Navigating the FIPS 140-3 Process

Tips for Developers and Integrators

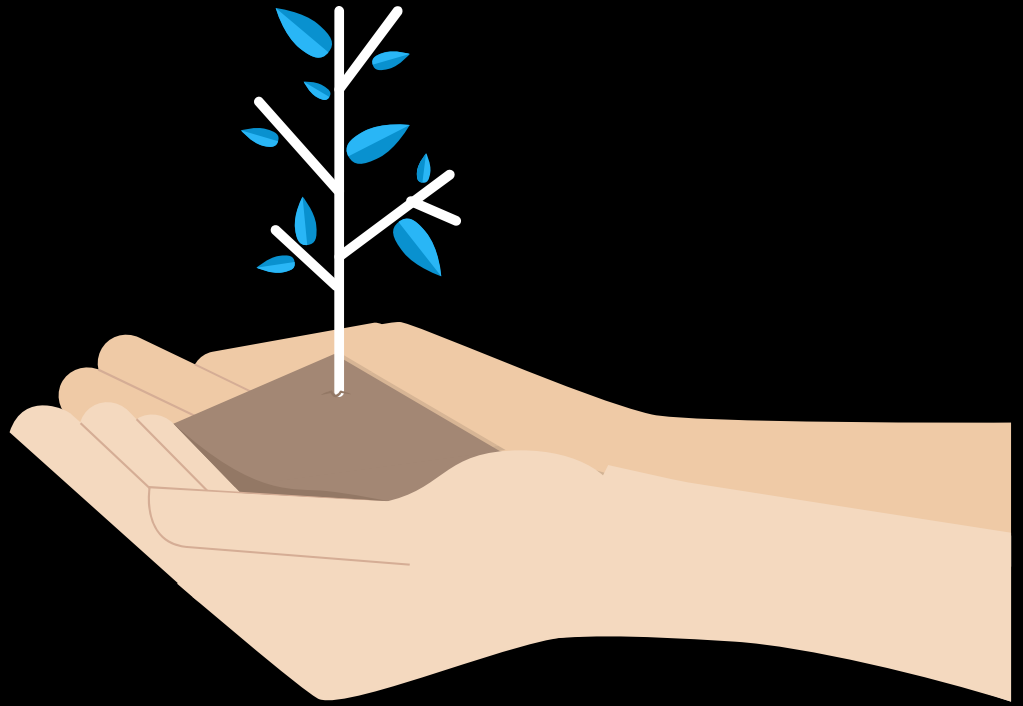
Jason Lawlor
October 2025

Lightship Security

Applus+

AGENDA

- PROGRAM OVERVIEW & STATUS UPDATES
- FIPS 140-3 VALIDATION PROCESS
- COMMON PITFALLS AND PRACTICAL TIPS
- WHAT'S NEXT?



CMVP / FIPS 140-3 KEY ELEMENTS

CMVP

- Joint program by NIST (US) and CSEC (Canada) – Comprised of ~15 people
- 140-3 based on ISCO19790 / SP 800 Series

ESV (Entropy Source Validation)

- Stand alone program under CMVP and prerequisite for full module validation
- Reqs based SP 800-90B

CAVP

- Validation of Approved NIST algorithms (SP 800-140C and 140D)
- Stand alone and pre req for module validation
- Demo Server is free to access, Production needs accreditation

CST's (LABS)

- Accredited by NVLAP and CMVP
- 23 labs worldwide (1st party and full labs)

IUT and MIP

- NIST maintained validation status websites
- Phases: IUT > MIP (Review Pending > In Review > Coordination > Finalization)

MODULE VALIDATIONS

- Generally valid for 5 years
- Publicly listed (NIST)
- Levels 1-4
- Mechanisms to update for module changes, CVEs etc

TIMELINES

- Typical level 1 validation takes ~1 year to complete (queue delays)
- 2-4 months of actual testing time

USE CASES

- Required for US Federal Procurement
- FIPS Certs / ESV / CAVP used in Common Criteria

FUTURE

- Active work on automated testing (ACMVP)
- PQC testing and implementation
- Entropy focus (ESV)

