SmartSuite

Framework / Cybersecurity / NIST Special Publications

FIPS 140-3

FIPS 140-3 specifies security requirements and validation procedures for cryptographic modules to protect sensitive government and regulated data.

What it is

FIPS 140-3 is a U.S. government standard that establishes security requirements for cryptographic modules protecting sensitive but unclassified information. Its primary purpose is to ensure the confidentiality and integrity of data in government and regulated industry systems through robust cryptographic controls.

Published by the National Institute of Standards and Technology (NIST), FIPS 140-3 is widely utilized by federal agencies and contractors, as well as organizations in sectors subject to regulatory oversight. The standard focuses on the validation and assessment of cryptographic modules, addressing areas such as key management, module authentication, physical security, and self-tests to support cybersecurity and compliance requirements.

At a glance

PUBLISHER National Institute of Standards and Technology (NIST)	TYPE Standard	VERSION FIPS 140-3
EFFECTIVE March 22, 2019	DOMAIN Cybersecurity	FAMILY NIST Special Publications
REGION United States	INDUSTRY Government & Public Sector	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY High		

Source: https://www.wolfssl.com/license/fips/?gad_source=1&gad_campaignid=916470942&gbraid=0AAAAAD_TYV3-i3dDirD40Mw2qyiU1zBNe&gclid=CjwKCAiAjc7KBhBvEiwAE2BDOc01pRiLki-W1jPNthQ11_qNWg-m81Nqi0Izu_NHmMRHsFUVHPafThoCPa0QAvD_BwE

Why it matters

- **Strengthen data protection practices** Ensure cryptographic solutions effectively safeguard sensitive but unclassified information across diverse hardware and software environments.
- **Enhance regulatory compliance** Demonstrate adherence to government and industry security requirements, enabling smoother audits and facilitation of contractual obligations.
- **Enable robust risk management** Support identification, assessment, and mitigation of data security risks through comprehensive requirements for cryptographic module validation.
- **Improve operational resilience** Increase reliability and continuity of business operations by reducing vulnerabilities in cryptographic mechanisms that underpin critical systems.

How SmartSuite supports FIPS 140-3

Crypto Module Inventory and Versions

Track cryptographic modules, validated versions, and where they're deployed.

Validation Evidence Repository

Store validation artifacts, configuration requirements, and module documentation.

Change and Release Governance

Manage updates that impact crypto modules with approvals and impact evidence.

Deployment Configuration Tracking

Document approved configurations and proof deployed systems match requirements.

Vendor and Library Oversight

Track third-party crypto dependencies, attestations, and monitoring.

Module Coverage and Version Compliance Reporting

Report module coverage, version compliance, and open issues across systems.

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 is FIPS 140-3 used for?

FIPS 140-3 is used to define security requirements for cryptographic modules protecting sensitive but unclassified information in government and regulated industry systems. It ensures that cryptographic mechanisms meet stringent standards for confidentiality, integrity, and authenticity. Implementation of FIPS 140-3 is essential for compliance with federal cybersecurity requirements.

Is FIPS 140-3 certification mandatory?

FIPS 140-3 validation is mandatory for cryptographic modules used in U.S. federal agencies and often required by contractors and regulated industries. Only modules listed as validated by NIST through the Cryptographic Module Validation Program (CMVP) are considered compliant. Organizations operating in federally regulated environments typically must use validated cryptographic modules.

What systems or environments does FIPS 140-3 apply to?

FIPS 140-3 applies to IT systems within U.S. federal agencies and organizations handling federal data, including government contractors and regulated industries such as healthcare and finance. It covers use cases where cryptographic modules are deployed to protect sensitive but unclassified information. The standard can also be referenced by private sector entities for best practices.

What are the four security levels in FIPS 140-3?

FIPS 140-3 defines four security levels, each with increasing requirements for physical security, module authentication, tamper-resistance, and key management. Level 1 provides basic protections while Level 4 offers the most comprehensive safeguards, including robust defenses against physical and environmental attacks. Organizations select the appropriate level based on their risk profiles and regulatory needs.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How does FIPS 140-3 validation work?

Vendors submit cryptographic modules for testing by accredited laboratories under the CMVP. Assessment covers areas such as key management, physical security, authentication, self-tests, and tamper-resistance. Upon successful validation, modules are listed on the NIST validated modules list, confirming their compliance with FIPS 140-3.

How does FIPS 140-3 relate to other standards like NIST SP 800-53?

FIPS 140-3 is often referenced in conjunction with frameworks such as NIST SP 800-53, which outlines broader security controls for federal information systems. While FIPS 140-3 focuses narrowly on the technical standards for cryptographic modules, it supports compliance with higher-level requirements found in broader risk management and cybersecurity frameworks.

What ongoing compliance requirements exist for FIPS 140-3?

Organizations must ensure that only NIST-validated cryptographic modules are deployed, track module versions, and monitor for status updates or revocation. Regular reviews of cryptographic inventories, documentation of compliance evidence, and readiness for audits are necessary to maintain ongoing FIPS 140-3 compliance.

How would SmartSuite support FIPS 140-3?

SmartSuite enables organizations to track the deployment and status of FIPS 140-3 validated cryptographic modules, manage associated cryptographic policies, collect compliance evidence, and document control implementation. It facilitates audit readiness by centralizing evidence and providing reporting tools, helping organizations demonstrate adherence to federal standards and monitor compliance over time.

License included / downloadable: Yes FIPS 140-3 is a U.S. federal standard published by the National Institute of Standards and Technology and is publicly available through official NIST publications.

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