FIPS 140-2 Technical Brief

FIPS stands for Federal Information Processing Standard (FIPS). The U.S. and Canadian governments co-sponsor this software, hardware, and firmware security standard. In fact, all products sold to U.S. and Canadian federal agencies must complete FIPS 140-2 validation if they process Sensitive But Unclassified (SBU) information or protected information. Through the Cryptographic Module Validation Program (CMVP), cryptographic modules must be validated to FIPS 140-2 standards by accredited independent laboratories. Once products secure FIPS 140-2 validation, they get accepted by the federal agencies of both countries.

In this technical brief, we cover the key features of the FIPS 140 standard, the validation levels, and the applications and industries where it is required — as well as additional industries that may comply with this standard as a benchmark for cybersecurity of sensitive data.

FIPS 140-2: Use Cases Where Validation Is Required

If you work with the U.S. or Canadian governments and handle sensitive or protected information, your cryptographic modules must be validated to the FIPS 140-2 standard. The Federal Information Security Modernization Act (FISMA) requires U.S. government agencies, U.S. government contractors, and third parties working for federal agencies to adhere to the FIPS 140-2 standard to protect sensitive data. For example, all defense contractors and law enforcement agencies must meet FIPS validation requirements and employ "cryptographic mechanisms" to protect confidentiality. Private sector organizations that comply with regulations such as the Health Insurance Portability and Accountability Act (HIPAA) must also pass FIPS 140-2 validation.

FIPS 140-2 serves as a benchmark for cryptographic hardware effectiveness. In other words, if a product is validated for FIPS 140-2, it meets the rigorous requirements of the U.S. and Canadian governments. The FIPS standard isn't just for governments. Governmental and non-governmental sectors around the globe may comply with the FIPS 140-2 standard as a best practice for encryption and cybersecurity. Because this unified standard provides extraordinary data protection against increasingly sophisticated cyberattacks and threats, it provides a measurable definition for cybersecurity.

Failing to comply with FIPS can result in significant financial and reputational damage. For regulated industries such as government agencies, financial institutions and medical facilities, any significant lapse in compliance can mean these organizations suffer loss of business and in some cases civil or criminal penalties, fines and government audits.

FIPS 140-2 Validation Levels

Within FIPS 140-2, four security levels exist to which a cryptographic module can be validated to align with the appropriate security requirements of the intended application and environment. Each level includes successively stronger security measures, with Level 4 providing the highest level of security.

Security Level 1

FIPS 140-2 Security Level 1 requires the cryptographic module to provide essential security functions. Level 1 modules are typically implemented in software and do not require special hardware protections. Today, this is the validation required for most use cases.

For more information, visit:

www.digi.com

877-912-3444 | 952-912-3444

Security Level 2

FIPS 140-2 Security Level 2 builds on Security Level 1 requirements by adding the use of tamper-evident coatings, seals or pick-resistant locks on removable module covers or doors. These physical additions protect against unauthorized physical access.

Security Level 3

Security Level 3 uses strong enclosures and tamper detection/ response circuitry that erases all plaintext critical security parameters whenever anyone physically accesses the cryptographic module.

Security Level 4

In Level 4, the cryptographic module must detect and respond to tampering attempts in real-time, rendering the module inoperable if tampering is detected. Level 4 requires rigorous physical security including protection against environmental attacks.

The FIPS 140-2 Validation Process

FIPS 140-2 validated or certified means all security-related hardware and software components must be tested and approved by a National Institute of Standards and Technology (NIST)-accredited independent laboratory.

The Current National Voluntary Laboratory Accredited independent labs program includes the following labs:

- **UL Verification Services, Inc. San Luis Obispo, CA**
- **Booz Allen Hamilton Cyber Assurance Testing Laboratory Laurel, MD**
- **Leidos Accredited Testing & Evaluation (AT&E) Lab Columbia, MD**
- **Atsec Information Security Corporation Austin, TX**
- **Aegisolve, Inc. Mountain View, CA**
- **Advanced Data Security San Jose, CA**
- **Penumbra Security, Inc. Clackamas, OR**
- **Gossamer Security Solutions Columbia, MD**
- **Acumen Security Rockville, MD**
- **Cisco Systems Automated Cryptographic Validation Protocol Lab Morrisville, NC**
- **Google LLC Mountain View, CA**
- **Apple Inc. SECLAB Cupertino, CA**
- **Dekra Cybersecurity Certification Laboratory Sterling, VA**

Getting FIPS validated requires more than simply meeting FIPS requirements. To become FIPS validated, organizations must provide detailed documentation and source code to a NIST testing laboratory. The testing process can take six to nine months or more and cost hundreds of thousands of dollars. The laboratory will check for well-documented, engineered, and tested source code and then examine things such as file transfer and client/server applications independently for any security vulnerabilities, predictable number generation, or improper key management.