PROGRAM STATS

1

RECENT QUEUE TIMES (COURTESY AWS)

- 2024 measures to ease backlog (provisional certs) didn't significantly decrease timelines

2

IUT STATS

- 243 modules on IUT (Sept 24)
- ~100 unique vendors

3

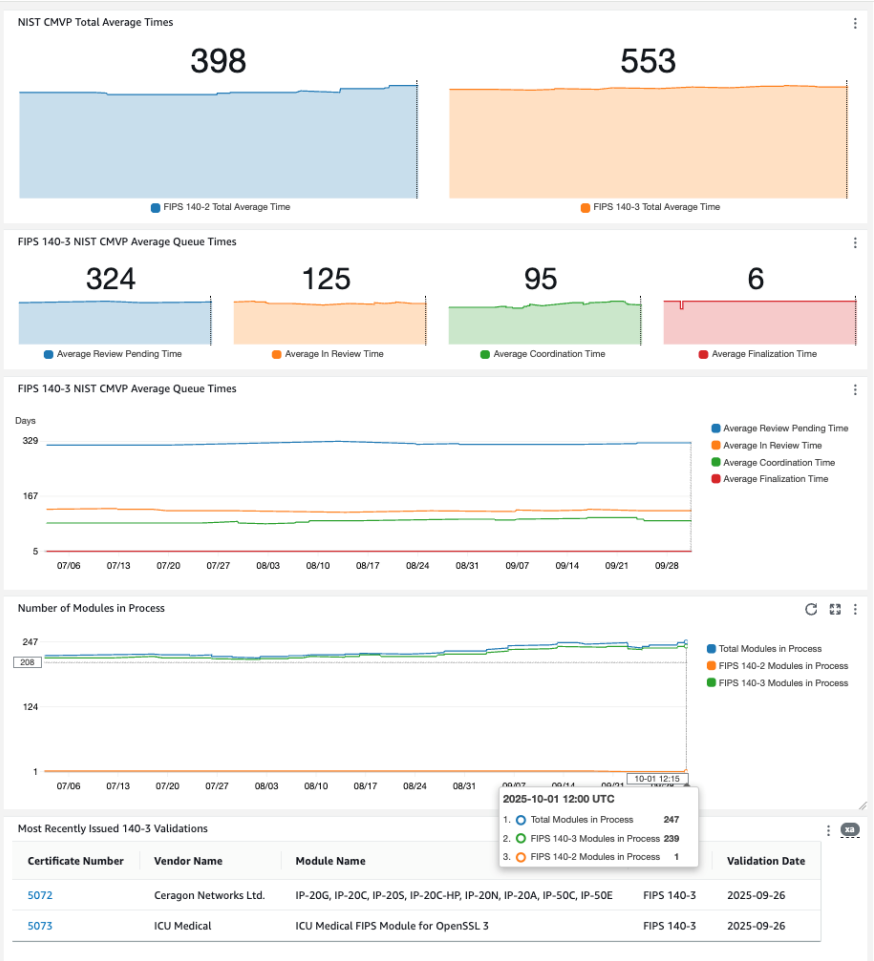
MIP STATS

- 236 modules on MIP (Sept 24)
- Requires payment of NIST CR fee
- 7 validations issued in Aug /Sept

4

PROGRAM NOTES

- Best estimate ~15 resources across the program
- Growing program – shrinking resources
- All FIPS 140-2 certs expire September 22, 2026
- Can no longer submit 140-2 reveals



