FIPS 140 Validation Process: Overview and Case Study

Tammy Green – Senior Principal Security Architect, Symantec

Carolyn French – Program Manager, CMVP

Ashit Vora – Co-Founder and Lab Director, Acumen Security

Ian Hall – Certification Architect, Symantec

May 16, 2017

Getting to know you

Vendors?

Attended other workshops?

What is FIPS?

FIPS validation?

T

Why validate?

1 - Get the deal signed

2 – Checkbox requirement

3 – Proven level of security

Images courtesy of TaxCredits.net

FIPS 140: Standard for US and Canada

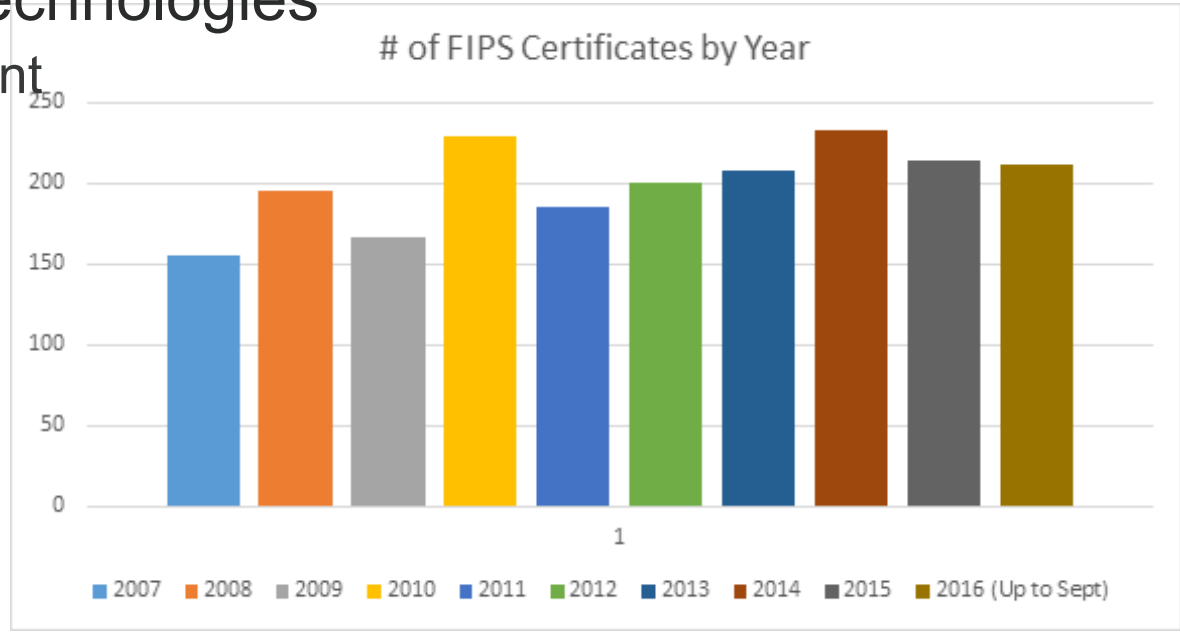
- The Federal Information Processing Standard (FIPS) 140-2 is the **standard** applied to all US Federal agencies that use cryptographic-based security systems to protect sensitive information
  - **US:** The standard is **mandatory for the design and implementation of cryptographic modules** that US Federal departments and agencies operate or have operated for them under contract.
  - **Canada:** Information designated Protected B **should be encrypted by a FIPS 140-2 validated module** running in FIPS mode. Agencies include procurement clauses for any type of Virtual Private Network (VPN), Authentication tokens, or other applications requiring cryptography.

In other words, if you want to sell the US or Canadian governments, get your cryptography FIPS validated

C

If you validate…

- **You will be in good company**
- 500+ companies
  - Almost 3000 products validated
  - Wide variety of vendors and technologies
    - Networking & Telecom Equipment
    - Smart Phones
    - Smart Cards
    - Software Libraries
    - Encrypted Drives
    - HSMs & TPMs



