FISMA COMPLIANCE—FIRMWARE SECURITY BEST PRACTICES

FISMA, and the NIST documents supporting it, repeatedly underscore the importance of firmware security as part of a modern security program. Yet, this area remains one of the most overlooked and poorly understood areas of risk within government agencies. This document walks through the requirements and guidance that the law establishes in regard to firmware, and provides practical guidance and recommendations that organizations can use to not only comply with FISMA, but also to build a stronger security program.

CONTENTS

Introduction . . . 2

FISMA Overview . . . 2

Prepare: Understanding the Firmware Attack Surface . . . 3

Categorize: Understanding Devices in Terms of Susceptibility and Impact of Firmware Threats . . . 3

Controls and Continuous Monitoring . . . 5

- SI—System and Information Integrity . . . 6
- SA—System Acquisition . . . 6
- CM—Configuration Management . . . 7
- AC—Access Controls . . . 8
- RA—Risk Assessment . . . 8
- IR—Incident Response . . . 9
- MA—Maintenance . . . 9

Conclusion . . . 10

INTRODUCTION

The Federal Information Security Management Act (FISMA) defines the information security requirements for all federal agencies. It extends across the lifecycle of a security program from planning, implementation, and ongoing administration of a security program. And in addition to covering all federal agencies, it also applies to any contractors, any entities that handle federal information, and even state agencies that administer federal funds.

FISMA is also quite different from many other regulatory security standards. Notably, the FISMA security controls clearly and repeatedly establish firmware security as being in scope. This is not surprising given that firmware implants and other firmware threats have long been a favorite tool for nation-state attackers who would naturally target federal information systems. This has become an even higher priority as firmware-based threats have recently spread to large-scale network-based and malware-based campaigns. Likewise supply-chain security has become a top priority for NIST, DoD, and many others both inside and outside of the government sector.

However, firmware security has often been challenging for many organizations. Historically it has been time-consuming, required specialized and rare security skills, and teams often lacked the tools to automate the work. Fortunately, new tools and innovations are changing the situation for the better. In this paper, we will take a closer look at some of the FISMA requirements, how they relate to firmware security, and specific steps you can take to bolster your security programs.

FISMA OVERVIEW

FISMA establishes far-reaching requirements that are guided heavily by two important NIST documents. SP 800-37 lays out a Risk Management Framework (RMF) and SP 800-53 addresses Security and Privacy Controls. At a high level, the Risk Management Framework establishes a lifecycle approach that guides the creation and ongoing administration of a security program. SP 800-53 then provides additional details on the types of controls that may be implemented and considerations for each.

Both documents identify firmware as a critical part of the security program and consistently use the phrase "hardware, software, and firmware" when describing the components of technology and devices to be protected.

However, that **does not** mean that all organizations subject to FISMA are necessarily mandated to adopt firmware security controls. FISMA gives organizations considerable flexibility over the details of a program. The guiding direction is that security controls should be "*customized for the specific missions, business functions, risks, and operating environments of the*

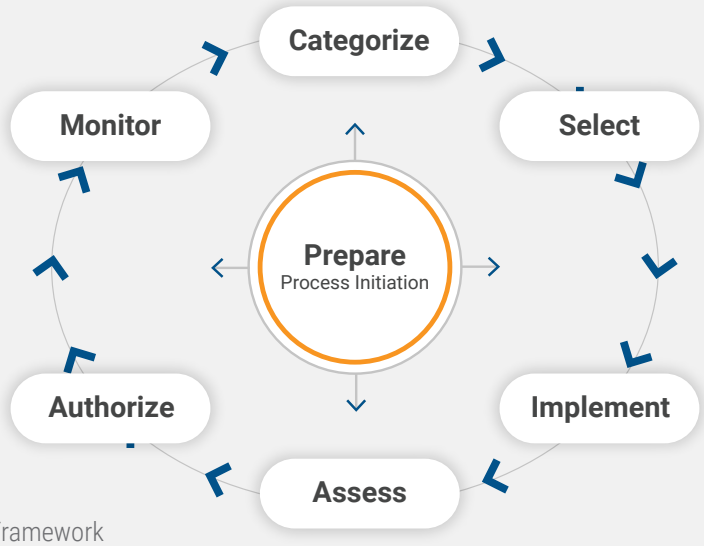

Figure 1: Risk Management Framework

organization." In short, some organizations, environments, or specific devices may need firmware security controls while others may not. With that in mind, the remaining sections of this paper will look at firmware security in the context of various FISMA requirements and direction, and then provide specific examples of firmware controls that may be appropriate.