CMVP

UPDATE TO CSTs

6 MONTH QUEUE BY END 2025

Expedited reviews

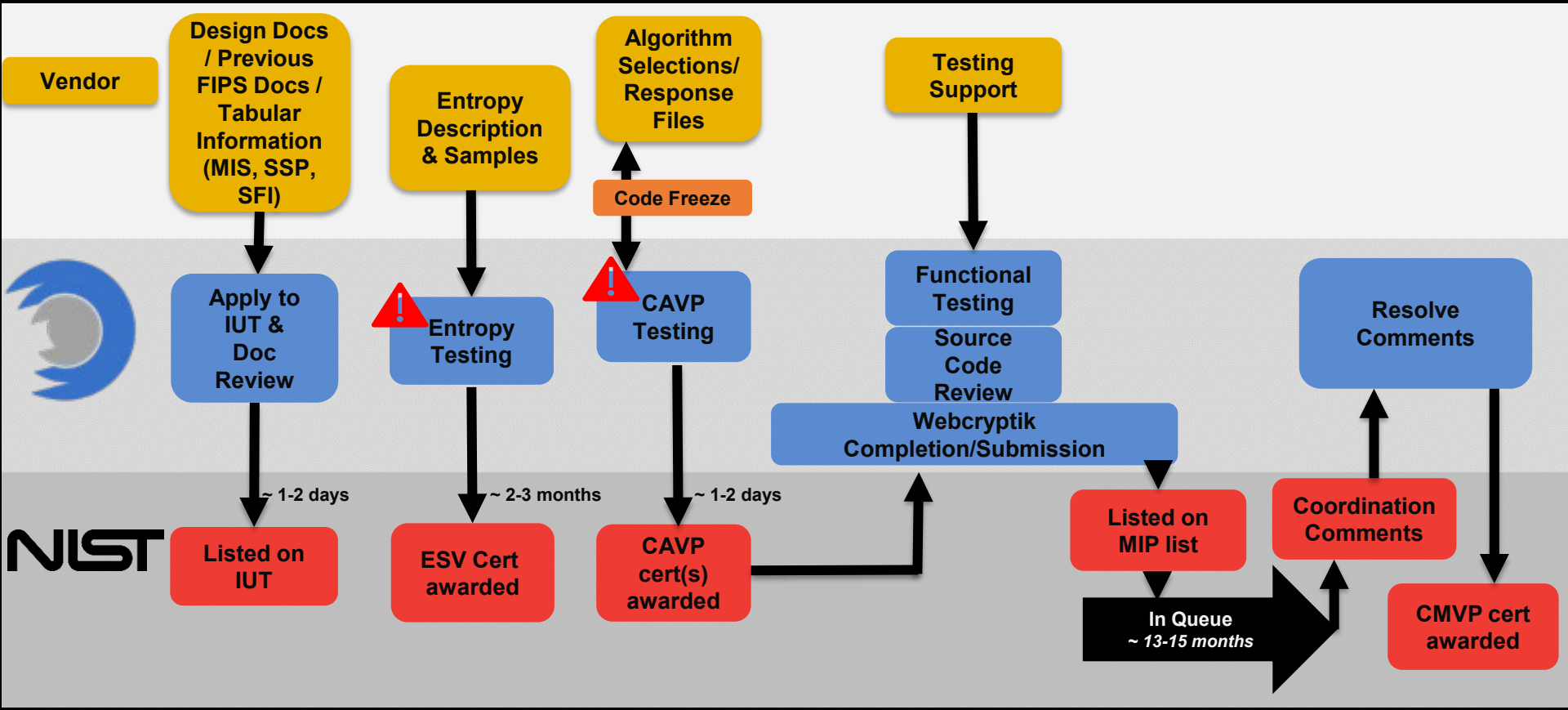
NO QUEUE BY MID 2026

To get queue length down, CMVP is going to do focused reviews on only some modules (level 1 SW etc)

PARTIALLY HIT BY SHUTDOWN

Reviewers are essential, but admin staff is not (paying NIST fees etc)

VALIDATION PROCESS (L1)



SCOPE TO GO FAST (ER)

HIGH RISK ITEMS FIRST - ESV, CAVP

SMALLEST USABLE BOUNDARY

VALIDATION ROADMAP RE-VALS, CVE'S

MAX REUSE OF MODULE BOUNDARY

TOOLING – TEST HARNESS (CAVP AND FUNCTIONAL TESTING)

LEVERAGE OPEN SOURCE / DON'T BLAZE TRAILS / RFGs NOT ALWAYS PRACTICAL

SUCCESS FACTORS

DOCS THAT PASS

- Security Policy aligned to SP 800-140B
- Vendor Evidence templates
- Leverage open source