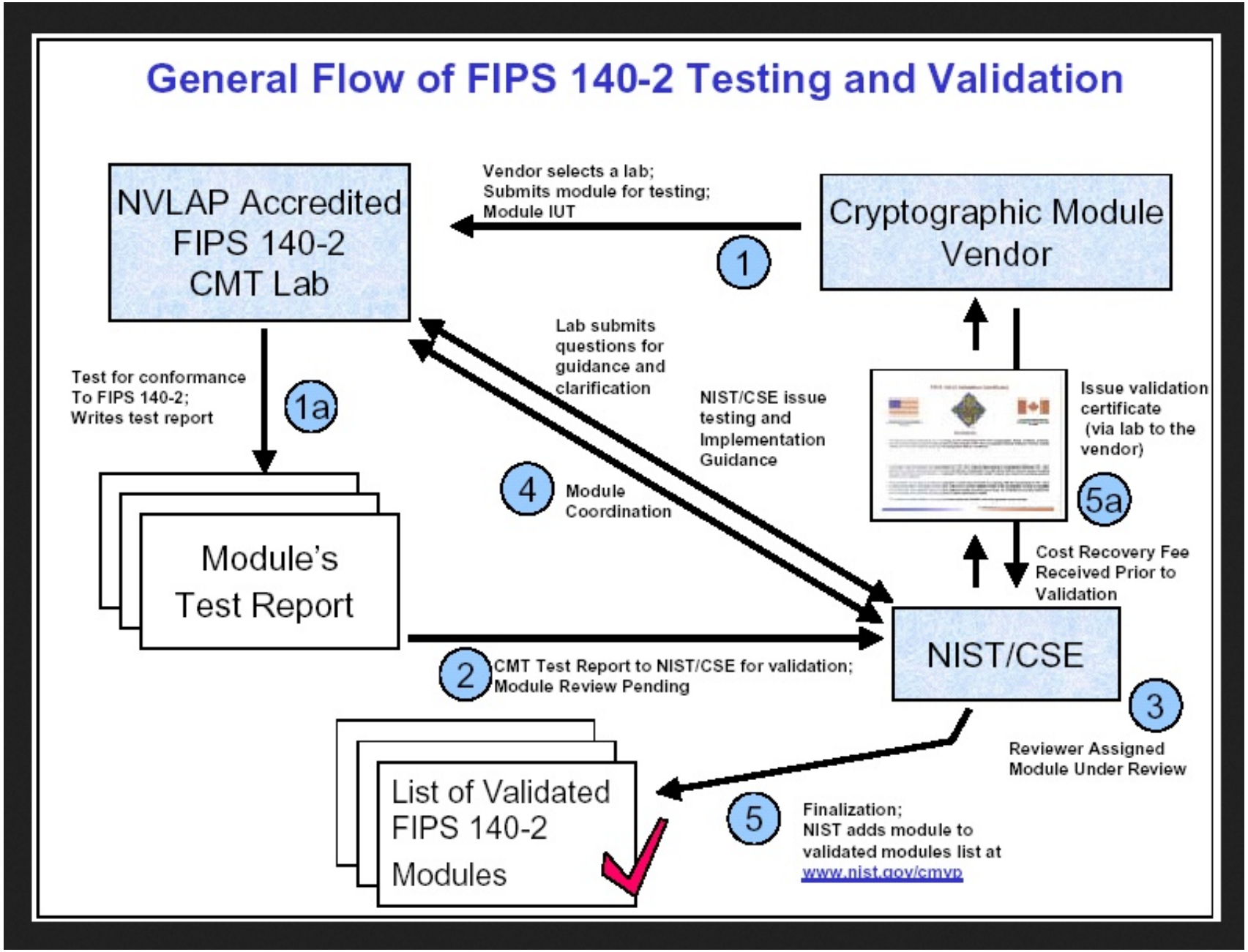
FIPS 140-2 Validation Process

FIPS 140-2 validation

- **FIPS 140-2 covers only specific areas**
  - Approved Algorithms & Security
  - Roles, Services, and Authentication
  - Physical security
  - Key Generation and Management
  - Self-Tests
  - State Models and Design Assurance
  - User Documentation (Security Policy)
- Everything else must be tested/validated separately
  - Common Criteria, Unified Capabilities, penetration testing, security tools, etc.

C

FIPS 140-2 validation process



C

Blocks


Block 1
Implementation Under Test
Block 2
Review Pending
Block 3
In Review
Block 4
In Coordination
Block 5
Finalize

The players

- Cryptographic Module Validation Program (CMVP)
- Cryptographic and Security Testing Lab (CST)
- Cryptographic Algorithm Validation Program (CAVP)
- Validation Authorities (CSD & CSE)
- Consultant
- Vendor

T

CMVP

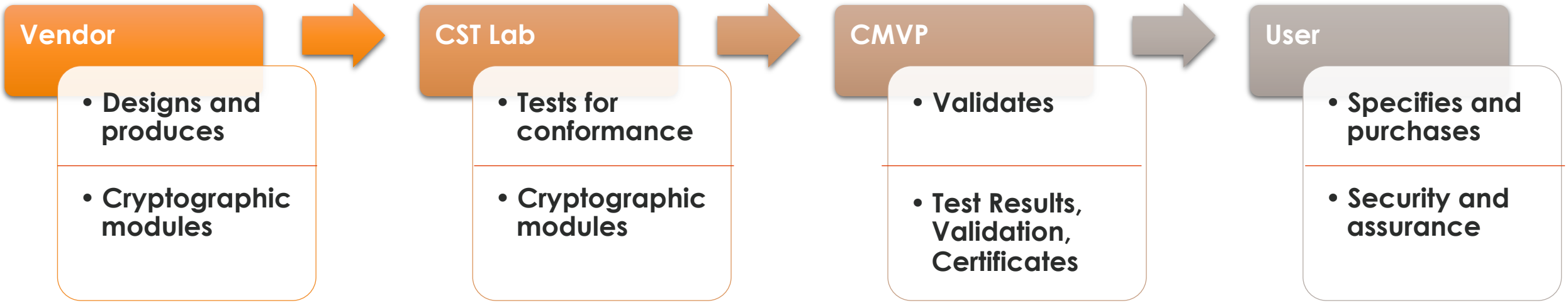
- The **Cryptographic Module Validation Program (CMVP)** is a program jointly managed by Communications Security Establishment (**CSE**) and National Institute of Standards and Technology (**NIST**)
  - **January 11, 1994:** Secretary of Commerce signed the FIPS 140-1 standard. FIPS 140-1 became a mandatory standard for the protection of sensitive data.
  - **July 17, 1995:** National Institute of Standards and Technology (NIST) established the Cryptographic Module Validation Program (CMVP) that validates cryptographic modules to Federal Information Processing Standards (FIPS)140-1 Security Requirements for Cryptographic Modules, and other FIPS cryptography based standards.
  - **May 25, 2001:** FIPS 140-2, Security Requirements for Cryptographic

CMVP: the players

- **Vendors** of cryptographic modules use independent, accredited* Cryptographic and Security Testing (**CST**) laboratories to test their modules.
  * Accreditation is through NVLAP
- The **CST** laboratories use the Derived Test Requirements (DTR), Implementation Guidance (IG) and applicable CMVP programmatic guidance to test cryptographic modules against the applicable standards.
- NIST's Computer Security Division (**CSD**) and **CSE** jointly serve as the Validation Authorities for the program, validating the test results and issuing certificates.

