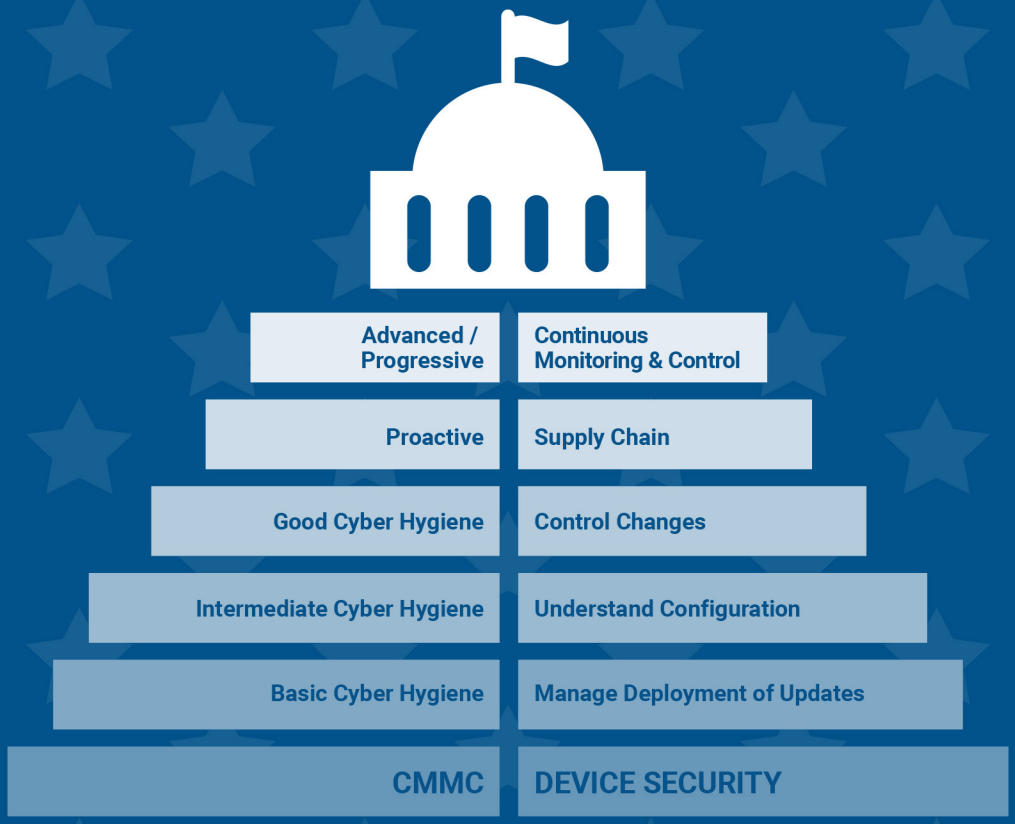


ENSURING DEVICE SECURITY IN FEDERAL ENVIRONMENTS

Progressing from basic cyber hygiene to preventing advanced persistent threats using the Cybersecurity Maturity Model Certification (CMMC) framework.

EXECUTIVE SUMMARY

Strong cybersecurity is foundational to both the economic health and overall national security of any government. And while this is true for all government entities, it takes on extra importance for federal agencies that work with sensitive information and for the many contractors, suppliers and other organizations that form the defense industrial base.

Establishing security at the device level is an integral part of any cybersecurity strategy. Unfortunately, traditional vulnerability scanning and antivirus tools are often blind to weaknesses and threats that reside at the underlying hardware and firmware level of a device. Attacks at this fundamental level violate assumptions and give attackers full control over the device. Such attacks are becoming increasingly common in the wild, driven by advanced actors and by more widespread, opportunistic attack campaigns.

