NIST 800-171 Requirements for Validated Cryptographic Modules

A Whitepaper from SafeLogic and Kratos Defense

Executive Summary

Data encryption is a fundamental security control, popular for mitigating the impact that a data breach has on an organization. By making data unusable to anyone without the decryption key, encryption provides an additional layer of depth to an organization's defensive posture. If threat actors manage to evade detection and exfiltrate data, they need the appropriate decryption key to use it, rendering their efforts moot and discouraging further activity.

While the first iteration of the Cybersecurity Maturity Model Certification (CMMC) program was released in 2020, the Department of Defense announced CMMC 2.0 on November 4, 2021. CMMC 2.0 maintains the same goals as the original program, but it also adds enhancements, including:

- Accountability while minimizing compliance barriers
- Collaboration
- Ease of execution while enhancing public trust[1]

Additionally, CMMC 2.0 simplifies the control requirements by reducing from five certification levels to only three:

- Level 1 (remains equivalent to CMMC 1.0 Level 1): Foundational
- Level 2 (formerly Levels 2 and 3) : Advanced
- Level 3 (formerly Levels 4 and 5): Expert

As members of the Defense Industrial Base (DIB) seek to meet CMMC compliance requirements, they need to employ best cryptographic practices for securing information.

Under the original CMMC program, the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, acted as a guiding set of best practices for CMMC with additional CMMC-specific controls attached.

However, under CMMC 2.0, NIST SP 800-171 is now the primary set of compliance requirements for setting minimum security baselines. Data encryption is featured prominently among those requirements, and 800-171 references another NIST publication, the FIPS 140 standard, for specific governance.

Organizations that need to comply with CMMC Level 2 or higher should understand:

- The intersection between NIST SP 800-171, the FIPS 140 standard for cryptography, and CMMC controls;
- CMMC Practices that directly reference encryption requirements;
- CMMC Level 2 and 3 compliance requirements for FIPS 140 validation;
- The distinction between FIPS Validated and FIPS Compliant encryption;
- And the process to achieve FIPS 140 validation with recommended strategies.

[1]U.S. Department of Defense. (2021, November 4). *Strategic Direction for Cybersecurity Maturity Model Certification (CM)*. https://www.defense.gov/News/Releases/Release/Article/2833006/strategic-direction-for-cybersecurity-maturity-model-certification-cmmc-program/

Table of Contents

Background

As threat actors increasingly target supply chains, the Department of Defense (DoD) established the Cybersecurity Maturity Model Certification (CMMC) to assess and enhance the cybersecurity posture of the Defense Industrial Base (DIB). According to the Office of the Under Secretary of Defense for Acquisition & Sustainment, the Council of Economic Advisors, an agency within the Executive Office of the President, estimates that malicious cyber activity cost the U.S. economy $57 billion - $109 billion in 2016.[2]

In 2020, the DoD released the first iteration of CMMC. However, several aspects remained confusing or burdensome. For example:

- Two of the five initial maturity levels were not clearly defined
- Costs of third-party attestation would be untenable for smaller organizations
- Inability to establish Plan of Action & Milestones (POAM) to address tasks needing to be accomplished

In response to these concerns, the DoD released CMMC 2.0 which eliminated several of these burdens while still looking to achieve its primary goals.

CMMC acts as a unifying cybersecurity implementation standard across the DIB, and certification will be required for DIB members to submit bids on contracts. Although currently in the early stages, CMMC will be the guiding compliance requirement for all DIB members by 2026.

CMMC is intended to be a comprehensive and scalable certification, setting out three levels that will be specified appropriately, depending on the contract.