C

Roles and responsibilities



C

CMVP responsibilities

- Program Management
- Lab Accreditation through NVLAP
- Ongoing Lab proficiency supervision as part of their accreditation
- Test Report review
- Publish technical guidance – those famous IGs
- Issue Validation Certificates

C

Lab

- Independent (usually) privately owned entity, accredited by the government to perform validation testing of the IUT
- The lab acts as the conduit between the vendor seeking FIPS validation and the CMVP which holds the ultimate authority in issuing certificates
- As such it is a fine balance between representing the vendor and acting as the independent authority
- In the end the lab acts as the steward of the standard and ensures adherence to it
- In addition to performing the validation testing, the lab is also responsible for interpreting requirements and applying appropriately

A

CAVP

- The Cryptographic Algorithm Validation Program (CAVP) provides validation testing of FIPS-approved and NIST-recommended cryptographic algorithms and their individual components. Cryptographic algorithm validation is a prerequisite of cryptographic module validation.
  - Also uses NVLAP accredited Labs.
- CAVP validations may be prerequisites in other programs, e.g. Common Criteria

C

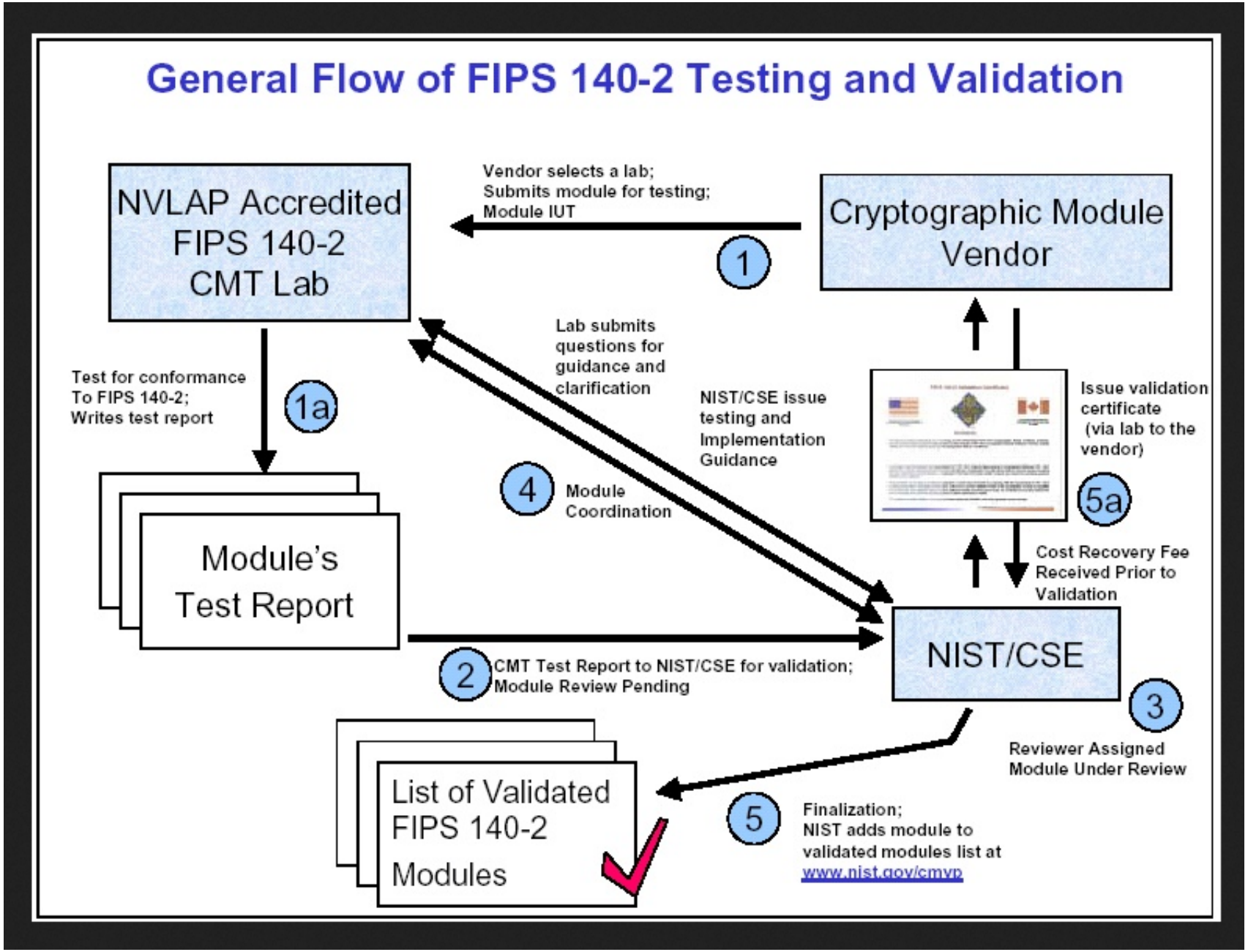
Consultants

- Provide instant expertise of the FIPS 140-2 standard and process to vendors
- Are highly recommended for vendors new to the FIPS validation process (and beyond based on company size/resources)
- Unlike FIPS labs, consultants can act as a direct extension of the vendor, being able to provide module design input, create documentation, perform algorithm testing, and respond to observations
- Using a consultant provides the FIPS lab assurance that the required FIPS documentation and deliverables will be correctly and accurately delivered.
- Can be hired ahead of the formal FIPS Validation process (“Block 0”), providing early design feedback
- FIPS Labs can also offer consultation services; however, they are limited in some aspects where internal barriers are required.
