CMVP INSIDE

LIFTING THE LID ON THE FIPS 140-2 VALIDATION PROCESS

ICMC
May 2016

Carolyn French & Jennifer Cawthra
Program Managers, CMVP

AS A VENDOR, HAVE YOU EVER WONDERED…

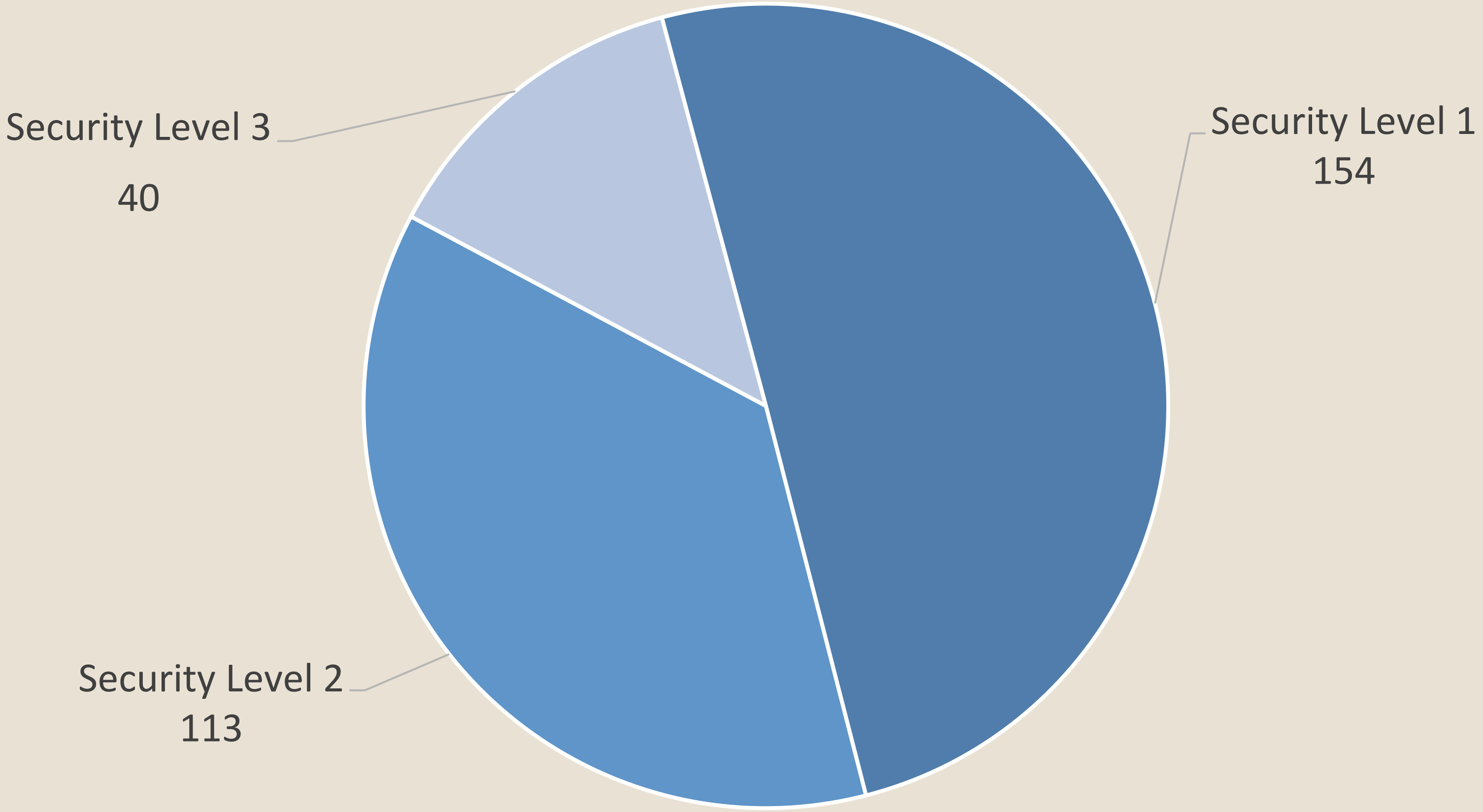
- What happens after the lab finishes testing and sends the report to the CMVP?
- What is the MIP list and what do the columns mean?
- Why does it take so long to get the certificate?
- What can you do to speed up the process?
- What is the Cost Recovery fee being used for?
- How can you keep your products validated?
  - New versions
  - Bug fixes
  - That new sunset date

