→

Postmarket Support
CVD, KEV tracking & patching

PATHWAYS, STANDARDS & METHODOLOGIES

Referenced throughout our work

510(k) · De Novo · PMA · Section 524B · FD&C Act · SPDF · ISO 14971 · NTIA SBOM · CISA KEV · STRIDE · MITRE ATT&CK · CWE

Securing the Future of Connected Medicine

Talk with ATOM about your device, your submission timeline, and your postmarket cybersecurity obligations.

CONTACT
603-501-0003
info@theatomgroup.com
www.theatomgroup.com