  - Producing new FIPS required documentation: barriers required between documentation production and documentation evaluation.
  - Fixes to meet FIPS requirements: barriers required between how to fix and to evaluate fixes.

Vendor

- Chooses and enters into a contract with a Lab of their choice to complete FIPS 140-2 validation
- Creates a product that meets all applicable FIPS 140-2 requirements
- Provides accurate and complete documentation to the Lab
  - Security Policy, Finite State Model, Vendor Evidence
- Conducts and passes all required FIPS 140-2 tests
  - Algorithm, Functional, and Physical testing

FIPS 140-2 validation process



C

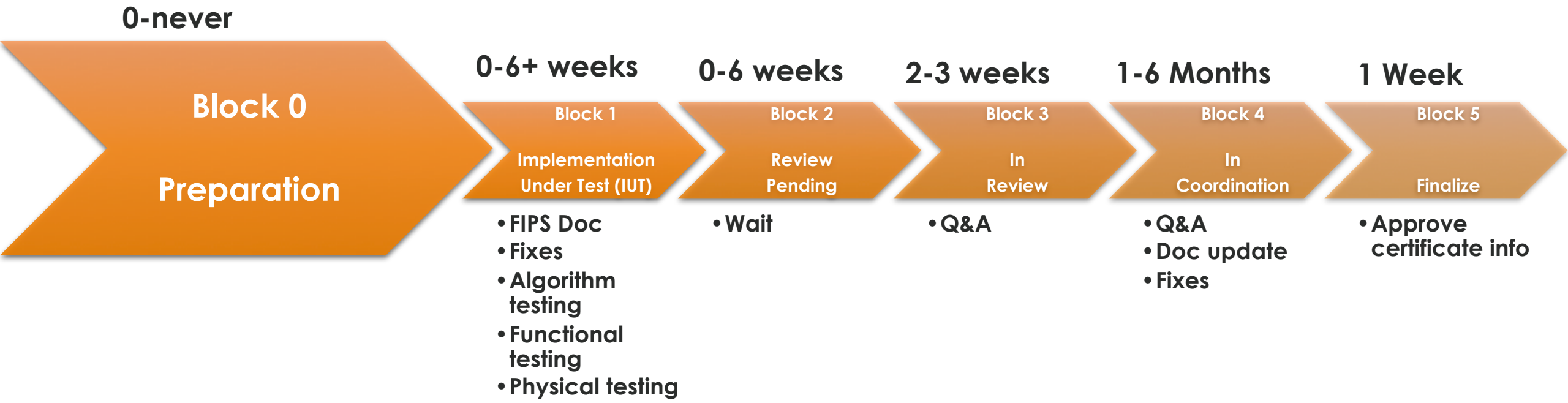
The vendor's view

1- 6 Months *(Max: 24)*	0-6+ Weeks	2-3 Weeks	1-6 Months	1 Week
Block 1 Implementation Under Test	Block 2 Review Pending	Block 3 In Review	Block 4 In Coordination	Block 5 Finalize
• FIPS Doc • Fixes • Algorithm testing • Functional testing • Physical testing	• Wait	• Q&A	• Q&A • Doc update • Fixes	• Approve certificate info

- *The vendor can influence the amount of time it takes.*
- ***Typical: 3 – 15 months***
- *Upcoming changes:*
  - ***Block 1**: max **18 months** as of July 1*
  - *Completion: max 24 months as of January 1*

IC

Vendor reality



Typical: 3 months – never

Block 0: Preparation

The foundation block

- Contract a Lab
- Identify what to validate
- Gap analysis
- Fix/update/extend the product
- Prepare the documentation
- Modify the product for algorithm and functional testing
- Prepare for functional testing

Do you need a consultant?

- Benefits to consider
  - Insights into the validation process, unwritten rules, and common pitfalls
  - Receive requirements early
  - Practical view of how to apply the FIPS standard
  - Practical view of the timeline and what is happening
  - You don’t have to write the FIPS documentation
    - You still have to review, edit, and correct it.
- Do you have a resource in house?
  - FIPS and product experience?
  - Time?
  - Desire?
  - Backup plan for the unexpected?