THE CMVP: CSE & NIST

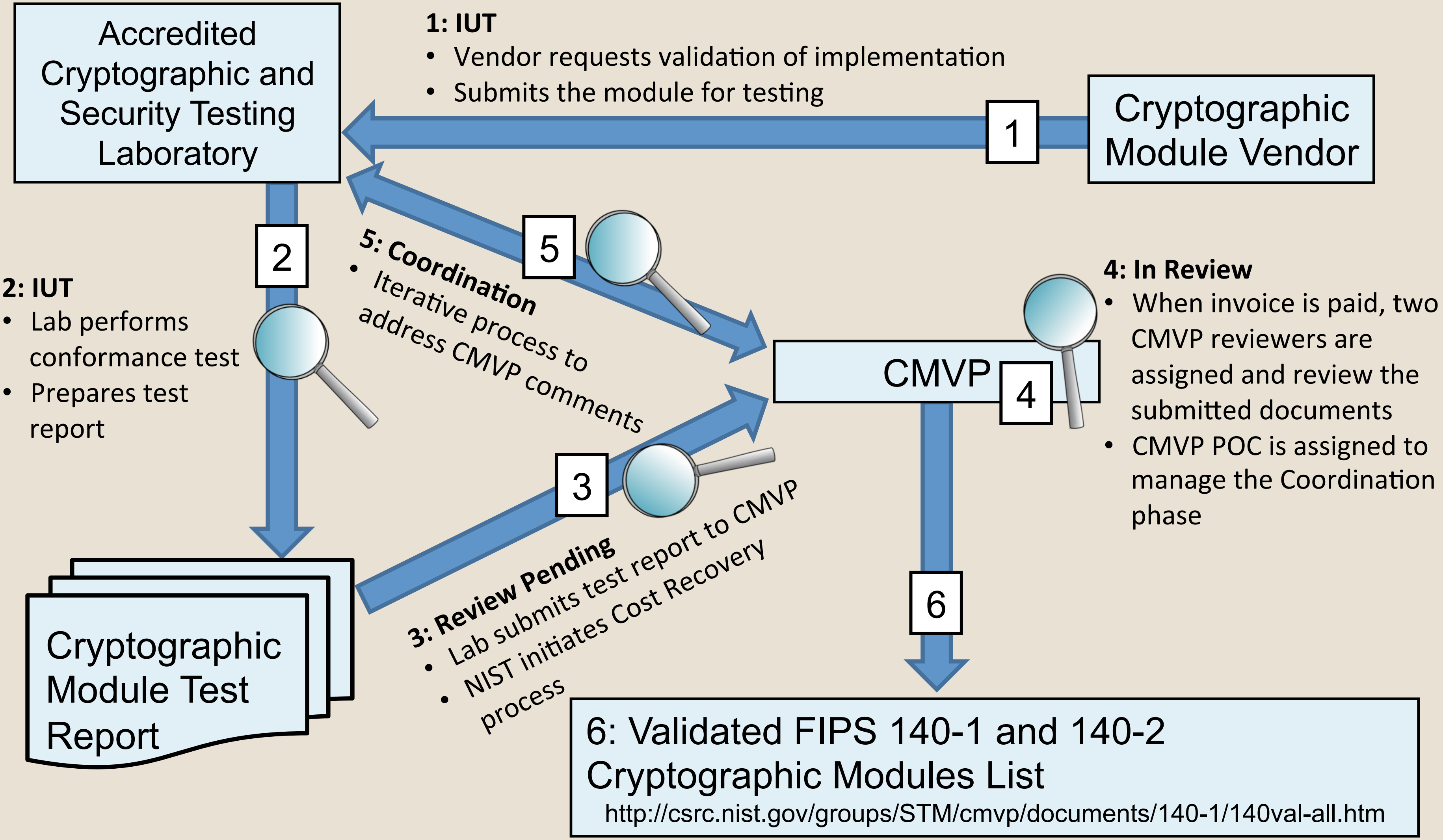
- The **Cryptographic Module Validation Program (CMVP)** is a program **jointly managed** by Communications Security Establishment (CSE) and National Institute of Standards and Technology (NIST)

