Recent and Upcoming Changes in the CMVP

2018-07

This newsletter is intended to inform our customers about the recent changes that have been published on the NIST Cryptographic Module Validation Program (CMVP) website as well as upcoming changes. We are standing by our customers and preparing you for these changes that may have an impact on your cryptographic modules.

Implementation Guidance (IG)

The current version of the IG was published on **May 25th** and is available at: https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/fips140-2/fips1402ig.pdf

Modified Guidance

IG G.8 Revalidation Requirements
Removed the “2 year” limitation on 3sub revalidations, which stated that modules on the historical list could not be submitted as a 3sub if the module’s sunset date exceeded 2 years. Now, modules that are Active or Historical are eligible for scenario 3 revalidation without this limitation.

IG 9.11 Reducing the Number of Known Answer Tests
Changed the “type” of the parameter that “remembers” that self-tests were run successfully on a specific environment, from a CSP, to something that is treated the same as a public key, in which case the integrity of this parameter is assured by the module.

NIST CMVP Fees

The following fee structure is effective October 1, 2018:

- **IG G.8** Scenario's 1, 2 and 4: CR fee N/A, ECR fee: $1000
- **IG G.8** scenario's 1A and 1B: CR fee $2000, ECR fee: $1000
- **IG G.8** Scenario 3: CR fee $4000, ECR fee: $1500
- **IG G.8** Scenario 5:
  - Security Level 1: CR fee: $8000, ECR fee: $3000
  - Security Level 2: CR fee: $10000, ECR fee: $4000
  - Security Level 3: CR fee: $10000, ECR fee: $4000
  - Security Level 4: CR fee: $10000, ECR fee: $4000

Automated Cryptographic Validation System (ACVS)

Per the NIST’s plan, an Automated Cryptographic Validation System (ACVS) for algorithm testing is expected to be launched **in the September/October of 2018.**

CMVP Report Queue

The NIST CMVP informed all CST laboratories on June 6 that NIST was continuing to work through contract issues which has put a “stop work” on the contract which provides report review and software development support for the NIST CMVP. The “stop work” commenced on May 29th and may last up to 100 days. Until a resolution is reached, queue times will be affected.