T

Contracting with a Lab

- There isn't an "Easiest" lab.
  - They all have the same requirements.
  - But … they may evaluate/enforce them differently.
- Experience and reputation
  - Validations completed
  - Ask colleagues, consultant
- Product familiarity
  - Previous validations of your product
  - Completed validations of your competitors
- Price
  - Negotiate
  - Due diligence: cost quoted may not represent everything you need

T

Set the target

- FIPS Level
  - Level 1, 2, 3, or 4
  - Achievable and meets sales requirements
- Module type
  - Hardware, software, or firmware
- Software version
  - Entire product or just crypto module?
- Hardware version
  - Still needed for software only
  - FIPS kit or part of appliance
- In context
  - New releases, EOS, EOM, EOL
  - Customer and sales requirements
  - Achievable in necessary time frame

Gap analysis

- Requires
  - Strong knowledge of the product architecture, implementation
  - Up-to-date understanding of FIPS requirements
- Identify FIPS requirements not met
  - Product and hardware
- Identify testing effort needed
  - Crypto self tests, failure tests, etc.
  - Tampering tests
- Wake up call
  - Perhaps you do need a consultant
  - Can the team fix everything to meet timelines?
  - Will the team/company agree to allocate resources?

T

Fix, update, and extend the target

- FIPS relevant
  - Existing and new gaps
  - Implementation Guidance changes
  - New gaps discovered
- Non-FIPS relevant (but important)
  - CAC authentication, notice & consent banner
  - Fixes for known vulnerabilities
  - Other certifications
    - E.g., Collaborative Protection Profiles, Common Criteria, Unified Capabilities
    - Focus on overlapping requirements

T

FIPS documentation

- Security Policy
  - Overview of module from a FIPS perspective
  - Instructions on initial setup and secure management
  - Public facing document
- Finite State Model
  - Flow chart
  - Shows critical FIPS 140 relevant functionality
- Entropy Analysis
- Vendor Evidence
  - Document or evidence for all requirements

Preparing for testing

- Algorithm
  - Failure and success test cases
  - Use sample vectors from NIST or Lab
  - Debug builds and root access allowed for demonstration purposes
- Functional
  - Failure and success test cases
  - Debug builds and root access allowed for demonstration purposes
- Physical
  - Test modifications early
  - Pay special attention to adhesives and mounted modifications

Case studies: Block 0

- Failure to launch
  - Insufficient commitment from engineering
  - Unrealistic expectations
  - No consultant, no experience
- Steep learning curve for a newbie
  - Consultant hired, new certification person on board
  - Lack of knowledge and experience for product, internal process, and certification
  - Unrealistic goals
- Successful gap analysis
  - Consultant, team, and security/certification
  - Early gap analysis
- PM with good intentions
  - Product Manager acted as consultant, Lab engaged, algorithm testing completed but not FIPS validation
  - Continued over time for 3 years until finally validated with certification architect, consultant, and dedicated team effort
  - Legal held up NDAs and contracts needed

T

Best practices: Block 0

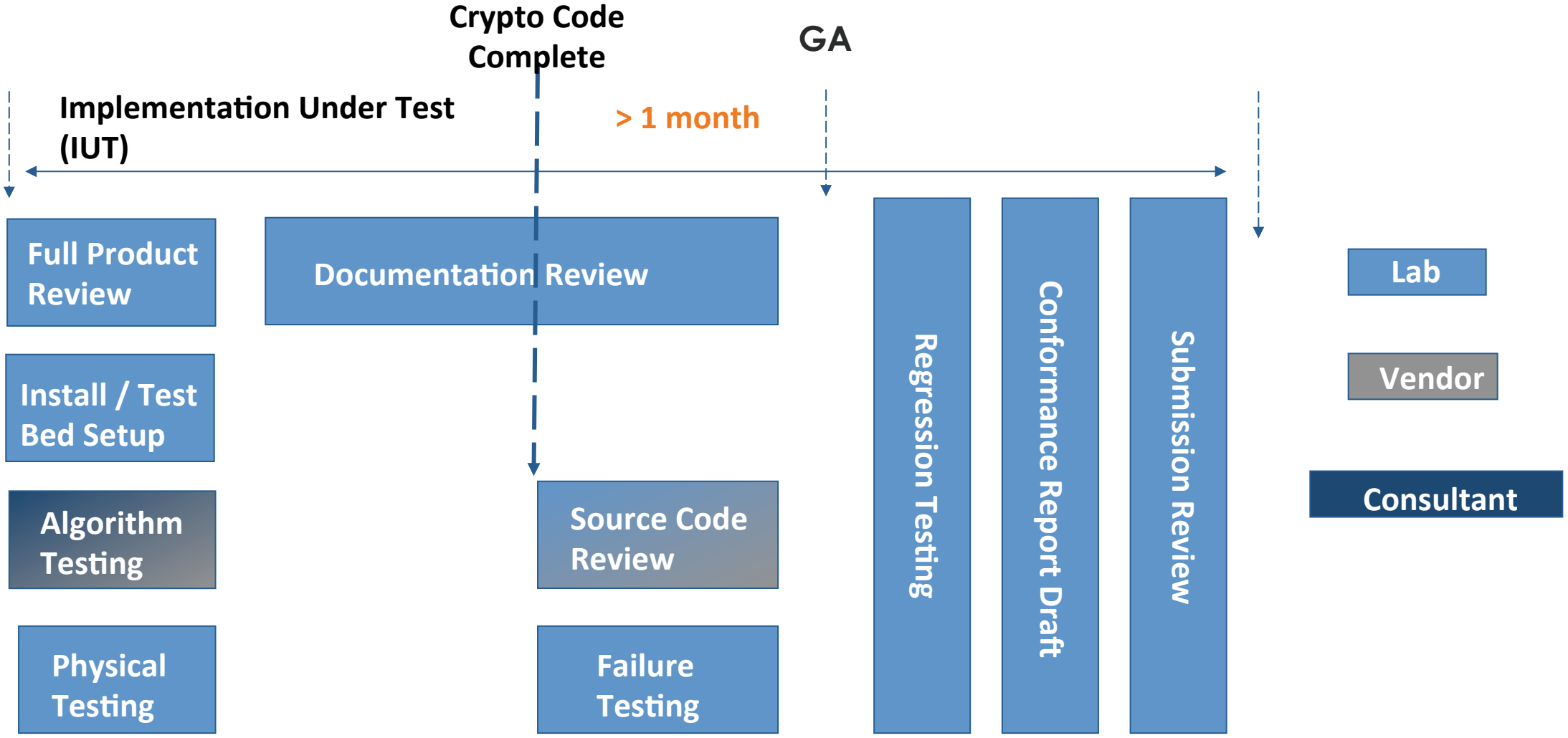
- Be realistic
  - Get dedicated engineering resources assigned
  - Identify a realistic timeline, then pad it
  - Get agreement, approvals, and funding before committing
- Manage the product team
  - FIPS training
  - Set requirements, timeline, expectations
  - Constant communication
- Order sufficient licenses, hardware, FIPS kits
  - Consultant and Lab testing
  - Engineering, QA, Hardware team
  - On-site functional testing