- Level 1: Foundational with 17 practices for safeguarding Federal Contract Information and an annual self-assessment
- Level 2: Advanced with 110 practices aligned with NIST 800-171 to protect Controlled Unclassified Information (CUI), triennial third-party assessment requirements for critical national security information, and annual self-assessments for select programs
- Level 3: Expert with all 110 practices from Level 2 plus additional, yet to be released, practices based on NIST SP 800-172, and triennial government-led assessments[3]

According to reports, the DoD estimates that approximately 300,000 vendors working with prime contractors will need to meet CMMC requirements or carry certification. While DIB members in Level 1 no longer need third-party assessments, the basic cybersecurity requirements remain the same. Ultimately, all organizations across the DIB need either self-attestation or third-party attestation proving that they use FIPS Validated encryption to protect information.[4]

---

[2]Webmaster, O. A. (2020). *Cybersecurity Maturity Model Certification (CMMC)*. Under Secretary of Defense for Acquisition & Sustainment. https://www.acq.osd.mil/cmmc/faq.html

[3]U.S. Department of Defense. (2021, November 4).

[4]Miller, J. (2019, June 17). *Why DoD's decision to make cybersecurity an 'allowable cost' matters*. Federal News Network. https://federalnewsnetwork.com/reporters-notebook-jason-miller/2019/06/why-dods-decision-to-make-cybersecurity-an-allowable-cost-matters/

Encryption and NIST 800-171

Although CMMC requirements extend beyond NIST 800-171, the Special Publication is the bedrock of compliance for the new supply chain security program. Under CMMC 2.0, organizations need to put NIST 800-171 practices into place as follows:[5]

- **Level 1**: 17 security requirements must be performed
- **Level 2**: 110 security requirements must be performed and documented
- **Level 3**: 110+ security requirements must be performed, documented, and managed

Each CMMC Level builds on the previous, so Level 3 includes all of the 110 NIST 800-171 security requirements from Level 2 as well as the Level 3 practices taken from NIST 800-172.

1.1 Digging into NIST 800-171: The Road to FIPS Validated Encryption

With NIST 800-171 as the fundamental baseline requirements for all CMMC levels, understanding where FIPS Validated encryption fits into a company's compliance is essential.

As with most compliance requirements, uncovering the technical controls leads to a winding road of references.

Under NIST 800-171 3.3.11,[6] the Discussion section directs readers to NIST's:

- Cryptographic Standards and Guidelines[7]
- Cryptographic Module Validation Program (CMVP)[8]
- Cryptographic Algorithm Validation Program (CAVP)[9]

These references all lead directly to the FIPS 140 standards, which govern the specifications for cryptographic modules, as well as the methodology for validating that those specifications have been properly implemented. The CMVP website directs readers to FIPS 140-2 and FIPS 140-3 management documents. Additionally, the page specifically includes the following emphasis-included warning:[10]

---

[5]Office of the Under Secretary of Defense for Acquisition & Sustainment. (2021). *OUSD A&S - Cybersecurity Maturity Model Certification (CMMC).* Acquisition & Sustainment. December 2020. https://www.acq.osd.mil/cmmc/about-us.html

[6]Ross, R. (2021, January 28). *SP 800–171 Rev. 2, Protecting CUI in Nonfederal Systems and Organizations* | CSRC. National Institute of Standards and Technology. https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

[7]*Cryptographic Standards and Guidelines* | CSRC. (2020). National Institute of Standards and Technology. https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines

[8]*Cryptographic Module Validation Program* | CSRC. (2020). National Institute of Standards and Technology. https://csrc.nist.gov/projects/cryptographic-module-validation-program

[9]*Cryptographic Algorithm Validation Program* | CSRC. (2020). National Institute of Standards and Technology. https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program

These references all lead directly to the FIPS 140 standards, which govern the specifications for cryptographic modules, as well as the methodology for validating that those specifications have been properly implemented. The CMVP website directs readers to FIPS 140-2 and FIPS 140-3 management documents. Additionally, the page specifically includes the following emphasis-included warning:[10]

> Non-validated cryptography is viewed by NIST as providing **no protection** to the information or data—in effect the data would be considered unprotected plaintext. ***If the agency specifies that the information or data be cryptographically protected***, then FIPS 140-2 (until September 22, 2026) or FIPS 140-3 is applicable. In essence, if cryptography is required, then it must be validated. Should the cryptographic module be revoked, use of that module is no longer permitted.

In short, organizations that need to be compliant with NIST 800-171 ***must employ*** FIPS 140-2 or FIPS 140-3 cryptographic protections.