Digi has achieved FIPS 140-2 validation for all Digi devices based on the Digi Accelerated Linux operating system (DAL OS), which can be implemented via Digi Remote Manager®. See the full list of supported devices at the end of this brief.

OEMs building connected devices should consider the following to ensure your devices meet the FIPS 140-2 standard:

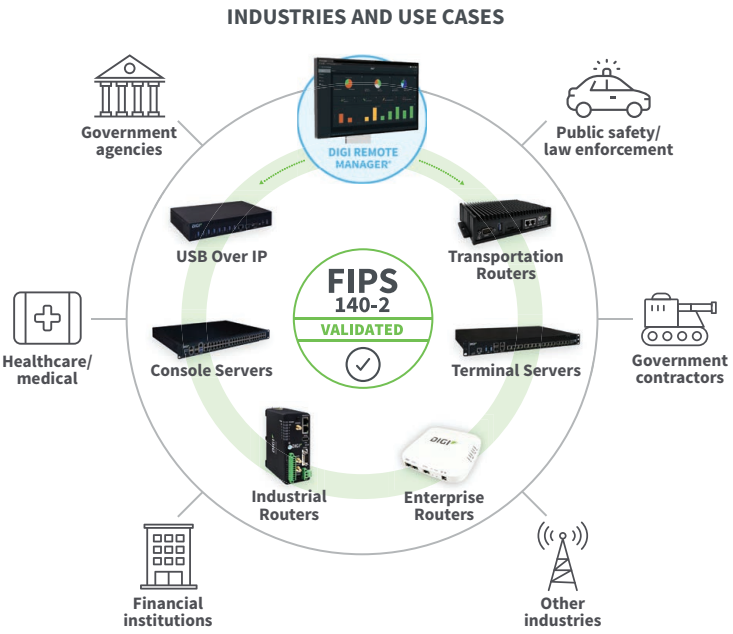
- Evaluate your design for potential vulnerabilities and assess your internal systems using FIPS guidelines. NIST and the Canadian Center for Cybersecurity (CCCS) have provided a guidance document that outlines and clarifies the FIPS 140-2 implementation process.
- Select a lab that aligns with your organization' requirements. Beyond fees, consider things such as team size, communication style, and track record for project completions.
- If your team lacks FIPS 140-2 implementation experience, it might make sense to have a lab provide additional support and helpful communication. Alternatively, a consultant that helps prepare the documentation and communication with the lab can help take the burden from your FIPS 140-2 team.
- Ensure that you have a method of providing ongoing firmware updates to deployed devices as the FIPS standard evolves. For example, Digi offers a complete ecosystem — the Digi ConnectCore® solution suite — for OEMs building connected devices, including security and cloud management services.

FIPS validation comes up for renewal every five years. Organizations must plan for future renewals to ensure products remain certified and thus remain on the market.

For more information, visit:

www.digi.com

877-912-3444 | 952-912-3444



Use Cases for FIPS 140-2 Validation and Compliance

Many use cases exist for cryptographic-based security systems. FIPS 140-2 compliance hardens security for computer and telecommunication applications, which includes data storage, access control and personal identification through network communications in offices and even hostile environments. The following use cases illustrate the wide-ranging applications for FIPS 140-2 compliance and validation.

For the purposes of this discussion, FIPS 140-2 *compliance* indicates that modules comply with the requirements of the standard, whereas FIPS 140-2 *validation* indicates that the modules have been officially tested and validated as compliant with the standard. For example, you can see Digi's certificate of validation for Digi devices based on the Digi Accelerated Linux operating system (DAL OS) here.

Government Agencies

All U.S. government agencies, law enforcement agencies and military organizations handle classified and sensitive information, and for this reason, FIPS 140-2 validation is mandated for all communication systems. FIPS 140-2-validated modules are used to secure command and control centers, as well as all data transfer and classified data storage. These modules provide the highest levels of security to prevent data breaches and unauthorized disclosures.

FIPS 140-2 is integral to U.S. government compliance with various laws and regulations, such as the Federal Information Security Modernization Act (FISMA) and the National Institute of Standards and Technology (NIST) guidelines. By following FIPS 140-2, government agencies demonstrate their commitment to upholding stringent cybersecurity measures and support the overall cybersecurity posture of the nation.

FIPS 140-2 validation of all cryptographic modules (hardware and software) in all U.S. government communication systems ensures the use of stringent encryption and access authorization standards. These requirements are essential to protect national security interests, safeguard sensitive government data, and maintain the trust of citizens in the security of government operations.