Best practices: Block 0

- Involve QA
  - Test in FIPS mode and non-FIPS mode
  - Include functional tests into regular automated testing.
  - Include FIPS modifications in hardware stress testing
- Functional testing
  - Do dry runs of testing until everything runs smoothly.
  - Capture screen shots or recordings of testing ahead of formal testing.
  - Make sure all hardware and people can be on-site for testing.
- Reduce complexity, time, and cost
  - Consolidate crypto libraries
  - Limit hardware appliances (e.g., based on what will sell)
  - Use crypto libraries that are already validated
- Document FIPS mode
  - Differences between FIPS and non-FIPS mode

Block 1: Implementation Under Test

Implementation Under Test



A

Lab best practices: Block 1

- Perform a deep dive analysis upfront – find issues early in the process
- Set-up and stage the IUT, familiarize yourself with the IUT
- Figure out source code access policies upfront and account for that in your plan
- Test plans should be structured to leverage efficiency e.g. one test can address number of requirements and not chronologically structured
- Complete a full round of testing prior to code freeze
- Capture copious amounts of results, it is always easy to throw away what you don't need rather than other way around
- Plan! Plan! Plan! And open lines of communications

A

Vendor best practices: Block 1

- The rules of audit apply: don't volunteer information, only answers.
- Ask for weekly status updates.
- Answer questions quickly and accurately.
- Make functional testing go quickly with little work
  - Make sure all necessary tools are installed (e.g., Wireshark)
  - Create scripts to run tests
  - All necessary special builds are at hand without needing to install/uninstall
- All necessary people are physically present for functional testing
  - SMEs and backup attendees identified in case of emergency.
- Practice tests using all hardware that may be required
- Provide easy access to screenshots and hardware.

Block 2:
Review Pending

Review Pending or “The Queue”

- Complete set of testing documents submitted to NIST and CSE for review, including:
  - draft certificate
  - detailed test report
  - non-proprietary Security Policy
  - website information
  - separate physical security testing *(select modules)*
  - separate entropy reports *(select modules)*
- Signed letter from laboratory stating recommendation for validation by NIST and CSE
- When the report is submitted, NIST sends an invoice to the Lab for the Cost Recovery (CR) fee

C

Review Pending – why the wait?

- A report stays in Review Pending until at least one reviewer has been assigned and starts the review
  - Reports cannot be assigned at NIST until the Cost Recovery fee has been paid – **this can take up to 6 weeks**, depending on the billing process at the individual labs
  - Most reports in the Review Pending column of the MIP list are waiting for payment
  - After the CR is paid, report assignment depends on **resource availability**
- What can the Lab/Vendor do to speed this up?
  - IUTB was introduced by the CMVP to speed up the billing process

C

Review Pending – a bit more about IUTB

- Implementation Under Test Billing (IUTB)
  - Request an invoice from NIST for Cost Recovery ***before*** report submission, i.e. in Block 1
- Introduced to move the billing process to the IUT stage
  - If the CR is paid by the time a report is submitted, the report often **immediately** goes into review
  - In other words, on average, reports are being reviewed as soon as the bill is paid or the report is received, whichever comes second.

C

IUTB fine print

- At any time after the lab submits the IUTA, the lab has the option to send an IUTB to initiate the CR process before submitting the report.
- If the lab sends an IUTB and then needs to cancel the invoice, the lab must send an IUTC. When the IUTC is successfully processed, the lab will receive the automated response, "*Your request has been received and will be processed. If there are any issues in cancelling the invoice, you will be notified*."
- Only unpaid invoices can be cancelled.
- No files are required for an IUTB or IUTC. Only a properly formatted subject line is required.
- When the cost recovery process starts, no changes to the Security Level or Submission Type will be accepted.
- When the invoice is paid, there are no refunds regardless of when the CR process is initiated.
- If a report has not been received by 90 days after the IUTB was accepted, the module will be moved to On Hold and removed from the IUT list. The module can be automatically removed from On Hold and placed on the Modules In Process (MIP) list by sending the report.