Further, the CMVP page offers a way to search for currently validated modules as a method for independent, public verification of validation claims. (SafeLogic's portfolio of validations provided as an example.)[11]

---

[10]NIST, *Cryptographic Module Validation Program* | CSRC

[11]*Cryptographic Module Validation Program* | CSRC. (2021). National Institute of Standards and Technology. https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search?SearchMode=Basic&Vendor=SafeLogic&CertificateStatus=Active&ValidationYear=0

FIPS 140 Validation: The Critical Security Distinction

Organizations that need FIPS Validated encryption may consider attempting to keep the effort in-house. However, the FIPS 140 validation process is extremely time-consuming and requires significant resources in engineering, finances, and subject matter expertise. In order to make that strategic determination, organizations should first understand the differences between FIPS Compliant and FIPS Validated.

2.1 What is FIPS Compliant?

FIPS Compliant usually means that an organization's product is one of the following:

- Using FIPS Approved cryptographic algorithms, but lacking independent laboratory testing;
- Incorporating someone else's FIPS Validated module, relying on that third-party's certification and maintenance teams and pointing to their validation;
- Or undergoing the validation process, but not yet certified and posted to the NIST website.

While in each of the above cases an organization may be incorporating the appropriate encryption, it lacks the formal, third-party validation which proves conformance, and as such, would be considered equivalent to "unprotected plaintext" by NIST.

2.2 What Is FIPS Validated?

Unlike the FIPS Compliant modules, FIPS Validated cryptographic technologies undergo an intense and rigorous independent, third-party review.

An independently accredited laboratory tests and verifies a product's encryption functionality to ensure that it meets the FIPS 140-2 or 140-3 cryptographic module requirements, as appropriate for the certification goal. The laboratory tests the individual algorithms in partnership with the CAVP, then tests the module as a whole before they submit the paperwork to the CMVP and coordinate the finalization of the certification. NIST and its Canadian counterpart, the Communications Security Establishment (CSE), jointly operate the CAVP and CMVP. Each standards organization is responsible to staff a reviewer for each validation effort. The testing laboratories themselves can be located anywhere in the world and are certified for this role via the National Voluntary Laboratory Accreditation Program (NVLAP), another significant body among the relevant oversight entities.

2.3 FIPS Validated Encryption for NIST 800-171 and CMMC Compliance

At first, the difference between FIPS Validated and FIPS Compliant might appear to be subtle. However, NIST and the US federal government take a strong stand that FIPS Validated encryption should be employed in all products used to transmit, store, and process Controlled Unclassified Information (CUI), and that perspective is inherited in all dependent compliance programs. Even with the evolution of CMMC 2.0, this requirement remains intact.

Ultimately, to meet the stringent CMMC and NIST compliance requirements, organizations need to ensure that all encryption across their systems, networks, and devices use explicitly FIPS Validated encryption technologies.

The January 28, 2021 release of NIST SP 800-171 Rev. 2 specifies that organizations need to use a FIPS Validated Advanced Encryption Standard (AES)-256 algorithm.[12] Organizations looking to streamline their CMMC and NIST 800-171 compliance initiatives should leverage technologies that have already completed these strict review cycles.

FIPS 140 validated cryptographic modules will satisfy all requirements in NIST SP 800-171 and, by extension, all requirements in the SPRS scoring and the CMMC.

An explicitly validated module, properly implemented and shown on the NIST's Active Validation List, reduces compliance risks, especially as organizations look to accelerate their NIST 800-171 compliance strategies. The U.S. public sector is actively working to tighten their focus on the supply chain and cybersecurity and the loss of CMMC Level 2 certification eligibility could negatively impact revenue opportunities.

SafeLogic's CryptoComply modules meet all FIPS 140 standards and have already been validated by the CMVP. SafeLogic bundles their modules with RapidCert, their proprietary program that accelerates FIPS validation by leveraging the existing certification, bypassing the CMVP queue, and delivering a new validation in less than eight weeks. It's a perfect fit for an organization that has identified their compliance checklist and understands the significant overhead of trying to address them all in-house.