FYI6 – CMVP STATUS

307 CMVP Certificates Issued in FY16 by Security Level



VALIDATION PROCESS



Accredited Cryptographic and Security Testing Laboratory

Cryptographic Module Vendor

1: IUT

- Vendor requests validation of implementation
- Submits the module for testing

2: IUT

- Lab performs conformance test
- Prepares test report

3: Review Pending

- Lab submits test report to CMVP
- NIST initiates Cost Recovery process

4: In Review

- When invoice is paid, two CMVP reviewers are assigned and review the submitted documents
- CMVP POC is assigned to manage the Coordination phase

5: Coordination

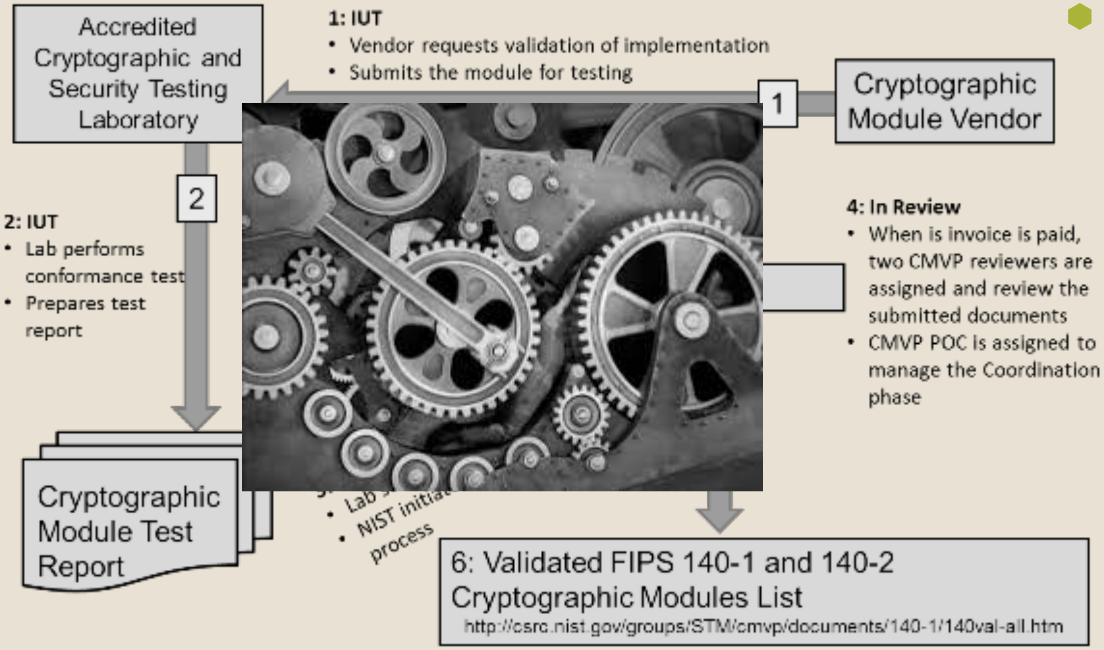
- Iterative process to address CMVP comments

CMVP

Cryptographic Module Test Report

6: Validated FIPS 140-1 and 140-2 Cryptographic Modules List
http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

BUT FIRST… COST RECOVERY



Accredited Cryptographic and Security Testing Laboratory

1: IUT
- Vendor requests validation of implementation
- Submits the module for testing

1

Cryptographic Module Vendor

2

2: IUT
- Lab performs conformance test
- Prepares test report

4: In Review
- When is invoice is paid, two CMVP reviewers are assigned and review the submitted documents
- CMVP POC is assigned to manage the Coordination phase