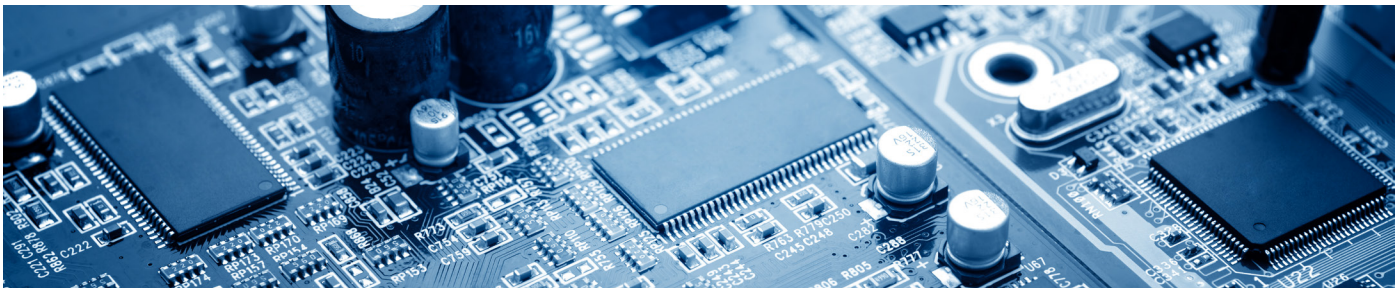
Device security and integrity, while included in frameworks such as NIST SP 800-53 and the DoD Cybersecurity Maturity Model Certification (CMMC), has often been a struggle for organizations. In most cases, they simply lack the tools to establish visibility into and detect threats at this all-important layer. In this document, we will introduce simple steps to build device security into your overall cybersecurity plan.

CONTENTS

INTRODUCTION TO DEVICE SECURITY

Overall device security includes continuous monitoring of both risk and integrity at the lowest, most fundamental levels of each device. This includes understanding settings and configurations specific to the hardware itself, the mechanisms that are used to establish a root of trust on the system, and a wide variety of firmware components both at the system level and in the various hardware components within the device.

Vulnerabilities or compromises at these critical points can allow attackers to subvert virtually any of the security controls running at higher levels, including the operating system and software layers. For example, by compromising the boot process of a system, an attacker could directly patch the kernel of the operating system and thus gain full control over the OS and everything that relies on it. This could include virtually anything on the device, ranging from the basics of breaking user login controls to disabling disk encryption and host-based security such as firewalls and antivirus protection. Additionally, attackers can use this level of access to silently persist on a device without detection. Simply put, organizations cannot trust a device without the ability to verify the integrity of the underlying hardware and firmware.



REAL-WORLD ATTACKS AGAINST DEVICE INTEGRITY

While the potential for such attacks has been well-known for some time, the risk has become far more immediate in recent years as high-impact attacks are increasingly common in the wild.

For example, the well-known Russian hacking group known by the names STRONTIUM, Fancy Bear, Sednit, and APT28 has been observed targeting firmware flaws in multiple attack campaigns. This has included VPNFilter malware, which targeted firmware in vulnerable networking devices, as well as LoJax malware, which compromised the UEFI firmware of devices as a way to maintain persistence on infected hosts. This group is generally considered to be state-sponsored, and a U.S. federal grand jury has indicted seven officers of the Russian GRU in connection with the attacks.

In other nation-state attacks, the Chinese hacking group known as APT41 has exploited vulnerabilities in Cisco, Citrix, and Zoho devices and subsequently attempted to install backdoors on the affected devices. The group's targets vary across areas of both national interest and direct financial gain. This actor had previously leveraged bootkits for persistence, establishing a history of expertise in this area.

Device-level vulnerabilities were also recently abused in order to disrupt critical infrastructure within the United States and other countries. Specifically, recent Denial-of-Service attacks against U.S. power plants were due to firmware vulnerabilities in Cisco ASA firewalls. NERC provided a detailed "Lessons Learned" analysis related to the attack titled Risks Posed by Firewall Firmware Vulnerabilities. Similarly, the attacks that shut down the power grid in portions of Ukraine targeted firmware in order to maximize disruption and complicate recovery.

Firmware has also become a target in a variety of malware campaigns. The recent QSnatch malware compromised network-attached storage (NAS) devices to steal usernames and other information. JungleSec ransomware has similarly targeted the intelligent platform management interfaces used for the out-of-band management of servers.

These examples show that hardware- and firmware-level attacks target many types of devices (laptops, servers, networking gear) and span a wide range of attackers — from advanced state-sponsored attackers to more opportunistic criminal campaigns. Federal agencies and their partners are naturally prime targets for all of these attack campaigns, making device security an immediate security concern.