FIPS 140's strict boundaries make it ideal to offload to a specialist. Using SafeLogic's solutions lowers costs, avoids the need to directly deal with laboratories and consultants, and gives your engineering team the ability to stay on task instead of dealing with frustrating compliance projects. Ultimately, most organizations consider the accelerated timeline as the most important advantage of working with SafeLogic for FIPS validation. With SafeLogic, organizations can achieve FIPS compliance within a short timeline while simultaneously working on other NIST 800-171 compliance requirements, all without disruption to sales cycles or contract awards.

While NIST 800-171 and CMMC compliance can feel overwhelming, FIPS Validated encryption does not have to be a roadblock or burden. By leveraging SafeLogic's FIPS Validated encryption technology, organizations can begin using certifications as a competitive advantage and a differentiator to reduce the time-to-value.

---

[12]Ross, R. *SP 800–171 Rev. 2, Protecting CUI in Nonfederal Systems and Organizations.*

CMMC Practices and FIPS Validated Encryption

In order to accelerate CMMC Level 2 compliance using FIPS Validated encryption, organizations need visibility into the Practices involved. Encryption is built into multiple CMMC Domains, directly taken from FIPS and NIST 800-171, including:

- Access Control
- Identification and Authentication
- Media Protection
- System and Communications Protection

Within these domains, 8 practices specifically reference cryptography and encryption. More detailed information around these controls can be found in Appendix A for further reference.

NIST Control	Encryption Requirement
AC.3.3.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.
AC.3.1.17	Protect wireless access using authentication and encryption.
AC.3.1.19	Encrypt CUI on mobile devices and mobile computing platforms.
IA.3.5.10	Store and transmit only cryptographically-protected passwords.
MP.3.8.6	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.
SC.3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.
SC.3.13.11	Employ FIPS Validated cryptography when used to protect the confidentiality of CUI.
SC.3.13.16	Protect the confidentiality and integrity of CUI at rest.

Key Takeaways

As organizations within the DIB look to meet CMMC compliance as part of maintaining their current contracts and apply for future contracts, validated encryption is fundamental to meeting certification requirements.

After reading this paper, certain action items should be on your radar:

- Confirm the relevant CMMC level for your business;
- Inventory the FCI and CUI held by your organization;
- Identify where encryption is deployed in your systems and whether it has been certified to meet the FIPS 140 standard;
- Discuss with SafeLogic if FIPS 140 validation has not yet been completed;
- And engage with Kratos to assess against NIST 800-171 and to proceed with CMMC certification.

About SafeLogic

SafeLogic's CryptoComply encryption modules meet all FIPS 140-2 standards and have already been validated by the CMVP. When an organization implements a SafeLogic cryptographic module, they immediately satisfy the NIST SP 800-53 controls and meet the requirements for NIST SP 800-171, CMMC, Federal Risk and Authorization Management Program (FedRAMP), Federal Information Security Management Act of 2002 (FISMA), DoD Information Network (DoDIN) Approved Products List (APL), and Common Criteria.

SafeLogic modules include RapidCert, the industry's only FIPS 140 validation service that provides a certificate in the customer's name. RapidCert drastically accelerates the timeline, requiring no additional engineering effort or interaction with testing laboratories, and is delivered at a fixed cost.

By providing the software and service in tandem, SafeLogic reduces the validation timeline to 8 weeks. SafeLogic then maintains the module and FIPS 140 certificate for the client organization to further leverage our dedicated team of experts. SafeLogic is focused on standards-based cryptographic engines that are fully validated to FIPS 140 standards and maintained to ensure ongoing compliance. The modules are built to offer drop-in compatibility for the most popular open-source modules and a variety of connectors to accommodate unique product architecture, including Cloud deployments.

SafeLogic's customers are among the most influential and innovative companies in technology today, from startups to the Fortune 100, including Hewlett Packard Enterprise, Broadcom, VMware, Raytheon, Cisco, Zscaler, and Okta.
SafeLogic was established in 2012, is privately held, and is headquartered in Palo Alto, California.

Contact SafeLogic directly to learn more and establish compatibility for your solution.

