DEFENDING THE FOUNDATION
OF THE ENTERPRISE

ECLYPSIUM.COM | @ECLYPSIUM

# INTRODUCTION

The Federal Information Security Management Act (FISMA) defines the information security requirements for all federal agencies. FISMA spans the fundamental pillars of information security (confidentiality, integrity, and availability). It extends across the lifecycle of a security program from planning, implementation, and ongoing administration of a security program.

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 brief we list the FISMA requirements and what actions we recommend to support them in your environment.

## UNDERSTANDING THE FIRMWARE ATTACK SURFACE

**Eclypsium® guidance and considerations:** Perform an initial firmware vulnerability assessment of critical devices or assets. Eclypsium can automate the analysis of devices assessing risk and integrity. 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- **Systems with out of date firmware**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**

## UNDERSTANDING DEVICE RISK AND IMPACT OF THREATS

**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 exposed more often than other assets. An attacker with physical access to a device can compromise the firmware in 5 minutes. Thus organizations may want to consider firmware security controls for devices that carry high-value information and/or travel to 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. With the complexity and quantity of components (baseboard management controllers, network cards, system firmware, etc.) securing servers that have high privilege and contain critical assets, can be unmanageable.

### Networking and Security Gear

Recent large-scale Russian attacks 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 be targets of attack.

| Control | References | Eclypsium Detections |
|---|---|---|
| **SI—System and Information Integrity**<br>SI-2 Flaw Remediation<br>SI-4 Information System Monitoring<br>SI-7 Software, Firmware, and Information Integrity | In-the-wild implants (eg. HackingTeam, Lojax) | **1**. Confirm firmware integrity<br>**2**. Identify insecure firmware and apply updates<br>**3**. Ensure that all firmware updates are cryptographically signed and that devices require any firmware updates to be signed<br>**4**. Monitor devices for signs of malicious firmware behavior<br>**5**. Analyze systems to ensure the integrity of the boot process and boot firmware<br>**6**. Detect firmware threats such as implants, backdoors, and rootkits |
| **SA—System and Services Acquisition**<br>SA-12 Supply Chain Protection<br>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.<br>**2**. Check all newly acquired devices to confirm the integrity of the firmware<br>**3**. Monitor devices for signs of malicious firmware behavior |
| **CM—Configuration Management**<br>CM-2 Baseline Configuration<br>CM-5 Access Restrictions for Change<br>CM-7 Least Functionality | Secure Configuration<br>PLATINUM malware campaign | **1**. Record expected configuration and behavior of device firmware and hardware<br>**2**. Activate firmware and hardware security features<br>**3**. Analyze critical devices to ensure unnecessary features are disabled, particularly remote management interfaces that are not used. |
| **AC—Access Control**<br>AC-6 Least Privilege | Firmware Storage Vulnerabilities | **1**. Ensure any unnecessary debug functionality is not enabled<br>**2**. Ensure firmware storage is properly protected |
| **RA—Risk Assessment**<br>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<br>**2**. Regular scans should be able to identify<br>**a**. Systems with out of date firmware<br>**b**. Systems with firmware vulnerabilities<br>**c**. Systems with missing protections |
| **IR— Incident Response**<br>IR-4 Incident Handling<br>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<br>**2**. Verify integrity of firmware of all affected hosts during system recovery<br>**3**. Arm staff with tools to assist in forensic analysis of firmware-based threats |
| **MA—Maintenance**<br>MA-3 Maintenance Tools | BMC, IPMI, and Intel AMT as potential attack vectors | **1**. Monitor management interfaces for vulnerabilities or signs of compromise<br>**2**. Scan management resources for vulnerabilities<br>**3**. Only enable remote management tools for devices that have an operational need |

## CONCLUSION

This document highlights some of the areas where firmware security can play an important role in FISMA compliance. Firmware security may have been overlooked in the past but with our work and others in the industry, this is changing. If you have any questions or concerns related to topics in this document, please contact the Eclypsium team at **info@eclypsium.com**.