SafeLogic

FISMA Requirements for Validated Cryptographic Modules

A White Paper from SafeLogic

SafeLogic

SafeLogic Inc.

530 Lytton Ave, Suite 200

Palo Alto, CA 94301

www.SafeLogic.com

Executive Summary

The encryption of sensitive data is one of the top requirements for enterprise and mobile applications. These requirements go beyond the implementation of complex algorithms to include a time-consuming and difficult validation process to ensure compliance with the Federal Information Processing Standard (FIPS) 140-2. Standard approaches to integrate encryption routines into custom software have resulted in increased development time, conflicting with the time constraints of end customers. Products often deploy late or without validated encryption routines. SafeLogic's 'Drop-In Compliance' approach provides a crypto module that meets customer demand for both validation and short development time. This paper presents the Federal Information Security Management Act (FISMA) requirements for validated encryption routines and the benefits of SafeLogic's CryptoComply module.

Table of Contents

List of Tables

1 FISMA Overview

The Federal Information System Management Act (FISMA), enacted in 2002, requires federal agencies, government contractors, and government service providers to implement and manage an information security program. The federal information security program requirements are defined in the FISMA Implementation Project by the publications authored by the National Institute of Standards and Technology (NIST). Table 1 provides a summary of the major documents of the FISMA Implementation Project.

Publication	Title	Description
FIPS 199	Standards for Security Categorization of Federal Information and Information Systems	Mandatory federal standard for determining the security category of information systems.
FIPS 200	Minimum Security Requirements for Federal Information and Information Systems	Mandatory federal standard for deriving the impact level from the security category for information systems.
SP 800-53	Security and Privacy Controls for Federal Information Systems and Organizations	Federal guideline for selecting the minimum-security controls for information systems and the organization.
FIPS 140-2	Security Requirements for Cryptographic Modules	Federal standard for the specification of cryptographic-based security systems used to protect sensitive data. Also established the Cryptographic Module Validation Program (CMVP) for the validation of cryptographic modules by Cryptographic and Security Testing (CST) laboratories.
FIPS 140-3 DRAFT	Security Requirements for Cryptographic Modules	Proposed revision for FIPS 140-2

Table 1 – FISMA Implementation Project Documents

The FISMA Implementation Project was established in 2003 as a result of the Federal Information Security Management Act (FISMA). The National Institute of Standards and Technology (NIST) defined the minimum security requirements for federal information systems processing sensitive data through this program.

All Federal information systems and their components are required to meet the minimum security controls as specified in NIST SP 800-53, based on a system classification defined by FIPS 199 and FIPS 200. In the next section, we will examine the encryption requirements derived from these standards.

Furthermore, the FIPS 140-2 validation program precludes the use of unvalidated cryptography for the protection of sensitive or valuable data within Federal systems. NIST considers systems that use unvalidated cryptography to be equal to those providing no cryptographic protection at all.

The Cryptographic Module Validation Program (CMVP) validates cryptographic modules to FIPS 140-2 security standards. Vendors of cryptographic modules use independent and accredited Cryptographic and Security Testing (CST) laboratories to test their modules.

2 Security Categorization

The minimum security requirements for all federal system and their components are based on a security category assignment of low, moderate, or high, according to FIPS 199 and FIPS 200 standards. Table 2 describes the security categories for federal systems.

Security Categorization		
Low	**Moderate**	**High**
The unauthorized disclosure of, modification of, destruction of, or disruption of access to information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of, modification of, destruction of, or disruption of access to information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of, modification of, destruction of, or disruption of access to information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Table 2 – FIPS 199 & 200 Security Categorization

All federal systems are assigned a security categorization based on the potential impact level of a security policy violation. These security categorizations are the basis of selecting the minimum security controls from NIST SP 800-53.

Limiting our discussion to the encryption requirements and other security requirements affected by encryption, there are six (6) areas in which encryption is addressed within the NIST SP 800-53. Some of the requirements specifically address encryption, while others allow for it to be used as a mechanism to support or enhance a security control. In all cases, if encryption is employed as a mechanism to meet a security requirement, it must be FIPS 140-2 compliant and validated under the Cryptographic Module Validation Program (CMVP).