HOW ATTACKERS COMPROMISE DEVICE INTEGRITY

Attackers have a variety of strategies and techniques at their disposal to compromise devices at the hardware and firmware level. The following section provides a high-level overview of how device integrity can be compromised. For details and analysis, please refer to the online Anatomy of a Firmware Attack resource.

As with many cybersecurity risks, device security problems can often be traced to a vulnerability or misconfiguration. However, instead of a traditional software vulnerability, device integrity is typically compromised due to vulnerabilities in one of its many firmware components or a misconfiguration in hardware security settings. The table below summarizes some of the more common areas of weakness and how they can impact the integrity of the device:

Firmware Component	Role in an Attack
System Firmware, Trusted Platform Module, and Other Boot Firmware (BIOS, UEFI, EFI)	This critical firmware is the first code to run on startup and is key to establishing a root of trust on the machine. If compromised, attackers can subvert the operating system by changing bootcode and directly patching the OS kernel, then further compromise virtual machines and deliver malicious firmware to other components in the system.
System Management Mode (SMM)	SMM and similar firmware control the runtime operation of the device and manage low-level behavior on the system completely independently of the OS. Weaknesses at this level can allow an attacker virtually unfettered access to the system without the knowledge of the OS.
Processors	By exploiting vulnerabilities in the CPU, attackers can view sensitive information such as keys that typically remain in privileged memory. Processor vulnerabilities also have the potential to be exploited remotely, and often can affect any system or operating system even if there are no vulnerabilities in the software and/or OS levels.
Intel ME	Intel's Management Engine (ME) is a common component built into personal computers to enable out-of-band management of the device. ME is also known as TXE in Atom platforms and CSME in Skylake and newer platforms. The firmware within ME includes Active Management Technology (AMT) which has functions and networking that are completely independent of the host operating system. AMT can be used by attackers for command-and-control, data exfiltration, and a variety of other functions.
Baseboard Management Controllers (BMC)	BMCs provide out-of-band management for servers and also have their own independent networking, firmware, and resources. Attacks against BMCs can allow attackers to have complete control over the server and all the higher-layer data and services it contains. These attacks can even be used to permanently brick the server.
USB Devices	USB devices can contain malware in their firmware, enabling attackers to spoof other USB devices, exploit OS kernel and drivers and even deliver malware or malicious firmware to other vulnerable or unprotected components.
Dozens of additional components and modules	Virtually every hardware component within a device relies on firmware that is potentially vulnerable. This includes everything from storage drives to the PCIe bus, which serves critical components such as GPUs, network interfaces and much more. If compromised, attackers can perform devastating DMA attacks that read and write system memory and execute malicious code in the context of the victim operating system.

DESIGNING DEVICE SECURITY INTO YOUR SECURITY PRACTICES

Despite the importance of device security, it has often been a challenge for security teams to get consistent visibility into the hardware and firmware layer of their organizations. Traditional vulnerability scanning tools lack the ability to find firmware vulnerabilities and hardware misconfigurations, and host-based antivirus tools likewise cannot detect threats at these levels. This has often made device integrity a manual, specialized task, typically performed by exception rather than by default.

Fortunately, new cybersecurity tools like those offered by Eclypsium® are changing this. Today, organizations can far more easily ensure that their hardware and firmware receive the same level of visibility and security as their software and networks. In addition to being part of good cybersecurity practice, these capabilities are also called out in a variety of federal regulations and security standards, such as FISMA and the Cybersecurity Maturity Model Certification (CMMC).

CYBERSECURITY REQUIREMENTS FOR DEVICE SECURITY

The principles of device security do not constitute a reinvention of security but rather an extension of strong cybersecurity practices most organizations already use. While the details are unique, the core concepts remain the same.

Establish Visibility - Visibility is a prerequisite for security, and many federal organizations lack the basic understanding of what is in their environments from a hardware and firmware standpoint. Security teams need to be able to see into a broad range of critical devices including laptops, desktops, servers, and networking infrastructure.

Within these devices, teams need visibility into the device configurations and the versions of firmware used in the device. This same visibility must extend to the many hardware components within a system, each typically having its own firmware. Critical components include storage drives, processors, network cards, trusted platform modules (TPMs), GPUs, baseboard management controllers (BMCs), and more.

