CIGENT
AlwaysPROTECTED™

What you need to know about FIPS 140-2

What you need to know about FIPS 140-2

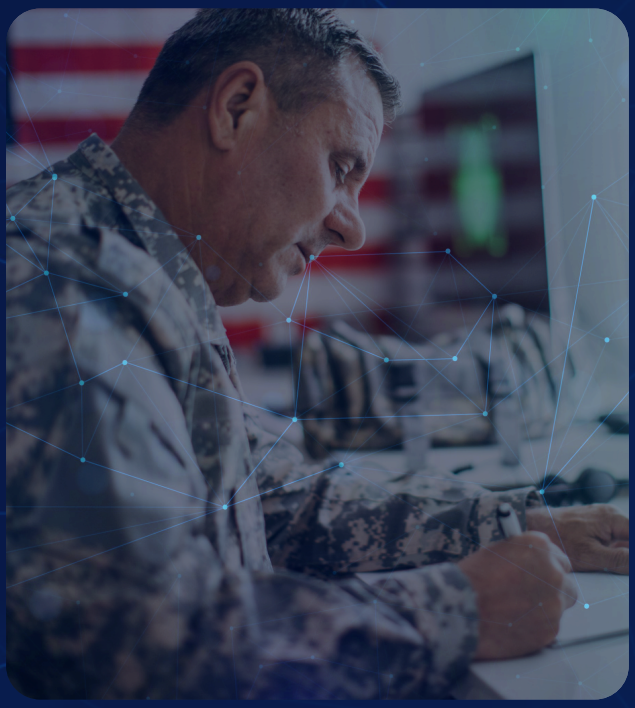
Federal Information Processing Standards, FIPS for short, detail the Federal Information Security Management Act (FISMA) was passed in December 2002. The National Institute of Standards and Technology (NIST) codified standards for cryptographic modules that protect sensitive information in a publication entitled Security Requirements for Cryptographic Modules, better known as FIPS 140-2.

With decades of experience in advanced cryptography and in complying with FIPS, Cigent has been providing the highest level of data security for federal agencies for nearly 40 years. We have always taken a modern "next-gen" approach to stay ahead of adversaries with proactive solutions across all aspects of the threat landscape.

At Cigent, we say: ***"We don't just know data security—we are leading the way."*** That is why we have compiled this comprehensive guide to FIPS 140-2. When you are well-informed, we can more effectively partner with you for FIPS solutions that provide exceptional security and efficient compliance with FIPS 140-2 from Level 1 through Level 3.

Importance of encryption in data security

FIPS 140-2 standards are the key to data trust Cryptography protects sensitive information by ensuring that only those authorized to access it have the ability to decrypt and use it. Thus, encryption and decryption are essential to maintaining the confidentiality and integrity of data.



By establishing security specifications for cryptographic modules—essentially the hardware, software, and firmware that work together to deny unauthorized people from gaining access to data—FIPS 140-2 provides a standard of trust. Data owners and users know that the information they send and receive has not been modified in transit, tampered with at rest, and can't be accessed by adversaries.

Cryptography is a critical component of cybersecurity

Cybersecurity is an umbrella term for the technologies, tactics, practices, and policies that protect data and systems. Cryptography contributes in several ways:

- **Data integrity:** Cryptography ensures data has not been accessed, tampered with, or stolen.
- **Identify verification:** With strong authentication methods, only valid authorized users can access sensitive data or systems.
- **Compliance:** When processes and tactics for protecting data are certified to meet strict standards like those detailed in FIPS 140-2, federal agencies can be confident in the security of their systems and data.
- **Private sector alignment:** When contractors and sensitive industries like finance, healthcare, and technology align along the same standard, data can flow securely between the two.
- **Key management:** If the encryption keys that lock and unlock data are compromised, security no longer effectively exists. Standards ensure secure management of keys to keep systems secure.

Understanding FIPS: Purpose, levels, and requirements

FIPs 140-2 standards seek to ensure that each of the components of a cryptographic solution can provide sufficient and effective security to protect sensitive data and systems. FIPS 140-2 covers secure communications, authentication methods, digital signatures, and, of course, data encryption and decryption.

FIPS 140-2 is a U.S. government standard that applies to all U.S. federal agencies. Many private sector organizations have adopted the standard, and it is recognized and used globally.

FIPS 140-2 security levels

Because the sensitivity of systems and data varies across agencies, cryptographic security standards are not one size fits all. FIPS 140-2 specifies four levels of security. Each one builds on the other, requiring stricter and stricter security controls.

Level 1: Basic security

Though this level represents the lowest level with the fewest security requirements, FIPS still specifies strong fundamental protections. The focus at this level is on properly implementing encryption software on general-purpose, off-the-shelf operating systems and devices. In many cases, cryptography is embedded in the firmware, particularly if it is a networked device or component. Hardware is not protected by physical security mechanisms at this level. Level 1 also does not require authentication and specifies the most basic of key management controls. It does require power-on self-testing to verify the correct function of cryptographic algorithms and continuous integrity checks. This level of FIPS 140-2 is for devices used in low-risk environments like a data center.