Government Contractors

All contractors working for the U.S. government are mandated to use FIPS 140-2 validated communication systems. For example, this includes defense contractors, as they handle sensitive Department of Defense (DoD) data. FIPS is required for any government contractor handling Controlled Unclassified Information (CUI) on any device. For example, the International Traffic in Arms Regulation addendum highlights the encryption FIPS 140-2 standards required for the transmission or storage of technical data outside the United States.

Contractors that do not meet validation requirements can pay a steep price for non-compliance. A federal contractor recently settled a $9 million case with the U.S. Justice Department for misrepresenting their compliance with cybersecurity requirements under the False Claims Act.

For more information, visit:

www.digi.com

877-912-3444 | 952-912-3444

Public Safety/Law Enforcement

FIPS 140-2 imposes stringent cryptographic security requirements on law enforcement agencies to protect sensitive data and communications. These requirements pertain to the use of cryptographic modules and algorithms in various aspects of law enforcement operations, such as secure communication systems, data storage, and access control.

Law enforcement agencies access the federal Criminal Justice Information System (CJIS) which requires FIPS 140-2 validated compliance to ensure the confidentiality, integrity, and authenticity of their data and communications. This includes employing approved cryptographic techniques, robust encryption algorithms, and secure key management practices. By complying with FIPS 140-2, these agencies can mitigate the risk of data breaches, unauthorized access, and cyberattacks, safeguarding critical information related to criminal investigations, national security, and public safety.

Medical/Healthcare

FIPS 140-2 compliance is likely to be increasingly required for all communication modules that can come into contact with sensitive data, which of course includes patient data. New cybersecurity laws are emerging that affect medical device manufacturers. For example, the Food and Drug Administration (FDA) is a U.S. federal agency, which means devices that transmit data to and from the FDA must be compliant.

Just as importantly, all organizations that utilize wireless modules (hardware and software) to access or transmit patient data can make use of this standard to ensure patient data is secure from hacking and data breaches.

According to securedata.com, over 37 million healthcare records experienced a breach in one year alone. Hackers pay thousands of dollars for stolen patient data on the dark web. For this reason, healthcare companies and medical device OEMs continue to adopt FIPS 140-2 compliance. Regulators and the healthcare industry see FIPS 140-2 as a critical part of medical device security because wirelessly connected devices increasingly store and transmit sensitive patient information.

Financial Institutions

FIPS 140-2 validation is required for all cryptographic modules in use by U.S. federal agencies and contractors, as discussed. This includes the Internal Revenue Service (IRS) and the Federal Reserve. But it is increasingly required for private sector financial institutions as well.

Several compelling use cases demonstrate how financial services can benefit from FIPS encryption. First, financial institutions can implement FIPS-compliant encryption protocols to secure online banking transactions to protect customer data, account information and financial transfers from unauthorized access. Communication between ATM machines, POS terminals, and the central banking infrastructure can also benefit from FIPS encryption to prevent skimming attacks, card data theft and unauthorized access to transaction data.

For secure data sharing, FIPS encryption can protect the communication of sensitive financial information between financial institutions, trading partners and regulatory bodies. This includes secure email communication and file transfers. FIPS encryption can even protect customer data and financial records stored in the cloud. International wire transfers and foreign exchange operations can take advantage of FIPS encryption to protect the confidentiality and integrity of financial information across borders.

For more information, visit:

www.digi.com

877-912-3444 | 952-912-3444

Other Industries

1. Energy

The energy sector has not so far mandated use of FIPS 140-2 for data encryption in wireless communication systems. But for very good reasons — including thwarting criminal attacks on critical infrastructure — this industry is highly likely to adopt stricter standards for wireless modules and data transfer.

Bitsight surveyed over 2,000 U.S. oil and energy companies and found that 62 percent of them are two times more likely to experience a ransomware attack based on their current cybersecurity performance. According to an update of S&P Global Energy Security Sentinel, oil assets and infrastructure accounted for a third of all cyberthreat incidents since 2017.

In 2022, the U.S. Department of Justice unsealed indictments of alleged efforts to compromise and control critical infrastructure through supply chain attacks, including a nuclear power plant. Complex, widely distributed energy infrastructure makes up a country's energy system and supports economic activity, national defense and emergency services. So, a cyberattack on the energy sector means serious financial losses and a threat to national security.

Electric utilities and power generation companies may use FIPS-compliant encryption algorithms and protocols to secure their communication networks and control systems. Energy companies in the oil and gas sector may use FIPS-compliant solutions to secure their data transmissions, such as those related to drilling operations, pipeline monitoring and remote sensor data.

