DCI MEMORANDUM ON FIPS 140-3

Approved 19 December 2019
Digital Cinema Initiatives, LLC, Member Representatives Committee

The long anticipated arrival of FIPS 140-3, "Security Requirements for Cryptographic Modules" was announced in the Federal Register on May 1, 2019. FIPS 140-3 will supersede FIPS 140-2, which is currently used by the digital cinema community.[1]

Pursuant to the current NIST schedule (detailed below), devices will be able to be submitted for testing to FIPS 140-3 starting September 22, 2020. One year later, **on September 22, 2021 no new devices may be submitted to a FIPS testing lab for testing to FIPS 140-2, effectively sunsetting FIPS 140-2.**

DCI Compliance to FIPS 140-3

DCI believes the new standard maintains assurance of a satisfactory threshold of security for the d-cinema industry. DCI will require FIPS 140-3 compliance in new devices once FIPS 140-2 sunsets in September 2021. Therefore, DCI strongly urges suppliers to create new designs to FIPS 140-3.

DCI will embrace the migration to FIPS 140-3 by publishing new errata that evolve the Digital Cinema System Specification (DCSS) to include references to both FIPS 140-2 and 140-3 for purposes of Media Block FIPS certification. In the year of overlap between the start of 140-3 testing and termination of 140-2 testing, Media Block suppliers will be free to choose under which standard they seek certification.

DCI will continue its policy that once a Media Block (or any Secure Processing Block) has been FIPS certified, the design will continue to be recognized as DCSS compliant. For purposes of future-proofing Media Blocks, DCI strongly urges suppliers to design to FIPS 140-3 sooner than later.

FIPS 140-3 Details and References

FIPS 140-3 relies upon two existing international standards:[2]

- International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 19790:2012(E) *Information technology – Security techniques – Security requirements for cryptographic modules;* and
- ISO/IEC 24759:2017(E) *Information technology – Security techniques – Test requirements for cryptographic modules.*

The new NIST Special Publication (SP) series 800-140*x* will specify updates, replacements, or additions to the currently-cited ISO/IEC standards, as necessary. The SP 800-140*x* documents will consolidate implementation and administrative guidance.[3]

[1] https://www.nist.gov/news-events/news/2019/05/announcing-approval-and-issuance-fips-140-3-security-requirements
[2] https://csrc.nist.gov/publications/detail/fips/140/3/final
[3] https://csrc.nist.gov/projects/fips-140-3-development#sp800-140

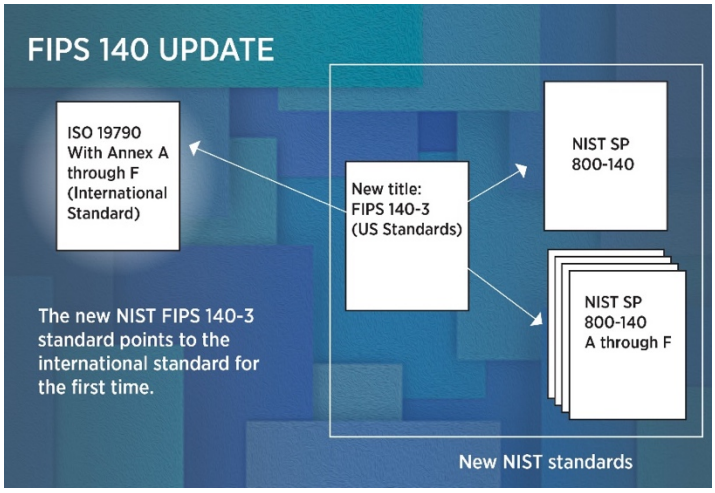
FIPS 140-3 testing via the Cryptographic Module Validation Program (CMVP)[4] schedule details are:[5]

Implementation Schedule

Current Schedule - 9-26-2019

Date	Activity
March 22, 2019	*FIPS 140-3 Approved*
September 22, 2019	*FIPS 140-3 Effective Date* *Drafts of SP 800-140x available for public comment (See status page)*
March 22, 2020	*Publication of SP 800-140x documents* *Implementation Guidance updates* *Tester competency exam updated to include FIPS 140-3* *Updated CMVP Program Management Manual*
September 22, 2020	*CMVP accepts FIPS 140-3 submissions*
September 22, 2021	*CMVP stops accepting FIPS 140-2 submissions for new validation certificates*
September 22, 2026	*Remaining FIPS 140-2 certificates moved to Historical List*

Regarding reliance on the ISO/IEC standards, NIST states "the newly released FIPS 140-3 modernizes the standard and essentially makes the U.S. standard a 'pointer' indicating that manufacturers should now use the international standard, which NIST helped to develop. Any product that adheres to the international standard – known as ISO 19790 – will therefore use an encryption approach that is acceptable both within and outside the United States."[6]



[4] https://csrc.nist.gov/projects/cryptographic-module-validation-program
[5] https://csrc.nist.gov/projects/fips-140-3-transition-effort
[6] https://www.nist.gov/news-events/news/2019/04/nist-links-federal-encryption-testing-international-standard-first-time