About Kratos

Kratos Defense & Security Solutions, Inc. (NASDAQ:KTOS)develops and fields transformative, affordable technology, platforms and systems for United States National Security affiliated customers, allies and commercial enterprises. Kratos is changing the way breakthrough technologies for these industries are rapidly brought to market through proven commercial and venture capital backed approaches, including proactive research and streamlined development processes. At Kratos, affordability is a technology, and we specialize in unmanned systems, satellite communications, cyber security/warfare, microwave electronics, missile defense, hypersonic systems, training, combat systems and next generation turbojet and turbo fan engine development.

Within the cybersecurity/warfare space, Kratos serves as a trusted advisor, supporting commercial companies and agencies through a full life cycle of system design, control implementation, and risk management processes. Most recently, Kratos was authorized as a CMMC Certified Third-Party Assessment Organization (C3PAO). Additionally, Kratos has years of robust compliance and certification experience with government and commercial standards and compliance frameworks requirements. In addition to being a C3PAO, Kratos was one of the first and largest Federal Risk and Authorization Management Program (FedRAMP) Third Party Assessment Organizations (3PAO). Kratos' compliance experience also includes Payment Card Industry (PCI), Federal Information Security Management Act (FISMA) and the National Institute of Standards & Technology (NIST)/Risk Management Framework (RMF). Kratos is viewed as a trusted compliance and governance partner by the DoD, Federal Civilian Agencies, Intelligence Community (IC), and commercial organizations.

Kratos is prepared to offer Advisory or Assessment services. Assessment services include scoping analyses, readiness assessments, penetration testing, and continuous monitoring. Advisory services include gap assessments, documentation, and process and engineering consulting services.

For more information, go to www.kratosdefense.com/cyber.

Appendix A: Best Encryption Practices for Using FIPS Validated Encryption to Meet CMMC and NIST 800-171 Requirements

In order to accelerate compliance activities, organizations need to know where FIPS Validated encryption fits into their overarching CMMC and NIST 800-171 compliance plans.[13] The following eight practices focus on where organizations need to employ encryption.

Access Control

Adopting cloud-based technologies makes access control more important than ever before. Increasingly, threat actors engage in credential theft attacks. This means that organizations need to put appropriate access controls in place to enhance their security and compliance posture.

NIST Control AC.3.3.13

AC.3.1.13 requires that organizations:

> Maintain the confidentiality and integrity of remote access sessions by employing cryptographic mechanisms.

This control focuses on implementing remote session encryption to enhance existing controls.

To meet these requirements, organizations should consider using FIPS Validated encryption when:

- Using virtual private networks (VPNs) to protect the confidentiality and integrity of remote access sessions
- Adopt Transport Layer Security (TLS) cryptographic protocols for end-to-end communications security over networks, including public internet connections
- Generating, aggregating, and/or correlating reports

Example

> As a system administrator you are responsible for implementing a remote network access capability for users who work offsite. In order to provide session confidentiality, you decide to implement a VPN mechanism and select a product that has completed FIPS 140 validation.

Potential Assessment Considerations

- Are cryptographic mechanisms used for remote access sessions (e.g., Transport Layer Security (TLS) and Internet Protocol Security (IPSec) using FIPS Validated encryption algorithms) defined and implemented? Note that simply using an approved algorithm is not sufficient – the module (software and/or hardware) used to implement the algorithm must be separately validated under FIPS 140.

[13]Office of the Under Secretary of Defense for Acquisition & Sustainment. (2020). *CMMC Assessment Guide: Level 3.*

NIST Control AC.3.1.17

AC.3.1.17 requires that organizations:

Protect wireless access using authentication and encryption.

This control focuses on ensuring that all users and devices authenticate to networks. Additionally, organizations need to protect wireless communications and encrypt devices.

To meet these requirements, organizations should consider using FIPS Validated encryption when:

- Using strong encryption to mitigate risks associated with wireless technologies
- Maintaining up-to-date device lists
- Maintaining strong user account and access controls

Example 1

You manage the wireless network at a small company and are installing a new wireless solution. You start by selecting a product that employs encryption validated against the Federal Information Processing Standard (FIPS) 140 standard. You configure the wireless solution to use WPA2, requiring users to enter a pre-shared key to connect to the wireless network.