Level 2: Adding physical security and authentication

Additional safeguards add to device security. This level mandates physical security in the form of tamper-evident protections. Seals or protective coatings that would slow unauthorized users from accessing internal components are examples. These protections make it possible to detect if anyone has attempted to physically access drives or data. Level 2 also requires access control with role-based authentication functionality. Users authenticate using a PIN or password to access certain data and software, with those in administrator roles having greater access. FIPS approves specific Level 2 cryptographic algorithms, such as AES, RSA, SHA, and Triple DES. It also specifies key management procedures for generating, storing, and destroying cryptographic keys. As in Level 1, Level 2 modules self-test upon power-on and run ongoing integrity checks. In an error state, the module suspends cryptographic operations. Level 2 is suitable for devices used in semi-secure environments, like an office.

Level 3: Enhanced security

This level of FIPS 140-2 requires more rigorous security physical security and demands strict user authentication. Whereas Level 2 specified tamper-evident physical security, Level 3 requires modules to be tamper-resistant. Not only must accessing components be made extremely difficult, but the device must also detect tampering and take action to protect data, such as zeroizing cryptographic keys and sensitive data. This level goes beyond role-based authentication to uniquely identify individual users. User names and passwords are not enough. Those seeking access may need to use multifactor identification or a hardware token. This level has more stringent key management requirements for establishing such keys, protecting them, and zeroizing them if tampering is detected. Self-testing, error state responses, and robust error reporting make it possible to identify and resolve issues that could compromise security, Level 3 is required when a device is exposed to high-risk environments where physical attacks or malicious tampering are possible.

Level 4: Highest security for high-risk environments and the most sensitive data

This level provides the toughest physical protection to safeguard data and systems from highly sophisticated attacks and environmental threats. This level of protection goes far beyond what is commercially available off-the-shelf. Level 4 requires tamper-evident, tamper-resistant, and tamper-responsive elements. If tampering is detected, the system must fully erase all cryptographic keys and data. Physical protections extend to addressing environmental attacks such as voltage spikes, magnetic interference, and high temperatures that might be used to manipulate a module to reveal sensitive data. This level requires the most stringent identity-based authentication, such as requiring both a smart card and a biometric scan. The highest-level key management protects the systems, and comprehensive self-testing, integrity checks, error-and-response, and reporting are required. Software and firmware protections are also specified. When data, devices, and systems face extreme security risks and where the most sensitive data is being handled, Level 4 is required.

Importance of FIPS in compliance frameworks

FIPS 140-2 works within other security standards, notably NIST 800-171 and CMMC Level 2. All three work together to protect the sensitive information within U.S. federal agencies, the Department of Defense, and their contractors. These standards overlap and interconnect.

NIST 800-171: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

The NIST 800-171 standard provides guidance on protecting controlled but unclassified information (CUI) in federal data systems, primarily for the Department of Defense and its contractors. It covers processing, storing, and transmitting CUI, and covers topics such as access control, incident response, configuration management, and encryption in its Control 3.13.11 security requirement. That is where it overlaps with FIPS 140-02. Where NIST 800-171 mandates cryptographic protection, FIPS defines the standards for the cryptographic modules used to comply with those mandates.

CMMC (Cybersecurity Maturity Model Certification) Level 2 Certification

The CMMC cybersecurity framework adds on to NIST 800-171, and, again, protects CUI. It requires DoD contractors to adopt and use robust and proven security practices. It includes the NIST 800-171 cybersecurity framework and requires contractors to demonstrate their security posture across incident detection and response, risk management, and training around security awareness and practices. These include encryption, specifically around data access, encryption key management, and cryptographic solutions.

FIPS 140-02 Validation

Federal agencies may only use cryptographic modules that have gone through a formal certification process that documents and validates that the hardware and software components used to encrypt and decrypt information actually does meet the FIPS 140-02 standards. The process ensures that only cryptographic modules that follow the most up-to-date best practices for handling sensitive data at rest and in transit are used by federal agencies.

Compliance vs. validation

- Cryptographic modules that have completed the NIST Cryptographic Module Validation Program (CMVP) are thus validated.
- If a module uses the principles of FIPS 140-2 but hasn't been through the testing, some can claim the module is "compliant." Federal agencies cannot use modules that merely claim to be "compliant" and private sector organizations should proceed with caution in using these modules.

Steps to becoming FIPS 140-2 validated

Federal agencies must follow the following steps to ensure that their cybersecurity is FIPS 140-02 validated:

1. **Design:** Develop cryptographic modules using FIPS 140-2 requirements from the ground up, using approved cryptographic algorithms and key management approaches. Potential components include:
    - Cryptographic algorithms
    - Key management processes
    - Physical security measures
    - Software and firmware protections
    - Self-test, integrity, and reporting

2. **Test:** Send modules to a NIST-accredited cryptographic and security testing laboratory. The lab tests designs, how solutions are implemented, and if physical security measures meet FIPS 140-2 requirements.