Cryptographic Module Test Report

- Lab
- NIST initia process

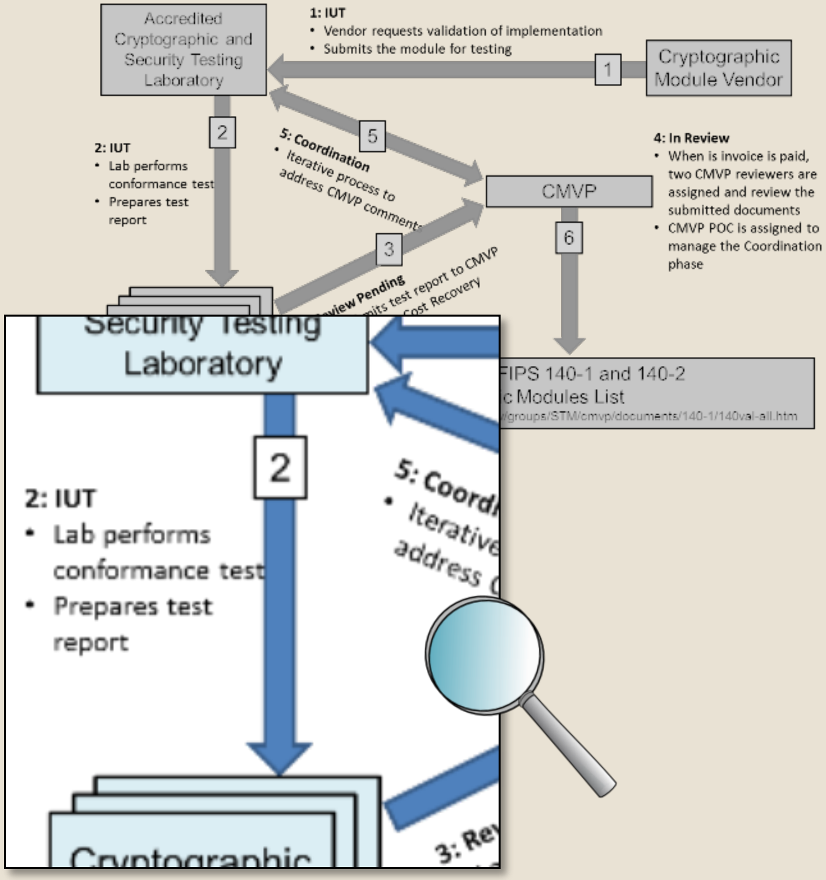
6: Validated FIPS 140-1 and 140-2 Cryptographic Modules List
http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

- How the Cost Recovery fees are working for you…
  - NIST collects a fee per report that goes towards:
    - Contracted resources (2)
    - System automation, which frees up resources for reviews

2. IMPLEMENTATION UNDER TEST (IUT)

http://csrc.nist.gov/groups/STM/cmvp/inprocess.html

- **Module is being tested at the lab**
- **A few changes for efficiency and transparency:**
  - IUT list is now separate from the MIP list
  - The IUT list includes an IUT date
  - Effective July 1, 2017, modules listed on the IUT List for 18 months or longer are automatically dropped
  - IUTB allows the lab to request an invoice while finalizing the test report



Accredited Cryptographic and Security Testing Laboratory

1: IUT
- Vendor requests validation of implementation
- Submits the module for testing

Cryptographic Module Vendor

1

2

2: IUT
- Lab performs conformance test
- Prepares test report

5

5: Coordination
- Iterative process to address CMVP comments

CMVP

4: In Review
- When is invoice is paid, two CMVP reviewers are assigned and review the submitted documents
- CMVP POC is assigned to manage the Coordination phase

3

6

view Pending
its test report to CMVP
Cost Recovery

FIPS 140-1 and 140-2
c Modules List
/groups/STM/cmvp/documents/140-1/140val-all.htm