Companies involved in building and maintaining smart grid infrastructure may rely on FIPS-compliant technologies to secure communication between smart meters, distribution networks, and centralized control centers. The highly sensitive nature of data transmission in the nuclear energy sector means FIPS 140-2 compliance is a viable solution to secure control systems and monitor data and communication networks of nuclear power plants.

Finally, companies providing maintenance, monitoring, and support services for energy infrastructure, such as substations and transmission lines, may use FIPS-compliant encryption and authentication mechanisms to ensure the security of their remote access and communication channels.

2. Transportation

FIPS 140-2 compliance can be employed to secure communication between train control systems, signaling equipment, and dispatch centers in rail and public transit systems. These measures can prevent cyberthreats from compromising train operations, schedules, and passenger safety.

As the transportation industry moves towards connected and autonomous vehicles, FIPS-compliant security measures can protect communications between vehicles, infrastructure, and central management systems. This prevents unauthorized access and potential hacking of autonomous vehicle functions. FIPS encryption can be applied to traffic management and control systems, including traffic lights, cameras, and sensors. This prevents tampering with traffic signals and data, reducing the risk of accidents and congestion. Emergency responders can employ FIPS 140-2-based encryption to ensure secure communication between response teams, command centers, and transportation resources during crises.

3. Manufacturing

Manufacturers rely on computerized systems, industrial control systems (ICS), and IoT devices for production and supply chain management. These systems frequently handle sensitive data, including proprietary designs, production schedules and intellectual property. By utilizing FIPS 140-2 compliant devices in their operations and communication systems, manufacturers can

For more information, visit:

www.digi.com

877-912-3444 | 952-912-3444

ensure that cryptographic modules used in these systems adhere to stringent security standards to protect against unauthorized access, data breaches and cyberthreats.

According to Blackberry, 43 percent of ransomware attacks on manufacturing systems disrupted operations for more than a week. Even more compelling is that 47 percent of manufacturing data breaches happen because of exploited vulnerabilities. The cost of a data breach can reach millions of dollars. Because FIPS 140-2 offers both an effective and available cryptographic standard, manufacturers increasingly use FIPS 140-2 compliant devices.

FIPS 140-2 compliance provides enhanced data integrity, confidentiality, and authentication. It ensures that encryption and cryptographic techniques used in these systems are robust and secure, mitigating the risk of data tampering and unauthorized manipulation of manufacturing processes. Additionally, FIPS 140-2 validation may be essential for compliance involving processes, communications and products for regulated industries such as healthcare. FIPS 140-2 can dramatically improve cybersecurity measures within the manufacturing sector, bolstering operational resilience and protecting valuable assets.

Explore FIPS 140-2 Validated Digi Solutions

When you want to ensure that you're always in compliance with FIPS 140-2 changes, consider that Digi products support FIPS 140-2 on our entire suite of cellular products based on the Digi Accelerated Linux operating system (DAL OS) — via simple firmware updates. This includes routers, console servers, USB management devices and other infrastructure management products.

The following Digi devices are FIPS 140-2 validated:

- **Digi EX series enterprise routers**
- **Digi IX series industrial routers**
- **Digi TX series transportation routers**
- **Digi Connect® IT console servers**
- **Digi AnywhereUSB® Plus**
- **Digi Connect® EZ**

Because Digi has simplified implementation of FIPS 140-2, not only do we ensure your FIPS 140-2 version stays current, but our always up-to-date encryption process makes it easy to implement. That means you simply upgrade your firmware and turn on FIPS. That's it. Avoid getting stuck with expensive, costly and complicated solutions. And if you need support at any point along your FIPS 140-2 journey, Digi Professional Services can help.

Conclusion

FIPS 140-2 provides stringent encryption requirements that continue to evolve over time. Validation for this standard is required when working with the U.S. and Canadian governments. However, any sector or industry can adopt the standard and develop or utilize FIPS 140-2 compliant modules to ensure secure handling of sensitive information. For this reason, we have covered several use cases that illustrate how FIPS 140-2 can protect sensitive data.

When you need FIPS 140-2 validated or compliant devices, contact the professionals at Digi.

Connect with Digi

- Ready to talk to a Digi expert? Contact us
- Want to hear more from Digi? Sign up for our newsletter
- Or shop now for Digi solutions: How to buy

As the FIPS standard continues to evolve, Digi is committed to transitioning to FIPS 140-3 as part of a firmware release before the expected expiration of FIPS 140-2 in September 2026. By keeping its security standards current, Digi continues to be a trusted provider of secure IoT connectivity solutions.

For more information, visit:

www.digi.com

877-912-3444 | 952-912-3444