2.1 Encryption Requirements

The following security requirements directly address the use of encryption technology in federal systems.[1]

IA-7 Cryptographic Module Authentication (Low)

The cryptographic module within the information system must implement authentication mechanisms (i.e., role-based or identity-based) to control access to the cryptographic module.

[1] A family identifier (two-characters assigned to uniquely identify the security control family), and a numeric identifier (one or two digits assigned to indicate the control number within the family) is assigned to each requirement. A complete listing of all control families and controls can be found in NIST SP 800-53.

Since this requirement applies to all federal systems with a security categorization of 'Low" or higher, this requirement applies to all federal systems.

SC-13 Use of Cryptography (Low)

For any cryptographic protection for policy enforcement within the information system, the cryptographic modules implementing those services and protections must comply with federal laws (i.e., FIPS 140-2 and the CMVP). Since this requirement applies to all federal systems with a security categorization of 'Low" or higher, this requirement applies to all federal systems.

SA-4 (7) Acquisitions - Enhancement (Not required)

If a commercially provided information technology product relies on cryptographic functionality to enforce a security policy, then the cryptographic module is FIPS-validated. This requirement is an "Enhancement" and only applies to federal systems if the system owner has tailored requirements to include it.

2.2 Data at Rest

The following security requirements utilize encryption technology in federal systems to protect sensitive data stored on information systems and components.

SC-28 (1) Protection of Information at Rest - Enhancement (Not required)

The organization employs cryptographic mechanisms to prevent unauthorized disclosure and modification of information at rest unless otherwise protected by alternative physical measures. This requirement is an "Enhancement" and only applies to federal systems if the system owner has tailored requirements to include it.

AU-9 (3) Protection of Audit Information - Enhancement (Not required)

The information system uses cryptographic mechanisms to protect the integrity of audit information and audit tools. This requirement is an "Enhancement" and only applies to federal systems if the system owner has tailored requirements to include it.

MP-4 (1) Media Storage - Enhancement (Not required)

The organization employs cryptographic mechanisms to protect information in storage. This requirement is an "Enhancement" and only applies to federal systems if the system owner has tailored requirements to include it.

2.3 Data in Transmission

The following security requirements utilize encryption technology in federal systems to protect sensitive data transmitted on information systems and components.

MP-5 (4) Media Transport - Enhancement (Moderate)

The organization employs cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas. This requirement is an “Enhancement” and required of all federal information systems with a security categorization of “Moderate” or higher.

SC-8 (1) Transmission Integrity – Enhancement (Moderate)

The organization employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures. This requirement is an “Enhancement” and required of all federal information systems with a security categorization of “Moderate” or higher.

SC-9 (1) Transmission Confidentiality – Enhancement (Moderate)

The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures. This requirement is an “Enhancement” and required of all federal information systems with a security categorization of “Moderate” or higher.

AC-17 (2) Remote Access – Enhancement (Moderate)

The organization uses cryptography to protect the confidentiality and integrity of remote access sessions. This requirement is an “Enhancement” and required of all federal information systems with a security categorization of “Moderate” or higher.

2.4 Access Control

The following security requirements utilize encryption technology in federal systems to prevent unauthorized access to sensitive information on information systems and components.

AC-3 (6) Access Enforcement - Enhancement (Not required)

The organization encrypts or stores off-line in a secure location. This requirement is an “Enhancement” and only applies to federal systems if the system owner has tailored requirements to include it.

MP-2 (2) Media Access - Enhancement (Not required)

The information system uses cryptographic mechanisms to protect and restrict access to information on portable digital media. This requirement is an “Enhancement” and only applies to federal systems if the system owner has tailored requirements to include it.

2.5 Identification & Authentication

The following security requirements utilize encryption technology in federal systems to authenticate the credentials of active entities in support of identification-based access control.

AC-18 (1) Wireless Access - Enhancement (Moderate)

The information system protects wireless access to the system using authentication and encryption. This requirement is an “Enhancement” and required of all federal information systems with a security categorization of “Moderate" or higher.