Example 2

You manage the wireless network at a large company and are installing a new wireless solution. You start by selecting a product that employs encryption that is validated against the FIPS 140 standard. Because of the size of your workforce, you configure the wireless system to authenticate users with a RADIUS server. Users must provide the wireless system with their domain usernames and passwords to be able to connect, and the RADIUS server verifies those credentials. Users unable to authenticate are denied access.

Potential Assessment Considerations

- Is wireless access limited only to authenticated and authorized users (e.g., required to supply a username and password)?
- If the organization is securing its wireless network with a pre-shared key, is access to that key restricted to only authorized users?
- Is wireless access encrypted using FIPS Validated cryptography? Note that simply using an approved algorithm is not sufficient; the module (software and/or hardware) used to implement the algorithm must be separately validated under FIPS 140.

NIST Control AC.3.1.19

AAC.3.1.19 requires that organizations:

Encrypt CUI on mobile devices and mobile computing platforms.

To meet these requirements, organizations should consider using FIPS Validated encryption when:

- Employing full-device or container-based encryption to protect CUI on mobile devices and computing platforms
- Encrypting data and information, including selected data structures like files, fields, or records
- Maintaining up-to-date mobile device inventories

Example

You are in charge of mobile device security. You configure all laptops to use the full-disk encryption technology built into the operating system. This approach is FIPS Validated and encrypts all files, folders, and volumes.

Phones and tablets pose a greater technical challenge with their wide range of manufacturers and operating systems. You select a proprietary mobile device management (MDM) solution to enforce FIPS Validated encryption on those devices.

Potential Assessment Considerations

- Is a list maintained of mobile devices and mobile computing platforms that are permitted to process, store, or transmit CUI?
- Is CUI encrypted on mobile devices using FIPS Validated algorithms?

Identification and Authentication

NIST Control IA.3.5.10

IA.3.5.10 requires that organizations:

Store and transmit only cryptographically-protected passwords.

To meet these requirements, organizations should consider using FIPS Validated encryption when:

- Transmitting passwords over protected channels (e.g., encrypted email or password vault file)
- Storing passwords in databases
- Establishing and enforcing strong password policies

Example

You are responsible for managing passwords for your organization. You protect all passwords with a one-way transformation, or hashing, before storing them. Passwords are never transmitted across a network unencrypted.

Potential Assessment Considerations

- Are passwords prevented from being stored in reversible encryption form in any company systems?
- Are passwords stored as one-way hashes constructed from passwords?

Media Protection

NIST Control MP.3.8.6

MP.3.8.6 requires that organizations:

> Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.

To meet these requirements, organizations should consider using FIPS Validated encryption when:

- Protecting portable storage devices (e.g., USB memory sticks, digital video disks, compact disks, external or removable hard disk drives)
- Securing all data across system components and data structures, including files, records, and fields

Example

> You manage the backups for file servers in your datacenter. You know that in addition to the company's sensitive information, CUI is stored on the file servers. As part of a broader plan to protect data, you send the backup tapes off site to a vendor. You are aware that your backup software provides the option to encrypt data onto tape. You develop a plan to test and enable backup encryption for the data sent off site. This encryption provides additional protections for the data on the backup tapes during transport and offsite storage.

Potential Assessment Considerations

- Are all CUI data on media encrypted or physically protected prior to transport outside of controlled areas?
- Are cryptographic mechanisms used to protect digital media during transport outside of controlled areas?
- Do cryptographic mechanisms comply with FIPS 140-2?

System and Communications Protection

NIST Control SC.3.13.8

SC.3.13.8 requires organizations to:

> Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.