CVE's

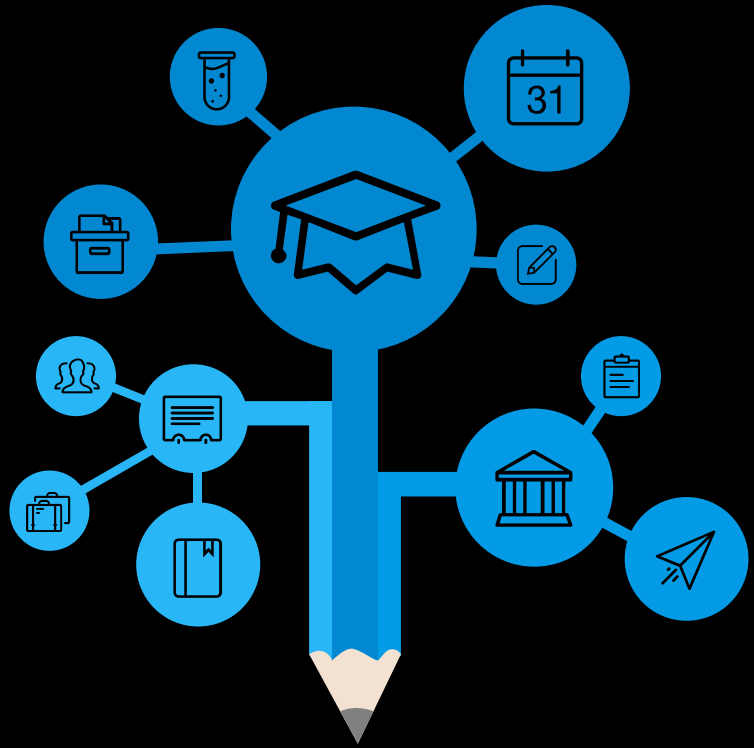
- Disclose applicable CVEs + mitigation plan
- Have a plan on addressing CVEs within validated modules over the 5-year period

PHYSICAL TESTING REQs

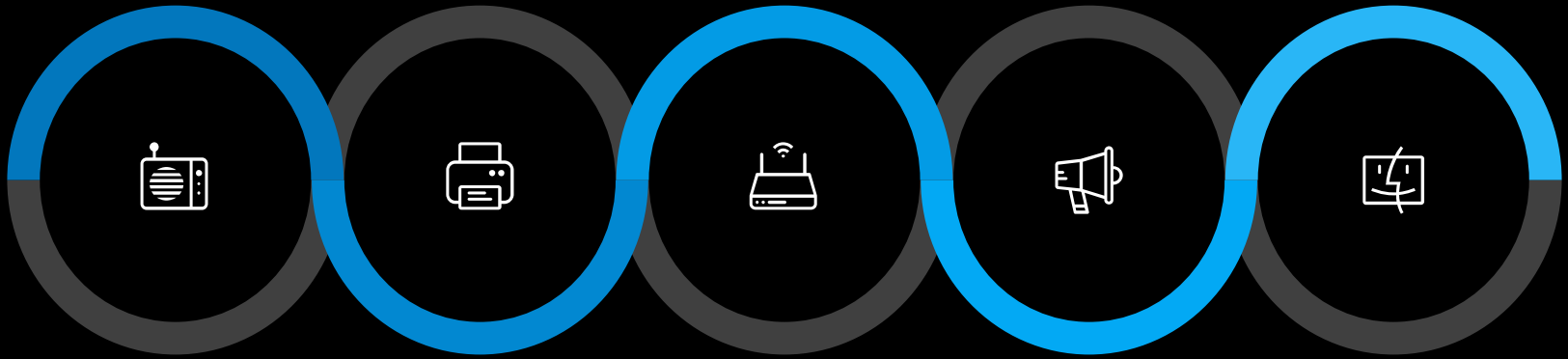
- L2-4 HW modules require physical testing / tamper seals etc.
- Shipping logistics / on site testing etc

3rd PARTY SUPPORT IF REQUIRED

- Access to partner tech / nda's, custom tooling
- Embedded platforms / IP cores etc.