Security Testing Laboratory

2

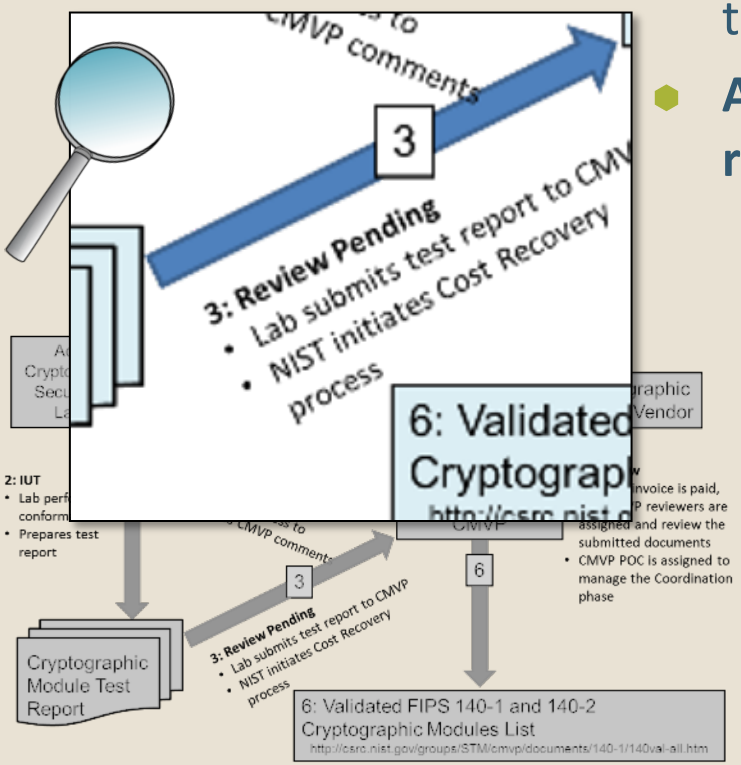
2: IUT
- Lab performs conformance test
- Prepares test report

5: Coord
- Iterative
address

3: Re

Cryptographic

3. REVIEW PENDING (AKA "THE QUEUE")


CMVP comments
3
3: Review Pending
• Lab submits test report to CMVP
• NIST initiates Cost Recovery process
6: Validated
Cryptograph
http://csrc.nist.g
Ac
Crypto
Secu
La
raphic
Vendor
2: IUT
• Lab perf
conform
• Prepares test report
CMVP comments
3
3: Review Pending
• Lab submits test report to CMVP
• NIST initiates Cost Recovery process
CMVP
6
invoice is paid,
P reviewers are assigned and review the submitted documents
• CMVP POC is assigned to manage the Coordination phase
Cryptographic Module Test Report
6: Validated FIPS 140-1 and 140-2 Cryptographic Modules List
http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

- The famous MIP List:

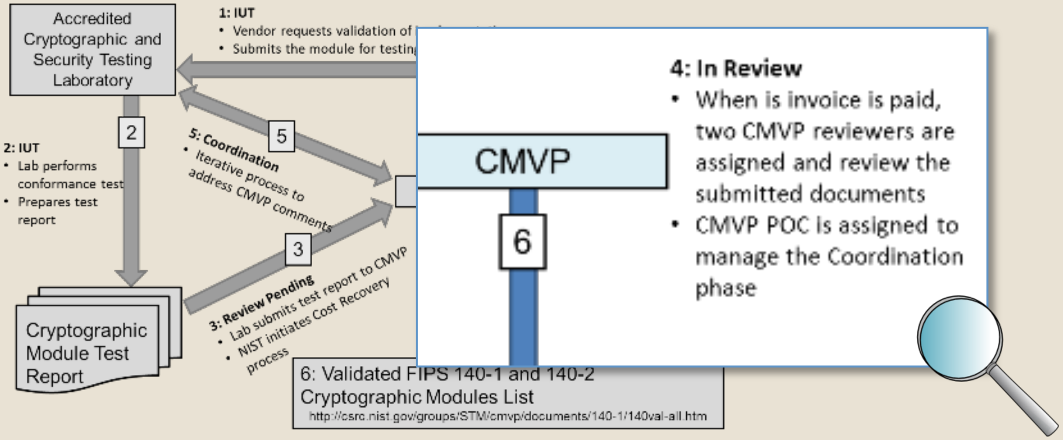
http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140InProcess.pdf

- The report has been sent to the CMVP and is waiting to be picked up for review
- **A report stays in this state 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
  - IUTB 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.