To meet these requirements, organizations should consider using FIPS Validated encryption when:

- Securing internal and external networks
- Protecting any system components that can transmit information including servers, notebook computers, desktop computers, mobile devices, printers, copiers, scanners, and facsimile machines
- Providing additional security controls when commercial telecommunication services packages make it infeasible or impractical to provide assurance
- Enhancing physical security controls to safeguard protected distribution systems (PDS)
- Monitoring where CUI goes throughout a system/process to determine whether there are gaps in the safeguards

Example

> You are a system administrator responsible for configuring encryption on all devices that contain CUI. Because your users regularly store CUI on laptops and take them out of the office, you encrypt the hard drives with a FIPS Validated encryption tool built into the operating system. For users who need to share CUI, you install a Secure FTP server to allow CUI to be transmitted in a compliant manner. You verify that the server is using a FIPS Validated encryption module by checking the NIST Cryptographic Module Validation Program website. You turn on the "FIPS Compliance" setting for the server during configuration because that is what is required for this product in order to use only FIPS Validated cryptography.

Potential Assessment Considerations

- Are cryptographic mechanisms used to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures (e.g., PDS)?

NIST Control SC.3.13.11

SC.3.13.11 requires that organizations:

> Employ FIPS Validated cryptography when used to protect the confidentiality of CUI.

To meet these requirements, organizations should consider whether the FIPS Validated encryption solution can:

- Be employed to support many security solutions including the protection of controlled unclassified information, the provision of digital signatures, and the enforcement of information separation
- Support random number generation and hash generation
- Secure provisioning and implementation of digital signatures

Example

> You are a system administrator responsible for deploying encryption on all devices that contain CUI. You must ensure that the encryption you use on the devices is FIPS Validated cryptography [a]. An employee informs you of a need to carry a large volume of CUI offsite and asks for guidance on how to do so. You provide the user with disk encryption software that you have verified via the NIST website that uses a CVMP-validated encryption module [a]. Once the encryption software is active, the user copies the CUI data onto the drive for transport.

Potential Assessment Considerations

- Is cryptography implemented to protect the confidentiality of CUI at rest and in transit, through the configuration of systems and applications or through the use of encryption tools?

NIST Control SC.3.13.16

SC.3.13.16 requires that organizations:

Protect the confidentiality and integrity of CUI at rest.

To meet these requirements, organizations should consider using FIPS Validated encryption to:

- Secure information located on storage devices as specific components of systems
- Protect system components including internal or external hard disk drives, storage area network devices, or databases
- Ensure appropriate encryption across file shares and off-line storage to protect system and user information
- Maintain the integrity of system

Example 1

Your company has a policy stating CUI must be protected at rest and you work to enforce that policy. You research Full Disk Encryption (FDE) products that meet the FIPS encryption requirement. After testing, you deploy the encryption to all computers to protect CUI at rest.

Example 2

You have used encryption to protect the CUI on most of the computers at your company, but you have some devices that do not support encryption. You create a policy requiring these devices to be signed out when needed, stay in possession of the signer when checked out, and to be signed back in and locked up in a secured closet when the user is done with the device [a]. At the end of the day each Friday, you audit the sign-out sheet and make sure all devices are returned to the closet.

Potential Assessment Considerations

- Is the confidentiality of CUI at rest protected using encryption of storage devices and/or appropriate physical methods?

Contact Information

SafeLogic Inc.
530 Lytton Ave., Suite 200
Palo Alto, CA 94301

(844) 4-ENCRYPTION

www.SafeLogic.com
www.Twitter.com/SafeLogic

Kratos Defense & Security Solutions, Inc.
5791 Kingstowne Village Parkway,
Suite 200
Alexandria, VA 22315

(703) 254-2000

www.KratosDefense.com/cyber
www.Twitter.com/KratosDefense

Acronym and Abbreviation Listing

Acronym / Abbreviation	Definition
3PAO	Third Party Assessment Organization
AES	Advanced Encryption Standard
ATO	Authorization to Operate
C3PAO	CMMC Third-Party Assessment Organizations
CAVP	Cryptographic Algorithm Validation Program
CMMC	Cybersecurity Maturity Model Certification
CMVP	Cryptographic Module Validation Program
CUI	Controlled Unclassified Information
DIB	Defense Industrial Base
FIPS	Federal Information Processing Standards
JAB	Joint Authorization Board
NIST	National Institute of Standards and Technology
SP	Special Publication
SPRS	Supplier Performance Risk System