C

CMVP resources

- Staff:
  - 4 NIST and 5 CSE: includes 2 program managers + 1 CSE admin
  - Lab audit and accreditation
  - Implementation and Program Guidance Development
  - Review
- Cost Recovery pays for:
  - Contract reviewers (2)
  - Automation system that administers e-mail and website

CSE and NIST work closely on report review and program management. Twice weekly meetings ensure consistent and efficient review.

C

Case studies: Block 2

- 13 minutes in Review Pending
  - IUTB can decrease wait time significantly
- Taking a vacation
  - Teams lose focus and momentum
  - Time is reallocated
  - Weeks of delay

CT

Best practices: Block 2

- Keep the teams engaged – this isn't a vacation.
  - Start other certifications
  - Write FIPS mode document
  - Begin planning next FIPS validation
- Use IUTB
  - Pay as early as possible
  - But, be sure your module will be submitted

TI

Block 3: In Review

In Review

- Starts when 1st reviewer is assigned and begins review
- Two CMVP reviewers assigned, one of which is the Point of Contact (POC)
  - Usually 1 contractor, 1 federal employee (NIST or CSE)
  - Reviewers review of all submitted documentation and send their comments to the 2nd reviewer.
  - 2nd reviewer completes their review and adds comments to the 1st's. Consolidated comments are sent to the lab.
  - This phase can take 2-3 weeks depending on resource availability.
- The report cannot leave this stage until both reviews are complete.
- Timeframe: 2-3 weeks

C

Why review?

- Adherence to FIPS 140-2
  - Comments and questions are usually technical in nature and are intended to ensure that:
    - the cryptographic module **meets the requirements** of the standard
    - the information provided is accurate and complete
- Ongoing quality and technical proficiency of the lab
  - Labs must maintain **proficiency** in order to remain accredited
  - Failure to maintain proficiency could result in suspension of a lab
- Inform guidance development in order to maintain **consistency** across labs
  - If the CMVP finds that the labs are interpreting requirements and guidance differently for similar test cases, or are unsure how to interpret requirements, we may issue guidance to create consistency

C

Block 4:
In Coordination

In Coordination

- Starts when comments sent from CMVP to the CST lab
- A round of comments may trigger:
  - Module changes (if required – this is very rare)
  - Additional testing (if required)
  - Additional documentation (if required)
  - Comments resolution developed for resubmission to NIST and CSE
  - Testing documents updated for resubmission to NIST and CSE
  - Responses to comments and revised test documents submitted to NIST and CSE
- Several iterations may be required to address all comments.
- Timeframe: ???

C

In Coordination (cont'd)

- The length of time for coordination depends on the number of rounds of comments
- Only one reviewer (the POC) takes the report through coordination
- Response from the CMVP generally takes a few days; more than two weeks is extremely rare
  - Exception is if an issue needs to be discussed internally within the CMVP
- If CMVP comments are sent to the lab and the lab has not responded within 120 days, the module will be placed on HOLD and removed from the MIP list until the CST laboratory provides a response. Effective July 1, 2017, the amount of time will be reduced from 120 days to 90 days.
- **When the POC is satisfied that all comments have been addressed, the report is sent for certificate review.**

C

CMVP certificate review

- Part of Coordination
  - Done by NIST and CSE (but not the assigned reviewers)
  - Originated back in the days of the program when each certificate was printed and signed
- May cause another round of comments
  - Consistency between certificate and Security Policy
  - Adherence to IG G.13
  - Any recent issues addressed properly (e.g. SP 800-131A transition)
- When both CSE and NIST are satisfied, report enters finalization

CSE and NIST work closely on report review and program management. Twice weekly meetings ensure consistent and efficient review.

C

Blocks 3 & 4: Lab perspective

- Difficult to predict when comments will come in, so impossible to plan resources
  - However delaying responding to CMVP comments is a disservice to your customer
- Once received, ideally the original validation team is assigned to responding to the comments
- Where required, the lab will work with the product vendor to address comments
- Most comments are documentation updates, however in rare cases, additional testing might be required. This is where having the test bed readily available is helpful
- If comments lead to making product changes, you have failed as a lab!
- In most cases expect 2-3 rounds of comments.

C

Blocks 3 & 4: Vendor/Consultant

- When required, labs will look to the vendor/consultant to answer some CMVP questions.
  - Ensuring the vendor provided responses to CMVP observations are thorough, helps avoid unnecessary back and forth, but it is important to avoid being too verbose.
  - While it might be great information, it stops being effective at a certain point and can only lead to additional scrutiny/time.
- The landscape and FIPS validation variables are always changing.
  - There are many things that can contribute to new comments during a revalidation: regular Implementation Guidance updates, different CMVP reviewer backgrounds, new emphasis placed on certain requirements, and not least of all, a fresh look.
  - Even if you are able to keep the Security Policy largely untouched as part of a revalidation, it is likely Security Policy updates will be needed.