Establishing this visibility can be a challenge. In addition to having a wide variety of device types, organizations also often have different versions of a particular device as they go through hardware refresh cycles. Visibility and tools can vary considerably from vendor to vendor and component to component. A device integrity platform can bring consistent visibility across these many devices and components.

Find and Fix Vulnerabilities - With visibility established, organizations next need to analyze their hardware and firmware for vulnerabilities or misconfigurations. These types of problems are incredibly common, having been found in most of the devices analyzed by Eclypsium in real-world deployments.

First, organizations need to know if they are running the latest firmware available from the device or component vendor. Teams will need to know if there are any vulnerabilities within their firmware as well as the risk and impact associated with those vulnerabilities.

Other vulnerabilities and configurations could put the integrity of firmware on the device at risk or compromise the boot process and root of trust on the device. For example, it is not uncommon to find devices that allow firmware updates even if the update code is not cryptographically signed. This could allow an attacker to easily replace valid firmware with a malicious implant. Likewise, a variety of settings and configurations could potentially disrupt the secure boot process of the device and allow an attacker to compromise it.

Once problems are found, organizations naturally need to be able to prioritize and address weaknesses based on the risk to the organization. Ideally, weaknesses can be addressed directly via patching and updates. However, not all systems can be patched, in which case organizations may employ continuous monitoring to identify signs of exploitation. Once again, a strong device security solution can automatically scan devices to reveal outdated and vulnerable firmware or device-level misconfigurations, and then assist staff through the update process.

Detect Threats and Compromises - Next, organizations need the ability to detect signs that the integrity of the device has been compromised. Firmware implants, backdoors, and other malicious code can give attackers full control over the victim machine, allow the threat to evade traditional security controls, and even persist across re-imaging of the device.

Organizations should be able to detect both known and unknown threats. First, verify that all firmware matches known good firmware images from the device OEM or component vendor. Firmware also should be scanned for known malicious implants. Even with both measures in place, it is possible for valid, vendor-supplied updates to be compromised in the supply chain or affected by unknown malicious code. In these cases, it is important to track the behavior of firmware and components to detect signs of a compromise.

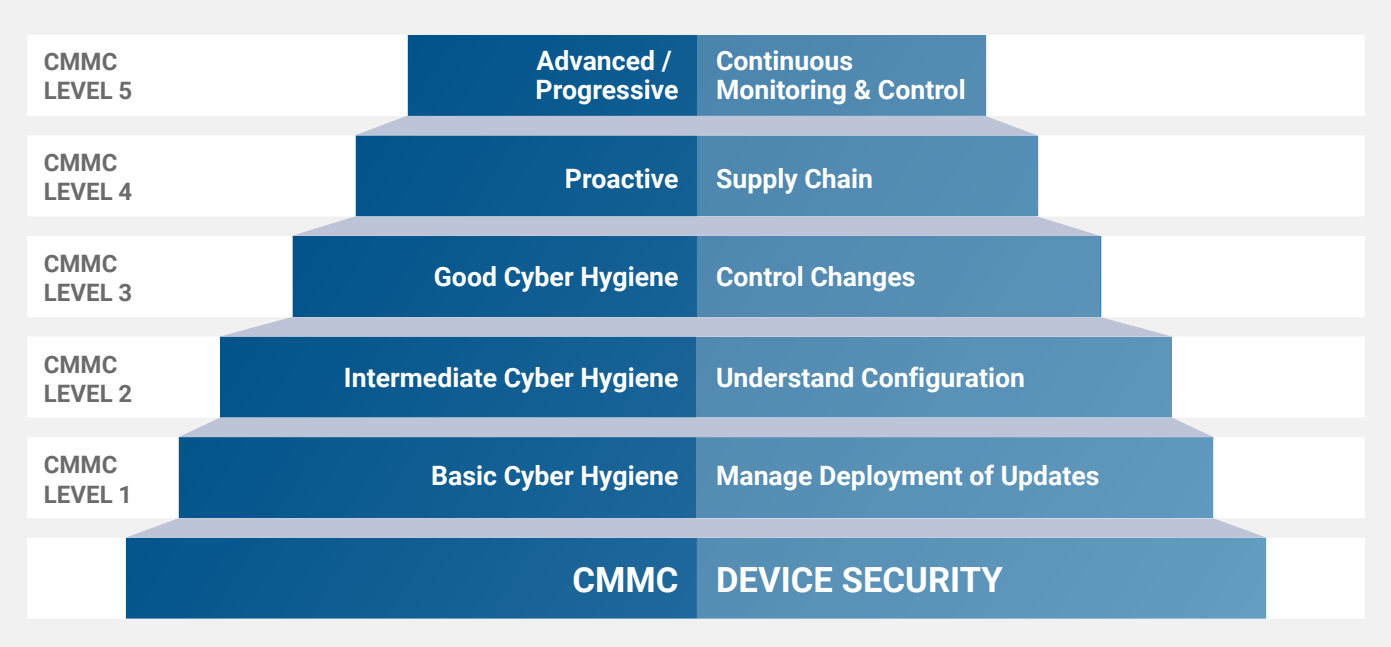
Hardware and firmware should likewise be included in any incident response, recovery, and threat-hunting efforts. Given that attackers often use firmware implants to establish persistence, it is important that any devices involved in a malware infection or other suspected attack be analyzed at the firmware level to ensure the device is not compromised.