IA-3 (1) (2) Device Identification and Authentication - Enhancement (Not required)

The information system authenticates devices before establishing remote, wireless network, and network connections using bidirectional authentication between devices that is cryptographically based. These requirements are an “Enhancement” and only apply to federal systems if the system owner has tailored requirements to include it.

MA-4 (6) Non-Local Maintenance - Enhancement (Not required)

The organization employs cryptographic mechanisms to protect the integrity and confidentiality of non-local maintenance and diagnostic communications. This requirement is an “Enhancement” and only applies to federal systems if the system owner has tailored requirements to include it.

2.6 Non-Repudiation

The following security requirements utilize encryption technology in federal systems to protect against an individual falsely denying having performed a particular action.

AU-10 (5) Non-Repudiation – Enhancement (Not required)

The organization employs FIPS-validated cryptography to implement digital signatures. This requirement is an “Enhancement” and only applies to federal systems if the system owner has tailored requirements to include it.

3 Requirements Summary and Conclusion

3.1 Summary

Summarizing the encryption requirements and other security requirements affected by encryption, there are a minimum of two (2) cryptographic requirements applied to all federal information systems and seven (7) cryptographic requirements for federal information systems with a Moderate security classification. Table 3 provides a matrix of the cryptographic requirements based on the security categorization in the federal information system.

Requirement	Security Categorization			
	Low	Moderate	High	Enhanced
Encryption				
IA-7	✓	✓	✓	✓
SC-13	✓	✓	✓	✓
SA-4 (7)				✓
Data at Rest				
SC-28 (1)				✓
AU-9 (3)				✓
MP-4 (1)				✓
Data in Transmission				
MP-5 (4)		✓	✓	✓
SC-8 (1)		✓	✓	✓
SC-9 (1)		✓	✓	✓
AC-17 (2)		✓	✓	✓
Access Control				
AC-3 (6)				✓
MP-2 (2)				✓
Identification & Authentication				
AC-18 (1)		✓	✓	✓
IA-3 (1) (2)				✓
MP-4 (6)				✓
Non-Repudiation				
AU-10 (5)				✓

Table 3 – NIST SP 800-53 Cryptographic Requirements and CryptoComply Feature Mapping

All federal systems must comply with a minimum of several cryptographic requirements. These systems must contain validated cryptographic modules.

3.2 Conclusion

Federal agencies and government contractors demand custom-developed enterprise and mobile applications for a diverse set of mission needs, and information security is always among the top requirements. Any federal information systems that need to meet any of the FISMA requirements listed above must obtain support from a validated cryptographic module.

SafeLogic's CryptoComply meets all FIPS 140-2 standards and has already been validated by the CMVP. By extension, CryptoComply surpasses the FISMA standards for cryptography. When an end user demands that a solution satisfies FISMA, the encryption requirements are met instantly and verifiably upon implementation of the CryptoComply module.

From the point of view of NIST, validated cryptographic modules are the only acceptable source for encryption. SafeLogic makes sure that this is achieved without compromising on delivery timeline.

3.3 About SafeLogic

SafeLogic's product line is focused on standards-based cryptographic engines designed for use in Cloud, mobile, wearable, IoT, server, workstation, and appliance environments. These modules have been fully validated to FIPS 140-2 standards and offer drop-in OpenSSL and Bouncy Castle compatibility, a variety of connectors to accommodate unique product architecture, and instant compliance for federal deployments to SafeLogic customers.

Even better, SafeLogic modules include RapidCert, the industry's only FIPS 140-2 validation service that provides a certificate in the customer's name, while drastically accelerating the timeline, requiring no additional engineering effort, zero interaction with testing labs, and at a fixed cost.

SafeLogic's customers are among the most influential and innovative companies in technology today, from startups to the Fortune 100.

SafeLogic was established in 2012, is privately held and is headquartered in Palo Alto, California.

SafeLogic

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

(844) 4-ENCRYPTION

www.SafeLogic.com

www.Twitter.com/SafeLogic