Case studies: Blocks 3 & 4

- Heartbleed
  - Affected how products met the standard
  - Vendors in process had to fix
  - Could happen again

Best practices: Blocks 3 & 4

- Lab Perspective
  - Ensure all comments are being reviewed in detail, each (and every comment) is addressed and clear responses are provided
    - Copy and paste updated text into the comments document, this helps reviewers in not having to go back and forth between documents
  - If a CMVP comment is not clear, pick up the phone and talk to the reviewer!
  - Strive to respond to comments within 1-2 weeks of receiving them
  - Strive to ensure comments do not exceed three rounds. If it looks like there is confusion, pick up the phone!
  - Keep customer updated.
- Vendor perspective
  - Keep product teams updated and on standby to act quickly.
  - Expect the unexpected – the same product may be reviewed differently over time, or reviewed by a different person all together.

AI

Block 5: Finalize

Finalization

- Final resolution of validation review comments submitted to NIST and CSE
- Testing documents updated based on resolutions and submitted to NIST and CSE
- A copy of the certificate is sent to the CST laboratory for a final review by the lab and vendor
  - It is important that they verify the correct module name, version, and contact information
- Once the CST laboratory approves the final draft certificate, the CMVP assigns a certificate number and NIST posts the certificate to the Validated 140-2 Cryptographic modules list
- **Finalization usually takes 1-3 days depending on turnaround from**

Certificates


FIPS 140-2 Validation Certificate

The National Institute of Standards and Technology of the United States of America

The Communications Security Establishment of the Government of Canada

Certificate No. 237

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the Cryptographic Module identified as:

F-Secure Kernel Mode Cryptographic Driver *by* F-Secure Corporation
(When operated in FIPS mode)

in accordance with the Derived Test Requirements for FIPS 140-2, *Security Requirements for Cryptographic Modules*. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting *Sensitive Information* (United States) or *Designated Information* (Canada) within computer and communications systems (including voice systems).

Products which use the above identified cryptographic module may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life cycle, continues to use the validated version of the cryptographic module as specified in this certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

This certificate includes details on the scope of conformance and validation authority signatures on the reverse.

- Certificates used to be printed, signed and delivered to the lab/vendor
- Now validations are posted, with the certificate number, here: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm
- Consolidated certificates are signed monthly and posted via a link in the validation entry
- The validation entry/certificate is the document that attests that a module with *that* name and version was tested and found compliant to the FIPS 140-2 standard.
  - Other information includes type, embodiment, security level, approved and allowed cryptography, and operational test environments

Case studies: Block 5

- Inaccurate product name on certificate
  - Wrong person reviewed
- Anti-climactic end
  - Long wait
  - Less work and excitement after functional testing
  - Team moved to new projects
  - Actual certificate meant nothing

Best practices: Block 5

- Review the certificate carefully for correctness.
- Celebrate the completion
- Do a post-mortem
  - Lab and Consultant
  - Product team (earlier is better)

Questions?

Tammy Green – Senior Principal Security Architect, Symantec

Carolyn French – Program Manager, CMVP

Ashit Vora – Co-Founder and Lab Director, Acumen Security

Ian Hall – Certification Architect, Symantec

Take aways

- Set expectations at the beginning
- Choose the right target
- Keep product teams engaged
- Government bodies do listen and will change
- We learn from our mistakes and failures
- Celebrations are necessary

Changes to Come

Revalidation

- So you have a certificate for your product, now what?
  - Can you make changes?
  - What if you find a bug?
  - What if a vulnerability is discovered?
  - What is the historic list?
- The CMVP has a number of ways to revalidate without going through the full testing process again

Remember: only the version number on the certificate is the version of your product that is validated.

Submission Scenarios – IG G.8

- Scenario 1 (1SUB) - updated certificate, no CR fee
  - Administrative updates, e.g. Contact information
  - No "Security Relevant" changes
    - In other words the changes made do not affect how the module meets the FIPS 140-2 standards
    - Could be bug fixes
  - Updated CAVS testing
  - New Operational Environment testing for a Software module

Time at CMVP: < 1 week

- Scenario 1A and 1B – results in new certificate, CR fees applicable
  - 1A – OEM
  - 1B – 1SUB but under a different lab

Time at CMVP: depends

Submission Scenarios – 3SUB & 4SUB

- 4SUB – updated Certificate, no CR fees
  - Only physical security has changed, e.g. new seals, new epoxy
- 3SUB – new Certificate, CR fee
  - Modifications are made to hardware, software or firmware components that affect some of the FIPS 140-2 security relevant items
  - "Some" is < 30%
  - Testing depends on what has been affected
  - New report submitted to the CMVP

Time at CMVP: < 1 week

Time at CMVP: depends

Historic List

- February 1, 2017 – Modules validated to FIPS 140-1 and modules that had not been validated or revalidated within the past 5 years were moved to the Historical List. Modules on this list can have the following updates:
  - 1SUBs for administrative updates where the module is unchanged (e.g. contact info). The certificate will remain on the Historical List.
  - 3SUBs for up to 2 years after the certificate's sunset date. The resulting new certificate will appear on the Active List.
  - No other submission scenarios will be accepted.
- **Note**: These certificates have NOT been revoked!

Can a product be brought back to the Active List?

2SUB

- 2SUB for extending the certificate's sunset date
  - Module has NOT changed
  - Module meets all of the latest standards, implementation guidance and algorithm testing in effect at the time the module revalidation package is submitted
  - Only available for modules with certificates on the active list

CVE?

- CMUF Working Group: Revalidation in Response to CVEs
  - Aiming for quick patching, testing, revalidation of modules that are subject to security relevant CVE