DEVICE SECURITY AND THE CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)

These fundamental requirements of device security are not only security best practices, they also fall within the scope of regulatory and security standards such as the Federal Information Security Management Act (FISMA) and the recently released Cybersecurity Maturity Model Certification (CMMC). For more information on the role of device integrity and FISMA, please refer to the Eclypsium FISMA Compliance Best Practices.

CMMC establishes a standardized approach to cybersecurity that applies to all of the many organizations in the Defense Industrial Base (DIB). The standard lays out specific processes and controls that organizations must meet in order to do business with the DoD.

The "maturity model" at the heart of the CMMC is one of its most important traits and distinguishes it from many other standards. The approach breaks cybersecurity practices into progressive levels ranging from basic cyber hygiene to more proactive measures designed to address advanced threats.



The maturity model does a few important things. First, it defines different levels of cybersecurity maturity based on the "type and sensitivity of information being protected and the range of threats." In other words, the cybersecurity maturity of an organization must align with its real-world risk. Additionally, the model lays out the progression of specific security processes across a variety of disciplines. For example, all organizations will need to be able to scan for malicious code, while organizations that face more advanced threats may also need to look for anomalous behavior that could indicate an advanced persistent threat (APT). This provides a blueprint of practices that should be addressed first while setting goals for improvement.

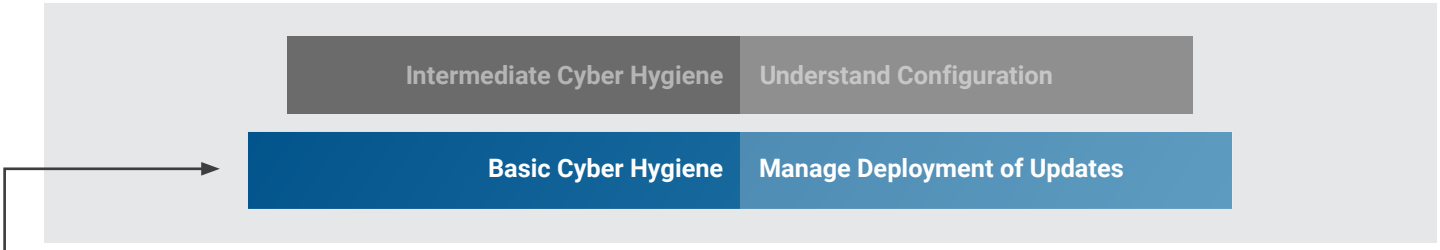
The goals of CMMC Levels 1-5 are defined as follows:

- **Level 1:** Safeguard Federal Contract Information (FCI)
- **Level 2:** Serve as a transition step in the cybersecurity maturity progression to protect Controlled Unclassified Information (CUI)
- **Level 3:** Protect Controlled Unclassified Information (CUI)
- **Levels 4-5:** Protect CUI and reduce the risk of Advanced Persistent Threats (APTs)

Much like FISMA, the CMMC refers to several highly influential NIST documents to spell out specific requirements for compliance. These documents include:

