Keeping it Valid: Maintenance of FIPS 140-2 Validated Modules

ICMC 2017, May 19th

Shashi Karanam

Secure Product, Secure Brand, Secure Bottom Line

FIPS 140-2 Validation Cycle

Modules In-validation

- Implementation Under Test (IUT) List
- Modules In Process (MIP) List

Modules Validated

- Active Validation List (Sunset period - 5 years)
- Historical Validation List

Modules Validation Maintenance

- 1SUB, 1A, 1B, 2SUB, 3SUB, 4SUB, and 5SUB

FIPS 140-2 IUT and MIP Lists

CMVP FIPS 140-2 Implementation Under Test (IUT) List

- Vendor establishes a contract with an accredited laboratory
- CMVP does not have detailed information about the crypto module

CMVP FIPS 140-2 Modules In Process (MIP) List

- **Review Pending:** Lab submits test report to NIST and CSE
- **In Review:** NIST and CSE assign reviewers
- **Coordination:** Coordination between NIST and CSE, and laboratory
- **Finalization:** Finalization and certificate issuance

FIPS 140-2 Validation Lists

Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules List

- Validation complete and certificate issued
- Five year validation sunsetting policy, **effective February 1, 2017**

CMVP Historical Validation List

- Modules that have been validated five years ago but not have been updated to reflect latest guidance and/or transitions
- Modules that includes retired RNG implementations, effective **January 1, 2016**

Corsec FIPS 140-2 Validation Maintenance Options

1SUB (Change Letter)	• Non-FIPS-relevant module changes • Re-branding of an unchanged OEM module
2SUB	• Extending the certificates sunset date
3SUB (Revalidation)	• Changes affecting less than 30% of the module’s FIPS-relevant features
4SUB	• Changes were made to the module's physical enclosure only
5SUB (Full Validation)	• Changes affecting 30% or more of the module’s FIPS-relevant features

1SUB

1SUB – Scenario 1

- Administrative updates
- **Modifications to HW/SW/FW without affecting FIPS-relevant features**
- Post validation, approved security functions for which testing was not available at the time of validation, or approved security functions that were not tested but submitted for inclusion

Active/Historical Lists	Active/Historical (only administrative updates)
Retesting	Yes (if adding previously untested approved security functions)
Regression Testing	No
New Certificate	No
Sunset Date	Unchanged
Security Policy	Updated (only if modifications occur)

1SUB – Alternative Scenario 1A

- Re-branding of an unchanged OEM Module

Active/Historical Lists	Active only
Retesting	No
Regression Testing	No
New Certificate	Yes (*This validation entry is rebranding from Cert. #nnnn*)
Sunset Date	Unchanged
Security Policy	Updated

1B

1SUB – Alternative Scenario 1B

- Scenario 1 revalidation for which the laboratory (different from laboratory contracted for original validation) did not perform the testing on the module

Active/Historical Lists	Active only
Retesting	May be (at lab's discretion)
Regression Testing	No
New Certificate	Yes with new laboratory's NVLAP code (*This validation entry is a non-security-relevant-modification to Cert. #nnnn*)
Sunset Date	Unchanged
Security Policy	Updated (only if modifications occur)

2SUB – For extending certificate's sunset date

- Module has not changed
- Module meets ALL the standards, IG and CAVP requirements at the time the module revalidation package is submitted to CMVP

Active/Historical Lists	Active only
Retesting	No
Regression Testing	No
New Certificate	Yes
Sunset Date	Changed (Extended)
Security Policy	No updates

3SUB – When changes affect <30% of FIPS-relevant features

- Modifications to HW/SW/FW that affect less than 30% of FIPS-relevant features
- Must meet ALL the standards, IG and CAVP requirements at the time module revalidation package is submitted to CMVP

Active/Historical Lists	Active/Historical (for up to 2 years after the sunset date)
Retesting	Yes
Regression Testing	Yes
New Certificate	Yes
Sunset Date	Changed (sunset date 5 years from the validation date)
Security Policy	Updated

4SUB – When changes affect module’s physical enclosure only

- Typically applies to modules meeting FIPS level 2 or higher physical security requirements
- **Involves no operational changes**

Active/Historical Lists	Active only
Retesting	Yes (fully test the physical security features)
Regression Testing	No
New Certificate	No
Sunset Date	Unchanged
Security Policy	Updated

5SUB – When changes affect >30% of FIPS-relevant features

- Modifications to HW/SW/FW that affect more than 30% of FIPS-relevant features
- Must meet ALL the standards, IG and CAVP requirements at the time module revalidation package is submitted to CMVP

Active/Historical Lists	Active only
Retesting	Yes (Full Testing)
Regression Testing	No
New Certificate	Yes
Sunset Date	Changed (sunset date 5 years from the validation date)
Security Policy	Updated