PREPARE: UNDERSTANDING THE FIRMWARE ATTACK SURFACE

The Prepare phase is the first step of the RMF and it covers a lot of important ground. This is where organizations define their high-level risk strategy based on their unique mission, tolerance for risk, types of threats such as cyber-attacks, and other factors. Given the historic use of firmware implants and backdoors by state-supported adversaries, many organizations will likely want to consider their firmware attack surface.

In particular, the Prepare phase covers important requirements such as the need for system-level vulnerability assessments. However, many organizations have historically ignored the firmware layer during vulnerability assessments simply due to pragmatic challenges. Teams have always been able to rely on highly automated vulnerability scanners for analyzing ports, services, and applications, but firmware security assessments were often far more manual, time-consuming, and required specialized skills. This lack of basic visibility into firmware-related risks has led many organizations to develop a persistent blind-spot in regard to firmware security in spite of the heavy attention it receives from sophisticated adversaries.

However, the Eclypsium platform as well as open-source frameworks such as CHIPSEC have evolved to make this a much more automatable process. Organizations can now scan their devices to identify the presence of outdated firmware, vulnerable firmware, and a wide variety of missing device protections that could put the device at risk. With visibility into the firmware attack surface, organizations can make much more informed decisions about how and when to prioritize firmware security for the organization.

ECLYPSIUM® GUIDANCE AND CONSIDERATIONS:

Perform an initial firmware vulnerability assessment of critical devices or assets. Consider using licensed or open-source tools to automate the analysis of devices. Firmware analysis should include system-level firmware such as BIOS or UEFI, but should also extend to firmware of hardware components within the system such as drives, processors, and network adapters. Scans should be able to identify the following:

- **Systems with out of date firmware**
- **Systems with firmware vulnerabilities**
- **Systems with missing hardware protections**

CATEGORIZE: UNDERSTANDING DEVICES IN TERMS OF SUSCEPTIBILITY AND IMPACT OF FIRMWARE THREATS

The Categorize phase requires organizations to classify their systems and assets based on the impact of a loss of confidentiality, integrity, or availability of that system. This applies to the system itself as well as any information the system processes, stores, or transmits.

In this context it is important to understand the power of firmware-based threats and why they have become so strategically important to sophisticated attackers. First, firmware represents the most fundamental code of a device. System firmware such as BIOS or UEFI run prior to the operating system and threats at this level can subvert the operating system and any higher level security controls that depend on the operating system.

Likewise, firmware is present in virtually every hardware component of the system from drives, to network adapters, to interfaces such as baseboard management controllers that manage the system. As a result, firmware threats could have insight into data stored on the system or transmitted over its network connections. Additionally, devices could easily be disabled altogether at the firmware level.

As a result, firmware threats would have high impacts to the confidentiality, integrity, and availability of the system. Likewise, these threats provide attackers with long-term persistence on a victim device by being able to subvert traditional security controls and surviving across common incident response processes such as reinstalling the host operating system to a known "gold" version.

ECLYPSIUM GUIDANCE AND CONSIDERATIONS: Organizations may want to consider the impact of firmware-based threats to the following high-value devices during the categorization phase:

High-Value Laptops

While all devices are potentially subject to attacks on their firmware, laptops are often exposed more often than other assets. An attacker can use known firmware vulnerabilities to remotely compromise a laptop despite protections like Secure Boot. Thus organizations may want to consider firmware security controls for devices that carry high-value information and/or operate in untrusted environments.

Critical Servers

Firmware provides an ideal path to both steal data or deny access to it altogether. This is particularly true of high-value servers. In particular, the baseboard management controllers (BMCs) that enable remote and out-of-band management of servers have incredible power over the data and operation of servers, an area where firmware vulnerabilities have been particularly common.

Networking and Security Gear

Recent large-scale attacks against VPN devices have shown that networking gear presents a particularly powerful prize for attackers. By subverting the network infrastructure, attackers could easily read, manipulate, or even redirect content on the network. Likewise the very network controls charged with securing the network could likewise be targets of attack. As called out in the AC-4 control of SP 800-53, organizations may want to "*consider the trustworthiness of filtering/inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement.*"

CONTROLS AND CONTINUOUS MONITORING

Once systems have been properly categorized, organizations will select and implement controls that are appropriate for the system and the organization's tolerance for risk. It is important to note that these controls are not applied as a single, one-time event. While an annual FISMA assessment represents a point-in-time check view of the security program, the standard requires organizations to implement ongoing monitoring programs to identify changes in risks and threats and to confirm that controls are having their intended effect. As with other FISMA requirements, the frequency of monitoring will vary based on the risk profile of the organization as stated below in SP 800-53:

> *Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security and privacy to support organizational risk management decisions. The terms continuous and ongoing imply that organizations assess security and privacy controls and associated risks at a frequency sufficient to support risk-based decisions.*

As discussed previously, manual analysis of firmware security is often prohibitively time-consuming for staff to perform on a regular cadence. As such, organizations will likely want to consider tools to automate firmware security for those systems that have been prioritized.