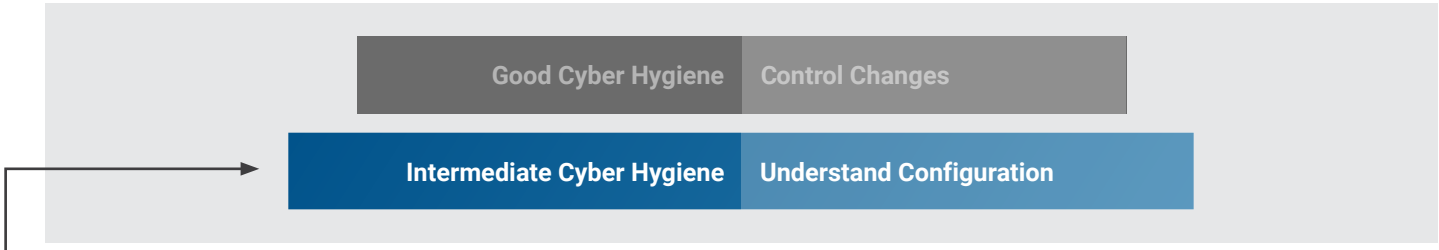
- **SP 800-171 Rev. 1:** Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. Controls in this document are applied to CMMC Levels 1-3.
- **SP 800-171B:** Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: Enhanced Security Requirements for Critical Programs and High Value Assets. Controls in this document are applied to CMMC Levels 4-5.
- **SP 800-53 Rev. 4:** Security and Privacy Controls for Federal Information Systems and Organizations. While not directly referenced in the CMMC, SP 800-53 is a foundational set of security controls that is heavily referenced in both SP 800-171 Rev. 1 and SP 800-171B.

These documents lay out the details of how organizations can achieve compliance while prominently featuring the roles of hardware, firmware, and overall device security. The following sections summarize the key security domains, levels, and practices defined in the CMMC that directly apply to device security. It is important to note that not all levels apply to every organization. Rather, they are shown to illustrate the concepts of progression and maturity within each type of security control.



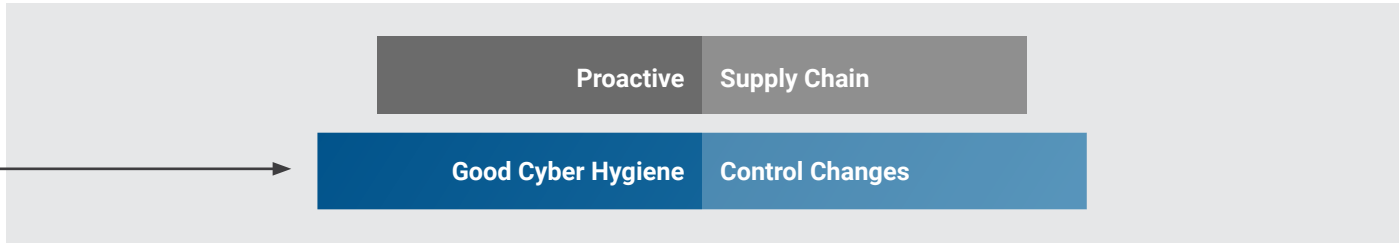
Level 1

SI.1.210 - Identify, report, and correct information and information system flaws in a timely manner.	This corresponds to the 800-53 control SI-2 FLAW REMEDIATION. Firmware vulnerabilities enable compromise both from the software layer, such as a malware infection, or from physical attacks such as DMA attack via exposed PCIe ports. As a result, organizations should regularly scan their devices for vulnerabilities and signs of firmware- or hardware-level tampering. More information on this topic can be found in our white paper, Enterprise Best Practices for Firmware Updates.