PITFALLS TO AVOID



OE SPRAWL

- Drives cost/effort
- Representative sample OE's
- Vendor affirm

TOOLING

- Test harness for CAVP/ entropy samples
- Access to internals
- Functional testing
- Leverage ACVP demo environment

SCOPE CREEP

- No brownie points for larger scope
- Review competitor approach

PROGRAM TRANSITIONS

- CAVP transitions
- Interim certs
- Program churn
- Upstream programs (ex: CSfC)

NOT LEVERAGING CERT

- Organizational awareness
- Reuse internally / marketed externally

PRACTICAL TIPS AND CONSIDERATIONS

BUILD VS BUY

- Adopt validated OSS modules
- Consider commercially available libraries
- OpenSSL rebrands

INTERNAL / EXTERNAL COSTS

- How much of the process you want to outsource (consulting, docs, etc)
- Lab fees can be significant

OWNERSHIP OF DELIVERABLES

- Ensure access to reports / validation deliverables upon completion.
- Facilitates changing labs and revalidations

NOT EASY

The FIPS 140-3 validation process is highly prescriptive and can be significantly longer and more resource-intensive than expected.

Success hinges on preparation: having a clear understanding of the Cryptographic Module Validation Program (CMVP) structure, aligning early with the latest Implementation Guidance, and building a disciplined documentation trail from the outset.

Vendors should expect that **100% conformance is required**—there is no room for partial compliance or “close enough.”

DE-RISKING

ENGAGE CSTL EARLY

- Gap assessments
- Scope alignment
- Ideally early in product development
- Functional testing prep

CODE FREEZES

- Lock 3rd party versions / algorithm implementations

LAB SELECTION

- Experience, critical mass, availability, tooling
- Accreditation status
- Contractual frameworks etc in place

CAVP AND ESV EARLY

- Leverage demo server to troubleshoot algs
- Entropy story is watertight: collection method, conditioning, and statistical testing

TAKE THE WELL WORN PATH

- Standard scope and implementations reduce risk and validation delays
- Avoid RFGs and nonstandard approaches when possible
- Consider rebranding validated modules (e.g., OpenSSL FIPS provider)

VALIDATION ROADMAP

Plan in advance:

- CVE disclosures, algorithm deprecations, and potential revalidation reqs.

FUTURE LOOKING – AUTOMATION AND ACMVP

NIST's ACMVP initiative to automate review, evidence submission, and rule checks

Goal: reduce manual bottlenecks, improve consistency, shorten review cycles

Divided into three workstreams: Test Evidence, Protocol, Research Infrastructure

Still in prototype / pilot phase; not yet fully operational

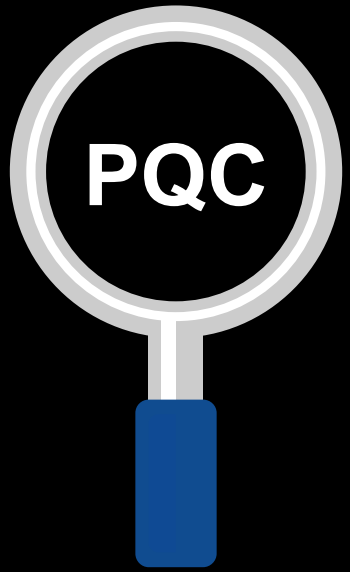
Pilots under way: JSON schemas, automated comment-round processing, API

Designed for vendor & lab integration — aims to support CI/CD pipelines, automated regression testing, and consistent evidence generation across different labs and vendors

EMERGING TRENDS: PQC, HYBRID MODES AND PROGRAM EVOLUTION

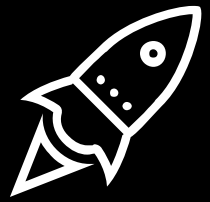
FIPS 140-3 & PQC
PQC algorithms (e.g. ML-KEM, ML-DSA, SLH-DSA) already approved in FIPS 203/204/205 and being integrated into module-level validations

HYBRID MODULES
Hybrid (classical + PQC) combinations are likely to remain common to manage transition risk



IG
Evolving implementation guidance (IG) will serve as de facto additional constraints; modules must keep up

FUTURE THREATS
Expect more demands for side-channel resistance, fault injection resistance, and resilience to quantum-era cryptanalysis, especially in higher security levels



THANK YOU

QUESTIONS?

Info@lightshipsec.com