4. IN REVIEW

- **Two reviewers assigned, one of which is the POC**
  - Usually 1 contractor, 1 federal employee (NIST or CSE)
  - The first reviewer completes their review of all submitted documentation and sends 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



Accredited Cryptographic and Security Testing Laboratory

1: IUT
- Vendor requests validation of
- Submits the module for testin

2: IUT
- Lab performs conformance test
- Prepares test report

Cryptographic Module Test Report

3: Review Pending
- Lab submits test report to CMVP
- NIST initiates Cost Recovery process

5: Coordination
- Iterative process to address CMVP comments

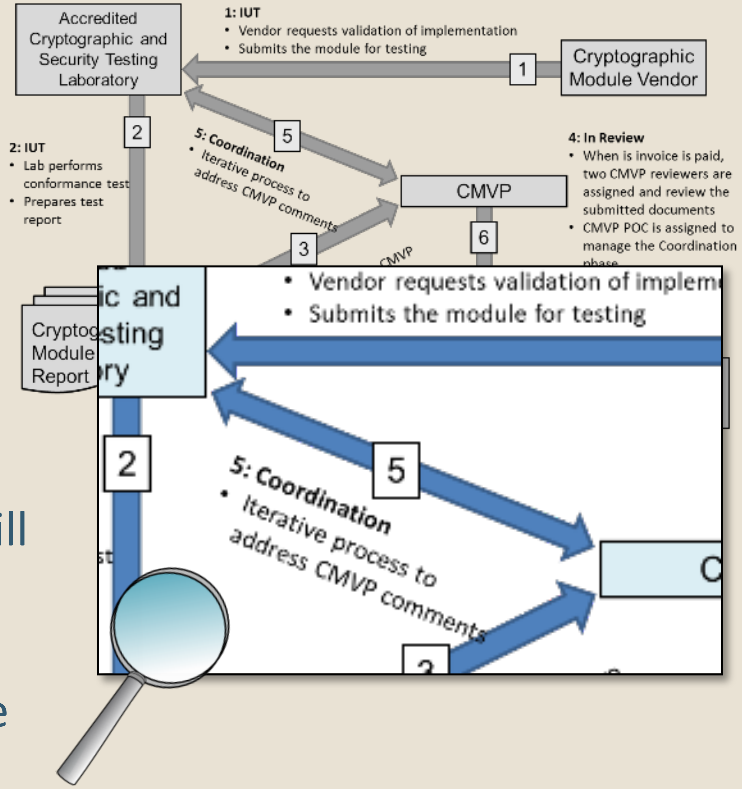
CMVP

4: In Review
- When is invoice is paid, two CMVP reviewers are assigned and review the submitted documents
- CMVP POC is assigned to manage the Coordination phase

6: Validated FIPS 140-1 and 140-2 Cryptographic Modules List
http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

5. COORDINATION

- 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 maximum response time will be reduced from 120 days to 90 days.