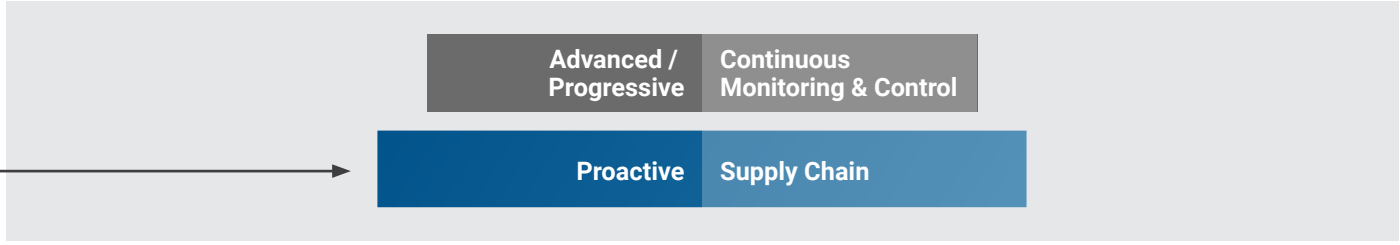
Level 2

CM.2.064 - Establish and enforce security configuration settings for information technology products employed in organizational systems	As in the 800-53 controls CM-2 BASELINE CONFIGURATION, CM-6 CONFIGURATION SETTINGS, and CM-8 INFORMATION SYSTEM COMPONENT INVENTORY, organizations need to specifically know the configurations of their hardware and firmware. This information allows organizations to maintain an up-to-date understanding of their hardware and firmware attack surface.
RM.2.142 - Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. **RM.2.143** - Remediate vulnerabilities in accordance with risk assessments.	The number of firmware vulnerabilities has spiked in recent years: 2019 had more than seven times as many firmware vulnerability reports compared with 2016. Weaknesses in firmware can be particularly high-impact due to the privileges and control they provide attackers.
CA.2.159 - Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	Security Assessments enable organizations to understand risk through capabilities to test, deploy, and even roll back firmware in the case of problems.
IR.2.092 - Establish an operation incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	Attackers can hide malicious code within firmware to persist even when the operating system is completely reinstalled or drives are replaced. As a result, the integrity of firmware should be checked as part of the standard incident response process.



Level 3

CM.3.067 - Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	After establishing a good baseline, Level 3 organizations will control changes with review and approval. As explained in 800-53 CM-5, firmware components and their configuration can have significant effects on security, and they are a crucial part of this change control.



Level 4

AM.4.226 - Employ a capability to discover and identify systems with specific component attributes (e.g., firmware level, OS type) within your inventory	AM.4.226 directly addresses the need for firmware and hardware visibility within an environment. This visibility is crucial in order for organizations to quickly and effectively know if they are impacted by newly discovered vulnerabilities or threat information.
RM.4.148 - Develop and update as required a plan for managing supply chain risks associated with the IT supply chain.	As in the 800-53 control SA-12 SUPPLY CHAIN PROTECTION, the organization's security strategy should cover the supply chain of the threats system and its components. Point-in-time or continuous checks can help detect and track down such issues.

Advanced / Progressive | **Continuous Monitoring & Control**

Level 5	
CM.5.074 - Verify the integrity and correctness of security-critical or essential software as defined by the organization (e.g., roots of trust, formal verification, or cryptographic signatures).	As in the NIST SI-7 controls that call out firmware integrity, Level 5 organizations must be able to securely verify the integrity of critical firmware. Such visibility is necessary to ensure that a system's firmware and boot process has not been compromised by attackers.
SI.5.223 - Monitor individual and system components on an ongoing basis for anomalous or suspicious behavior.	More than just a one-time check, at Level 5, the organization performs ongoing monitoring of firmware/hardware behavior to identify threats that do not match known signatures or IOCs.
IR.5.106 - In response to cyber incidents, utilize forensic data gathering across impacted systems, ensuring the secure transfer and protection of forensic data.	Threat hunters and forensic teams of Level 5 organizations should be armed with tools to collect and analyze suspicious or malicious firmware in the environment.

CONCLUSION

Ensuring the security of devices is a critical component of any strong cybersecurity practice, one that has taken on particular importance in federal agencies and federally regulated businesses. The increase of hardware- and firmware-based attacks — from both nation-state adversaries and opportunistic criminal organizations — has the potential to undercut many of the traditional security measures used today, putting critical systems, information, and ultimately national security at risk in the process.

However, while securing the hardware and firmware infrastructure of an organization has traditionally been a difficult, time-consuming process, the availability of new security tools such as Eclypsium and the open-source CHIPSEC framework allows security teams to efficiently extend protection to these critical layers. Device security platforms allow security teams to ensure consistent visibility into their devices, including the hardware components and firmware within. With visibility established, organizations can automatically detect vulnerabilities and misconfigurations that put devices at risk, as well as identify threats such as firmware implants and other malware. If you would like to learn more about device security and how to integrate it into your security practice, please contact Eclypsium at info@eclypsium.com.