There are several specific families of security and privacy controls defined by SP 800-53 where firmware security may naturally apply. Five such areas are highlighted below, but organizations may naturally want to consider firmware-based controls in other areas as well.

Applicable NIST SP 800-53 Controls:

Control	References	Eclypsium Detections
SI—System and Information Integrity SI-2 Flaw Remediation SI-4 Information System Monitoring SI-7 Software, Firmware, and Information Integrity	In-the-wild implants (eg. HackingTeam, Lojax)	**1**. Confirm firmware integrity **2**. Identify insecure firmware and apply updates **3**. Ensure that all firmware updates are cryptographically signed and that devices require any firmware updates to be signed **4**. Monitor devices for signs of malicious firmware behavior **5**. Analyze systems to ensure the integrity of the boot process and boot firmware **6**. Detect firmware threats such as implants, backdoors, and rootkits
SA—System and Services Acquisition SA-12 Supply Chain Protection SA-19 Component Authenticity	Supply chain interdictions	**1**. Evaluate prospective technology for firmware security and avoid products that can be easily modified at the firmware level. **2**. Check all newly acquired devices to confirm the integrity of the firmware **3**. Monitor devices for signs of malicious firmware behavior
CM—Configuration Management CM-2 Baseline Configuration CM-5 Access Restrictions for Change CM-7 Least Functionality	Secure Configuration PLATINUM malware campaign	**1**. Record expected configuration and behavior of device firmware and hardware **2**. Activate firmware and hardware security features **3**. Analyze critical devices to ensure unnecessary features are disabled, particularly remote management interfaces that are not used.
AC—Access Control AC-6 Least Privilege	Firmware Storage Vulnerabilities	**1**. Ensure any unnecessary debug functionality is not enabled **2**. Ensure firmware storage is properly protected

Control	References	Eclypsium Detections
RA—Risk Assessment RA-5 Vulnerability Scanning	Firmware and hardware vulnerabilities (eg. Speculative execution side-channels, vulnerable firmware storage, insecure SMM code)	**1**. Prioritize the analysis and monitoring of firmware and hardware vulnerabilities **2**. Regular scans should be able to identify **a**. Systems with out of date firmware **b**. Systems with firmware vulnerabilities **c**. Systems with missing protections
IR— Incident Response IR-4 Incident Handling IR-10 Security Analysis Team	Attackers using firmware implants to persist across system re-imaging.	**1**. Perform firmware scans of devices related to incident to track scope **2**. Verify integrity of firmware of all affected hosts during system recovery **3**. Arm staff with tools to assist in forensic analysis of firmware-based threats
MA—Maintenance MA-3 Maintenance Tools	BMC, IPMI, and Intel AMT as potential attack vectors	**1**. Monitor management interfaces for vulnerabilities or signs of compromise **2**. Scan management resources for vulnerabilities **3**. Only enable remote management tools for devices that have an operational need

SI—SYSTEM AND INFORMATION INTEGRITY

The System and Information Integrity family of controls is heavily focused on the detection of and response to threats. This includes the important topics of Flaw Remediation, Malicious Code Protection, System Monitoring, and specifically Software, Firmware, and Information Integrity. A firmware security platform should be able to address all of these key areas.

Control SI-7 specifically address the topic of Software, Firmware and Information Integrity. Items SI-7(9) and SI-7(10) specifically address the need to ensure the integrity of the system boot process and well as the integrity of the boot firmware. The section specifically notes:

> *Unauthorized modifications to boot firmware may be indicative of a sophisticated, targeted attack. These types of targeted attacks can result in a permanent denial of service or a persistent malicious code presence. These situations can occur, for example, if the firmware is corrupted or if the malicious code is embedded within the firmware. System components can protect the integrity of boot firmware in organizational systems by verifying the integrity and authenticity of all updates to the firmware prior to applying changes to the system component; and preventing unauthorized processes from modifying the boot firmware.*

Additionally, SP 800-53 calls out that organizations may want to consider both signature based and non-signature based approaches to the detection of malicious code. Eclypsium applies both types of analysis to the detection of firmware-based backdoors, implants, and rootkits. In addition to checking for known implants and threat, Eclypsium monitors the behavior of the firmware and components to identify firmware threats that are unknown or do not have a known signature.