Summary

Must meet ALL the standards, IG and CAVP requirements

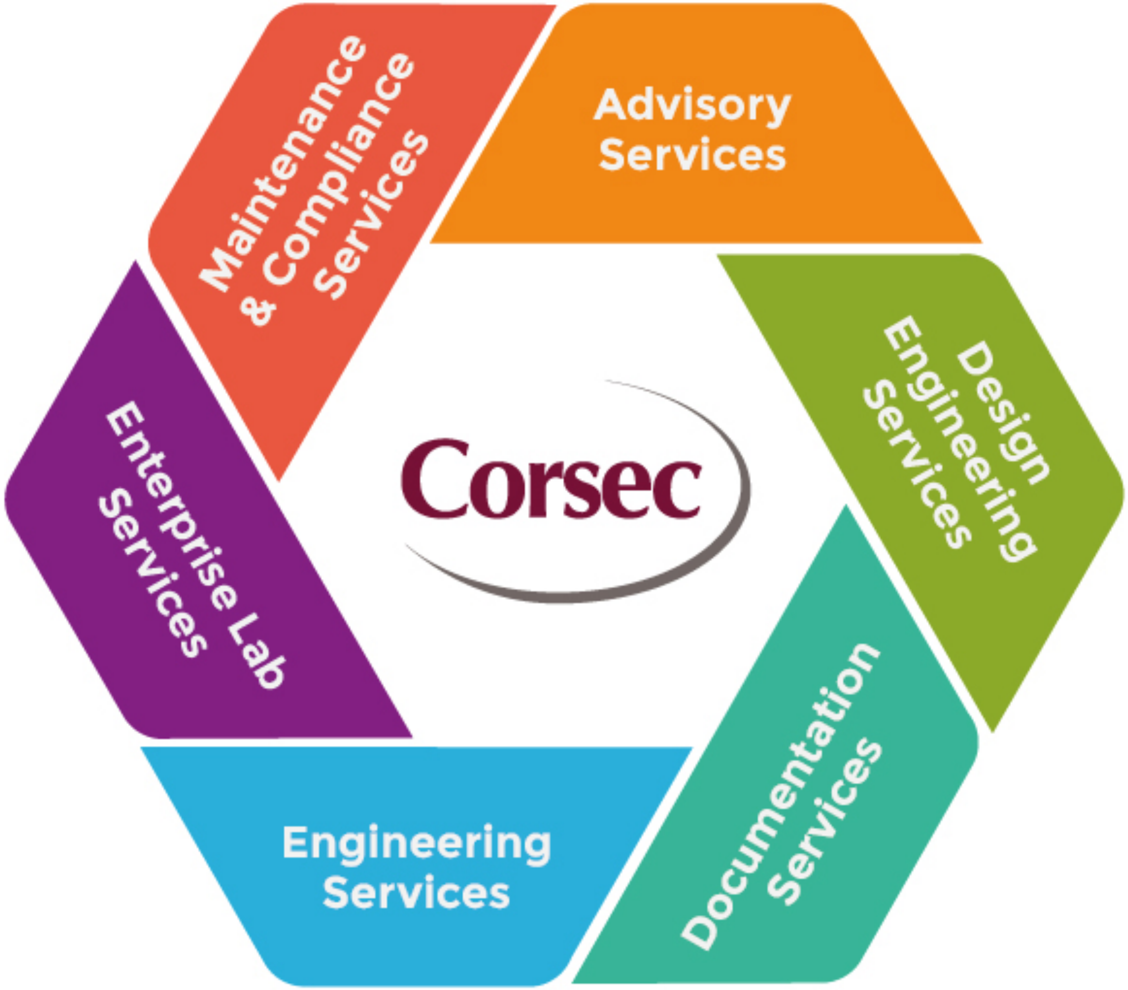
- At the time of original submission – 1, 1A, 1B, and 4
- At the time module is submitted to CMVP – 2, 3 and 5

Active List	• 1, 1A, 1B, 2, 3, 4 and 5
Historical List	• 1 (administrative updates) • 3 (for up to 2 years after the sunset date)
Retesting	• 1 (if adding previously untested approved security functions) • 1B (at lab's discretion) • 3, 4 and 5
Regression Testing	• 3
New Certificate	• 1A, 1B, 2, 3 and 5
Sunset Date Inherited	• 1, 1A, 1B and 4
Sunset Date Changed	• 2, 3 and 5 (5 years from the validation date)

Corsec

Why Corsec?

A Turnkey Engagement



Corsec

Some of the Clients We Serve

totemo ag

SONICWALL

TippingPoint

riverbed

CERTES NETWORKS

CYBERARK

GENERAL DYNAMICS

ciena

hp

QinetiQ North America

crossbeam

NUTANIX

HUGHES

CISCO

extreme networks

CITRIX

Tintri

HARRIS

BOMGAR

FORUMSYSTEMS

SOLIDFIRE

CURTISS WRIGHT

NETEZZA

NetApp

vmware

EMC2 where information lives

Vidyo

WatchGuard

ORACLE

SECURED SERVICES

Allegro

Corsec

Questions?

Need further information?

Additional questions?

Your Corsec Contact

Shashi Karanam| Senior Certifications Consultant

+1 (703) 267-6050 x129 | skaranam@corsec.com