SmartSuite

Framework / Cybersecurity / Other

FIPS 140-3

FIPS 140-3 is the U.S. standard for cryptographic modules, validated by CMVP at four security levels; effective September 22, 2019, it adopts ISO/IEC 19790 and 24759.



What it is

FIPS 140-3, Security Requirements for Cryptographic Modules, is the U.S. federal standard that every cryptographic module protecting sensitive but unclassified federal information must meet, at one of four security levels, and that is enforced through validation by the Cryptographic Module Validation Program (CMVP). The Secretary of Commerce approved it on March 22, 2019, it took effect on September 22, 2019, CMVP began accepting FIPS 140-3 submissions on September 22, 2020, and on September 21, 2026 all remaining FIPS 140-2 certificates moved to the Historical List.

At a glance

PUBLISHER
National Institute of Standards and Technology (NIST); approved by the Secretary of Commerce; validation by the CMVP (NIST and Canada's CCCS)

TYPE
Standard

VERSION
FIPS 140-3 (March 22, 2019), adopting ISO/IEC 19790:2012 and ISO/IEC 24759:2017 with the NIST SP 800-140 series

EFFECTIVE
September 22, 2019 (CMVP testing from September 22, 2020)

DOMAIN
Cybersecurity

FAMILY
Other

REGION
United States

INDUSTRY
Government & Public Sector

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
High

Source: csrc.nist.gov/pubs/fips/140-3/final

Why it matters

- **Four graded levels** Level 1 to Level 4 raise the requirements for physical security, authentication and tamper response so a module can match the data and environment it protects (standard, section 3 and Applications).
- **One international basis** Adopting ISO/IEC 19790:2012 and 24759:2017 aligns U.S. and Canadian validation with the standard other schemes test against, limiting FIPS-specific differences to the SP 800-140 annexes.
- **A public register** The CMVP Validated Modules list records each certificate, its level, approved algorithms and security policy, and the Historical and Revoked statuses that govern use.
- **Fixed transition dates** CMVP stopped accepting FIPS 140-2 submissions for new certificates on April 1, 2022 and moved all FIPS 140-2 certificates to the Historical List on September 21, 2026.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports FIPS 140-3

Module Inventory with Certificate Status

Record each cryptographic module, its CMVP certificate number, validation standard (140-2 or 140-3), security level, Active, Historical or Revoked status and five-year sunset date.

Approved Mode Configuration

Document for each deployment that the module runs in the approved mode and uses only algorithms listed in its security policy, with the evidence attached.

Data Flow Encryption Map

List data at rest, data in transit across and within the boundary, remote access, key management and authentication, and the validated module covering each.

Transition Tracking

Flag systems still on FIPS 140-2 modules, now Historical, and plan the replacement module, owner and date for each.

Supplier Certificate Watch

Track the modules in vendor products and the certificates they depend on, with alerts before a sunset or status change.

Control Evidence for SC-13

Link module records to the SC-13 and SC-8 or SC-28 control statements in each system's authorization package.

Common framework mappings

ISO 27001:2022 | NIST 800-53 Rev.5 | PCI DSS 4.0.1 | SOC 2

Official resources

FIPS 140-3 Standard

Defines security requirements for cryptographic modules to protect sensitive information.

csrc.nist.gov/publications/detail/fips/140/3/final

FIPS 140-3 Implementation Guidance

Provides guidance on implementing cryptographic module requirements as per FIPS 140-3.

csrc.nist.gov/publications/detail/sp/800-140c/final

Cryptographic Module Validation Program (CMVP)

Outlines the program for validating FIPS 140-3 compliant cryptographic modules.

csrc.nist.gov/projects/cryptographic-module-validation-program

NIST SP 800-140x Series

Describes supporting documents for FIPS 140-3, including operational and security guidance.

csrc.nist.gov/publications/sp#800-140

Frequently asked questions

What are the four FIPS 140-3 security levels?

The standard provides four increasing, qualitative levels, Level 1 to Level 4, intended to cover the range of applications and environments in which modules are used. The requirements for a level include those specific to it and those that apply to all modules; the level must be chosen to suit the security the application and environment require.

What does FIPS 140-3 actually contain?

Very little of its own. It adopts ISO/IEC 19790:2012 for security requirements and ISO/IEC 24759:2017 for testing, and section 3 lists the NIST SP 800-140 series that modifies them: SP 800-140 (derived test requirements) and SP 800-140A to F for documentation, security policy, approved security functions, sensitive security parameter methods, authentication and non-invasive attack metrics.

Can I still use FIPS 140-2 validated modules?

Only in existing systems. CMVP stopped accepting FIPS 140-2 submissions for new certificates on April 1, 2022, and on September 21, 2026 all FIPS 140-2 certificates moved to the Historical List, which the standard says should not be used for procurement decisions. New procurements need an Active FIPS 140-3 certificate.

How does a module get validated?

The vendor engages an NVLAP-accredited Cryptographic and Security Testing laboratory, which tests the module against ISO/IEC 24759 as modified by SP 800-140 and submits the report to CMVP, a joint NIST and Canadian program. CMVP reviews it and issues a certificate that stays Active for five years, or two years for the interim validations introduced on June 6, 2024.

 © 2026 SmartSuite Inc. All rights reserved.

Is FIPS 140-3 mandatory outside federal agencies?

The standard is mandatory for federal agencies and for modules operated for them under contract; private organizations may adopt it voluntarily. In practice NIST SP 800-53 control SC-13 and FedRAMP's cryptographic module rules require FIPS-validated modules, so suppliers to government meet it by reference.

License included / downloadable: Yes FIPS 140-3 and the SP 800-140 series are U.S. government works available free of charge from NIST; the ISO/IEC 19790 and 24759 standards it adopts are sold by ISO and are not included.

Full framework page and mappings: smartsuite.com/frameworks/fips-140-3-security-requirements-for-cryptographic-modules

© 2026 SmartSuite Inc. All rights reserved.