SA—SYSTEM ACQUISITION

FISMA and the supporting NIST documents strongly highlight the importance of the supply chain to a security program. Section 2.8 of the Risk Management Framework is dedicated to Supply Chain Risk Management (SCRM) and calls out the risk as follows:

> *The growing dependence on products, systems, and services from external providers, along with the nature of the relationships with those providers, present an increasing amount of risk to an organization. Risk may increase based on the likelihood of occurrence and adverse impact from threat events such as the insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software and hardware, as well as poor manufacturing and development practices in the supply chain, including the failure to build in security or privacy capabilities that enable an organization to better manage risk in its environment.*

Likewise 880-53 section SA focuses on system acquisition with SA-12 dedicated to supply chain risk management, and SA-19 on component authenticity. These two sections bring focus to the need to have intelligence about the supply chain, including how easily it would be for attackers to compromise the supply chain, as well as the ability to detect if a system has been altered in any way before delivery.

Detecting threats in the supply chain can be particularly challenging, particularly at the firmware level. If a system or one of its components has been tampered with in the supply chain, then that change could easily be included as part of a "known-good" or "golden" configuration.

A firmware security platform can be instrumental both in the initial selection of hardware and components as well as verifying the integrity of all newly acquired assets. For instance, during the evaluation of the potential products, firmware scans can be performed to ensure that the systems are not vulnerable to modification of firmware components. Selecting appropriately secure devices would reduce the opportunities for a device to be tampered with while in the supply chain.

Likewise, each newly acquired system should be scanned to ensure that the firmware has not been tampered with in the supply chain by matching the firmware to known good firmware from the manufacturer. However, as was the case with the recent Sunburst campaign, vendors themselves can be compromised including their official signed updates. For these cases it is important to monitor newly acquired systems for anomalous behavior at the firmware level to detect firmware threats.

ECLYPSIUM GUIDANCE AND CONSIDERATIONS:

For systems that have been categorized as priorities, consider implementing the following SCRM controls for firmware:

- Evaluate prospective technology for firmware security and avoid products that can be easily modified at the firmware level (accepting unsigned firmware updates, etc.)
- Check all newly acquired devices to confirm the integrity of the firmware
- Monitor newly acquired devices for signs of malicious firmware behavior
- Organizations may want to require firmware scans from partners in their supply chain in order to identify and isolate where any unwarranted changes are introduced

CM—CONFIGURATION MANAGEMENT

It is important to ensure that the systems are configured properly and that any changes to the system are performed securely. Regular firmware scanning can ensure that firmware is updated, protections are properly enabled, and that the firmware has not been modified or tampered with. SP 800-53 CM-5 calls out the importance of only using updates that have been cryptographically signed as follows:

> *Software and firmware components prevented from installation unless signed with recognized and approved certificates include, for example, software and firmware version updates, patches, service packs, device drivers, and basic input output system (BIOS) updates.*

Eclypsium research has identified widespread issues of systems that do not require firmware updates to be cryptographically signed. In addition to scanning for outdated or vulnerable firmware, the organizations may want to use tools such as Eclypsium to identify systems that do not require signed updates and are thus far more vulnerable to malicious firmware.

ECLYPSIUM GUIDANCE AND CONSIDERATIONS:

Check device setting and configurations that could allow attackers to easily modify firmware.

- Activate firmware and hardware security features
- Ensure that systems require firmware to be signed before applying an update
- Analyze critical devices to ensure unnecessary features are disabled, particularly remote management interfaces that are not used

AC—ACCESS CONTROLS

Section AC-6 is dedicated to one of the most fundamental aspects of information security - the concept of least privilege. These controls are focused on making sure that users and processes are only granted an appropriate level of access in order to deliver their business function. And while we often think of access controls in terms of human users, the standard specifically notes that this should apply to processes as well.

This concept is highly relevant to firmware as organizations need to know how users are able to modify firmware, and likewise what privileges the firmware has to modify the device. For example, if debug features are available on the machine, it can make it very easy for a human attacker to modify firmware on the device via evil-maid attacks. Likewise, the firmware itself can be allowed to configure hardware in an insecure manner. Either of these issues could allow an attacker to gain control over a system. As a result, organizations need to remember that least privilege isn't limited to user policies and Active Directory permissions. Firmware is in scope, and if not properly secured, could subvert all higher-level user policies.