3. **NIST review:** As part of the NIST CMVP, the organization will review designs, test results, and documentation to ensure the module complies with FIPS 140-2.

4. **Validation:** This formal step approves the module for use in government applications, issues the solution a FIPS certificate number, and publishes its availability on the NIST website.

Identifying Genuine FIPS-Compliant Products

Only modules that are verified and certified by the NIST CMVP are actually FIPS- 140-2 compliant.
That does not stop some vendors from suggesting FIPS compliance without having gone through the testing process. The use of phrases such as “FIPS compliant,” “partially FIPS compliant,” or “FIPS inside” are at best ambiguous and, at worst, misleading. In a high-trust environment, these kinds of claims cannot be tolerated.

It is clear from the validation process outlined above that FIPS compliance begins at the design phase. Getting a module validated that doesn’t begin and end with FIPS guidance is a tall order.

Federal agencies may only use validated cryptographic modules listed in the NIST database that bear a genuine FIPS certificate number. Non-validated components are a severe security risk. Be sure to go through product documentation in detail to make sure each component is, indeed, validated. Generic claims are highly suspect.

Challenges in implementing FIPS encryption

Implementing FIPS 140-2 encryption modules requires meeting stringent certification requirements. Organizations face both technical and operational challenges, particularly in complex systems that are always evolving. These challenges include:

Varying IT environments and compatibility issues
IT environments can be described as highly intricate landscapes of technologies and interdependencies. Diverse hardware, software, operating systems, drivers, and interfaces, third-party integrations, and security requirements barely scratch the surface of the potential complexities.

Impact on legacy systems
Replacing outdated encryption modules and methods is an arduous process that often requires the re-architecting of systems in whole or in part. Not all legacy components will support FIPS encryption. Older hardware and custom applications can be serious roadblocks.

Budget constraints and resource limitations
Money and manpower shortages are real. Resources must be moved off mission-critical work to implement FIPS, which is not an easy thing to ask. In some cases, it is an impossibility.
spect.

Overcoming obstacles: Best practices for FIPS migration

FIPS compliance is simply mandatory for federal agencies, no matter what obstacles you face. These strategies and best practices can mitigate the challenges and lead to successful implementation.

1. **Use pre-validated cryptographic modules**
   Using off-the-shelf solutions saves time, allowing you to focus on your issues versus getting bogged down in a lengthy validation process.

2. **Use a risk-based approach to compliance**
   Assess your environment and prioritize those aspects that are most critical and most at risk first. Apply FIPS only where you must, so you can focus your resources on your priorities.

3. T**ake an incremental upgrade approach**
   Reduce disruption and slowdowns by deciding what needs modernizing first. Explore the possibility of placing FIPS-validated wrappers around critical legacy systems.

4. **Work with a FIPS expert vendor**
   Collaborate with vendors that have extensive cryptographic experience and that have a documented history of successful FIPS implementation. They know how the process works, how you can expedite your project, and know the best tools to use.

Resources for FIPS implementation

- For full-drive encryption, use NSA-validated AES-256-bit hardware with pre-boot authentication and multi-factor authentication built into the same solution.
- Use existing secure storage solutions that work on-premises and in the cloud with a direct command line interface for Linux and Windows operating systems.
- Adopt an ecosystem that works with the major CSfC integrators, such as FRL, Booz Allen, CACI, and Exerfox that have a solid track record of trust.
- Streamline procurement with approved equipment from Dell, HP, and GETAC.

Key takeaways

The crucial role that FIPS 140-2 plays in ensuring that sensitive data and systems are protected by reliable and up-to-date cryptography cannot be overstated. FIPS-compliant cryptography is mandatory for agencies that handle CUI. That is why it is vital to use FIPS-validated modules and to work with experts in FIPS compliance who can help you overcome obstacles and achieve compliance to secure critical data and IT infrastructure, both for achieving your mission and maintaining public trust.

How Cigent Can Help

The Federal Information Processing Standard (FIPS) 140-2, defined by NIST, is a set of standards that define the security requirements for cryptographic modules used to protect sensitive information. Cigent portfolio of Secure Storage provides organization with a secure, proven, and efficient solution to meet FIPs 140-2 Level 3 requirements.

Full Drive Encryption

Cigent's solution uses proven, and NSA validated encryption methodology, including full drive AES-256-bit hardware encryption. Organizations seeking to elevate their security can utilize pre-boot authentication and multi-factor authentication with the same solution.

Enterprise Administration

Cigent provide scalable management of its Secure Storage Solutions including enterprise management console that can be deployed on premise and in the cloud. Additionally, Cigent offers a Command Line Interface (CLI) for Linux and Windows devices.

Robust Ecosystem

Cigent is working with all major CSfC integrators including AFRL, Booz Allen, CACI, and Exerfox to enable your mission requirements. With successful deployments including SecureView and Data Defense the Cigent solution is tested and trusted by leading security experts.

Easy to Acquire

Cigent seeks to streamline your procurement process with Cigent Secure Storage available directly from major device manufacturers including Dell, HP, and GETAC.

Book a Demo with Cigent to see how we can help with FIPS Certification.