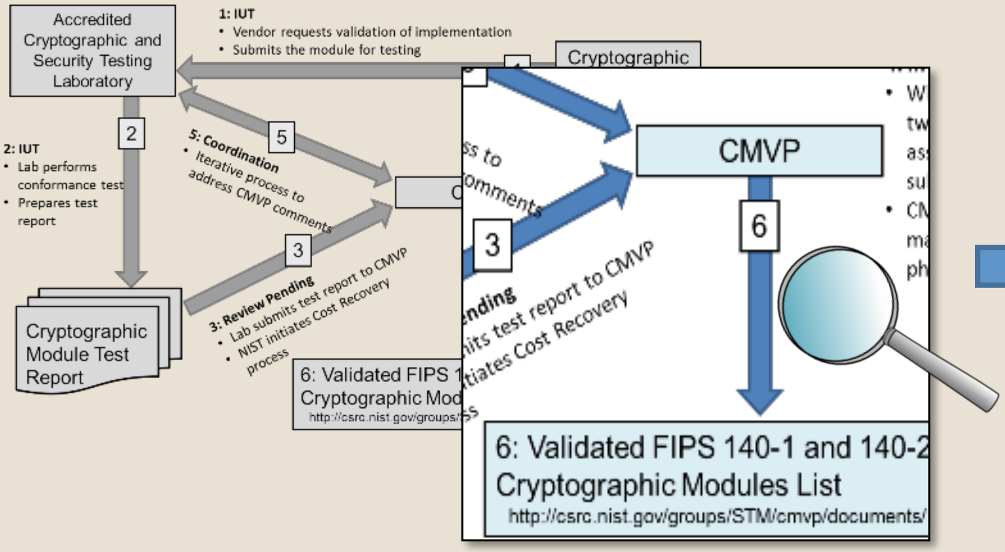

Accredited Cryptographic and Security Testing Laboratory
1: IUT
• Vendor requests validation of implementation
• Submits the module for testing
1
Cryptographic Module Vendor
2
2: IUT
• Lab performs conformance test
• Prepares test report
5
5: Coordination
• Iterative process to address CMVP comments
CMVP
3
6
CMVP
4: In Review
• When is invoice is paid, two CMVP reviewers are assigned and review the submitted documents
• CMVP POC is assigned to manage the Coordination phase
Cryptog Module Report
ic and
sting
ry
• Vendor requests validation of impleme
• Submits the module for testing
2
5
5: Coordination
• Iterative process to address CMVP comments
C

When the POC is satisfied that all comments have been addressed, the report is sent for certificate review.

6. FINALIZATION

- Finalization is entered, after all comments including those from the CMVP certificate review are closed.
- This is the final check by the lab and the vendor of the certificate and contact information

When all parties are satisfied with the final report, comments, SP, and certificate, the module is assigned a certificate number and it is posted on the CMVP Validation Page.


Accredited Cryptographic and Security Testing Laboratory
1: IUT
Vendor requests validation of implementation
Submits the module for testing
Cryptographic
2
2: IUT
Lab performs conformance test
Prepares test report
5
5: Coordination
Iterative process to address CMVP comments
3
3: Review Pending
Lab submits test report to CMVP
NIST initiates Cost Recovery process
Cryptographic Module Test Report
6: Validated FIPS 1
Cryptographic Mod
http://csrc.nist.gov/groups/
CMVP
6
6: Validated FIPS 140-1 and 140-2 Cryptographic Modules List
http://csrc.nist.gov/groups/STM/cmvp/documents/

CASE STUDIES

- **With IUTB:**
  - New Validation (5SUB): Hardware, Overall Level 1
    - Review Pending: 13 minutes
    - In Review: 10 days
    - Coordination: 20 days (2 rounds of comments)
    - Finalization: 3 days
    - Overall from Report Submission to Posting : **33 days**

- **Without IUTB:**
  - New Validation (5SUB): Hardware, Overall Level 1
    - Review Pending: 14 days
    - In Review: 14 days
    - Coordination: 32 days (2 rounds of comments)
    - Finalization: 1 day
    - Overall from Report Submission to Posting: **61 days**

ET CETERA

A few other changes introduced recently:

- **Sunsetting**:
  - 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
  - Scenario 1, 1A, 1B and 4 submissions do not affect the sunset date
  - Scenario 2 submissions will update the sunset date
- **Stagnant Modules**:
  - As of January 1, 2018 all submissions must be completed within 2 years of the report submission date or the IUTB request date, whichever occurred first
  - At the 2 year anniversary, the module will be dropped. The vendor and lab will have to restart the validation process from the beginning including paying a new cost recovery fee at the current rate
- **Twice weekly Reviewer Meetings:**
  - CSE and NIST staff meet to discuss technical issues, review IGs, and answer questions from the lab
  - Ensures consistent knowledge and review across the CMVP

HOW CAN WE MAKE VALIDATION EVEN FASTER?

- There are a number of CMUF working groups trying to answer this questions:
  - Equivalency Working Group
    - How to minimize the amount a testing and still provide assurance
  - Revalidation in Response to CVEs Working Group
    - How to quickly test and revalidate a module in response to a CVE

Please join us!

QUESTIONS?