ECLYPSIUM GUIDANCE AND CONSIDERATIONS:

Extend the concept of least privilege to user's ability to control firmware, as well as firmware's ability control the device:

- Check devices for any enabled debug features that could provide any user with visibility and control over firmware that should be limited to developers or administrators.
- Ensure that firmware storage is protected properly to prevent attackers from accessing and modifying firmware.
- Evaluate systems for any vulnerabilities where the firmware is allowed to insecurely configure hardware components.

RA—RISK ASSESSMENT

While the Risk Management Framework addresses the important of vulnerability scanning, section RA-5 is dedicated the specific tools and controls needed to do the job. Specifically, RA-5 calls the importance of tracking both the depth and breadth of any vulnerability scanning. As discussed in earlier sections, many organizations lack the ability to perform automated vulnerability scans of the firmware attacks surface at all, leading to high rates of outdated and unpatched firmware.

However, firmware also resides in a wide variety of components within a device, and this breadth is highly important for vulnerability scanning. Weaknesses in a system drive, or network adapter, or BMC could lead to complete loss of either integrity, confidentiality, or availability of a system. As such, vulnerability scanning should extend to component-level firmware in addition to system level firmware.

ECLYPSIUM GUIDANCE AND CONSIDERATIONS:

Perform regular vulnerability scans of system and component firmware:

- Regular scan all devices for outdated firmware
- Scan for known firmware vulnerabilities
- Extend scanning to critical device components

IR—INCIDENT RESPONSE

The IR set of controls helps an organization operate during an attack or incident and coordinates the response and return to a secure state. This can include analyzing systems that were involved in a security incident and identifying other systems that may have been contaminated.

Malware and sophisticated attackers will often attempt to implant code in firmware in order to persist in the network, and even survive across a complete re-imaging of the host. As such, organizations should consider firmware when performing forensic analysis and hunting for other devices that may have been compromised. Likewise, integrity checks of the firmware should be a standard part of the recovery process for any device involved in an attack.

ECLYPSIUM GUIDANCE AND CONSIDERATIONS:

For systems that have been categorized as priorities, organizations may want to implement firmware controls in the following areas:

- Identify insecure firmware and apply updates
- Ensure that all firmware updates are cryptographically signed and that devices require any firmware updates to be signed
- Analyze systems to ensure the integrity of the boot process and boot firmware
- Detect both known and unknown firmware threats such as implants, backdoors, and rootkits
- Integrate firmware checks into incident response procedures

MA—MAINTENANCE

Section MA-3 calls out the importance of the security of the tools that administrators often use when servicing a system. The document provides the following guidance:

> Maintenance tools can include hardware, software, and firmware items. Maintenance tools are potential vehicles for transporting malicious code, intentionally or unintentionally, into a facility and subsequently into systems.

This is once again a very important area as it applies to firmware security. Modern servers are designed to be remotely administered via IPMI and the system's baseboard management controllers (BMCs). Firmware in BMCs has been a very common source for vulnerabilities, which could allow an attacker to compromise or even completely disable a system. Some vulnerabilities even enable the system to be compromised remotely. These BMCs are designed to provide out-of-band management for the servers, so compromises at this level would give an attacker complete control over the server and its data.

Laptops and other systems will likewise have similar tools designed for remote management. Attackers have recently been observed using Intel's Active Management Technology (AMT) to communicate with a compromised system without being detected by security controls running at the operating system level.

ECLYPSIUM GUIDANCE AND CONSIDERATIONS:

Ensure the security of remote management tools and firmware components:

- Prioritize the analysis and monitoring of server BMCs for vulnerabilities and signs of attack
- Analyze critical devices to ensure remote management tools are not enabled if not necessary.

CONCLUSION

This document highlights some of the many areas where firmware security can play an important role in FISMA compliance and the overarching goal of protecting an agency's mission. Of course the prioritization of firmware security will vary from organization to organization. However, in the past, firmware security was often overlooked not by choice, but due to a lack of tools to automate the work. We believe that through our work at Eclypsium as well as others in the industry, this is changing. The recommendations in the document should in no way be considered exhaustive, but rather to highlight some of the common areas where firmware security can provide immediate value. If you have any questions or concerns related to topics in this document, please contact the Eclypsium team at info@eclypsium.com.