NIST | SP 800-53

FIRMWARE, SUPPLY CHAIN, AND FRAMEWORKS: NIST SP 800-53

NIST Special Publication 800-53 rev 5, *Security and Privacy Controls for Information Systems and Organizations*, is one of the most important and influential documents in cybersecurity today. SP 800-53 provides the industry's most detailed listing of security controls designed to help organizations protect their many assets from a wide range of threats. Originally targeted toward U.S. federal agencies, SP 800-53 has become a mainstay within the private sector and organizations from virtually every industry.

SP 800-53 also plays a critical role in relation to other industry regulations and security frameworks by providing highly detailed information on the security controls needed in order to achieve higher-level security goals and best practices. The document is directly referenced as part of NIST's Cybersecurity Framework (CSF) and is mapped to many of the most important security standards and regulations including ISO 27001, COBIT, PCI-DSS, and the CIS Critical Security Controls.

It is important to note that 800-53 undergoes regular revisions in order to keep pace with changes in the threat and technology landscape, and firmware security and supply chain risk management are two of the most notable examples. For example, in the older Rev 3 version of publication, the term "supply chain" only appeared 13 times, compared to 106 times in Rev 4, and over 700 times in the most recent Rev 5. Rev 5 also saw the introduction of an entire family of security controls dedicated to Supply Chain Risk Management in addition to the previous Systems and Services Acquisition family of controls.

Firmware security is following a similar trajectory and is consistently referenced throughout the document across a wide range of controls. In fact, the term "firmware" appears 155 times in Rev 5 compared to only 16 times in Rev 3.

Firmware a supply chain security also play critical roles in many controls even when not called out by name. For example, the control, *SI-3 Malicious Code Protection*, rightly does not distinguish between malicious software and firmware and instead leaves the requirement open to address any type of malicious code. Likewise, firmware and supply chain play a direct role in controls such as vulnerability management and many others even when not directly referenced.

As a result, supply chain and firmware security play key roles in a very wide range of security controls. However, many organizations are still in the early stages of integrating these disciplines into their overall cybersecurity strategy. This document attempts to ease this transition by providing organizations with a view of SP 800-53 specifically through the lens of firmware and supply chain security. To this end, we cover the specific 800-53 controls that are relevant and how a firmware security platform can be used to address these needs.

FIRMWARE AND SUPPLY CHAIN IN SP 800-53 CONTROLS

SP 800-53 is organized into 20 "families" of controls, which each contain a variety of underlying specific controls with detailed guidance and discussion. For example, Access Control (AC) is a control family, which contains 25 controls such as AC-2 Account Management and AC-17 Remote Access.

We have identified 40 controls across 12 control families in which firmware or supply chain security is either directly named or plays a critical role in the context of the control. **Appendix A** provides a consolidated table of these controls along with brief excerpts from SP 800-53 for reference. Additionally, for each control family, we have highlighted some of the most common and high-impact firmware and supply chain security gaps found in most organizations today, along with steps that security teams can take to reduce their risk.

AC - Access Control

Relevant Controls:

- AC-4 Information Flow Enforcement
- AC-6 Least Privilege

Firmware is the most privileged code on virtually every device, and it is critical that organizations properly enforce least privilege for access to this code. However, firmware also plays a major and often overlooked role when it comes to the protection of networking and security infrastructure. AC-4 Information Flow Enforcement also calls out firmware, stating:

> *Organizations also consider the trustworthiness of filtering and/or inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement.*

Network devices and security tools such as **firewalls** and **VPNs** have themselves become some of the most heavily attacked assets in any organization. Advanced threat actors and ransomware groups have targeted vulnerabilities in these devices in order to gain initial access into an environment, which can then be used to spread further into the network and establish ongoing persistence. Compromising network devices also means that attackers could potentially manipulate traffic and/or disable security inspection.

Firmware security plays a particularly important role in protecting these devices. Unlike laptops and servers that run standard operating systems, network devices rely on highly customized firmware and other device-level code that is tightly integrated with the hardware itself. These devices typically can't support a traditional security agent, making it even harder for security teams to find vulnerabilities and threats using traditional tools. Organizations should consider firmware security tools that can both identify vulnerabilities within these devices as well as verify the integrity of their firmware to identify any potentially compromised devices.

CA - Assessment, Authorization, and Monitoring

Relevant Controls:

- CA-2 Control Assessments
- CA-7 Continuous Monitoring
- CA-8 Penetration Testing

CA-7 Continuous Monitoring states:

> *Continuous monitoring at the system level facilitates ongoing awareness of the system security and privacy posture to support organizational risk management decisions. The terms "continuous" and "ongoing" imply that organizations assess and monitor their controls and risks at a frequency sufficient to support risk-based decisions.*

While most security teams have automated tools for monitoring the posture of their software and operating systems, the protection of firmware often requires manual, time-consuming effort from staff. This makes it almost impossible for organizations to maintain appropriate visibility into the posture and integrity of their firmware. A firmware security platform automates the analysis of firmware and can be configured to perform regularly scheduled scans of all firmware assets based on the unique needs of the organization and its assets.

CM - Configuration Management

Relevant Controls:

- CM-2 Baseline Configuration
- CM-3 Configuration Change Control
- CM-5 Access Restrictions for Change
- CM-6 Configuration Settings
- CM-7 Least Functionality
- CM-8 System Component Inventory
- CM-14 Signed Components

Organizations often try to keep an inventory of their physical devices, yet this discipline typically does not extend down to the underlying firmware. This is an important gap because it is the firmware that defines the actual behavior of the hardware as well as the many potential weaknesses that could allow an attacker to take control of the asset.

It is critical that organizations have a complete understanding of the firmware in their devices and how it is configured in order to properly manage their hardware attack surface and to verify the integrity of the supply chain. Devices rely on a variety of low-level settings and protections that can leave a device defenseless if they aren't configured properly. As SP 800-53 notes, this extends down to the level of firmware in the physical components within a device.

Organizations should pay close attention to control, CM-2 Baseline Configuration. A firmware security platform can automatically monitor the baseline of all critical firmware on a system and can alert staff to any changes to the firmware baseline. Updates can be controlled and include the ability to roll back to previous known "good" versions.

Likewise, firmware security tools can vastly simplify the work of building and maintaining an inventory of the firmware and components within a system as defined by CM-8 System Component Inventory. This can include components such as network adapters, CPUs, memory, and storage drives, among many others.

CM-14 Signed Components calls out the need for organizations to ensure that firmware updates are valid and properly signed. This is one of the most basic configuration settings of a device or component, but without it, attackers can overwrite valid firmware with malicious code. A proper firmware security platform can proactively identify systems with such misconfigurations or missing protections. Additionally, they can maintain a library of valid vendor-supplied firmware to verify that only valid versions of the firmware are used or applied during updates.

IA - Identification and Authentication

Relevant Controls:

- IA-5 Authenticator Management

IA-5 Authenticator Management calls out that private keys, naturally must remain private. And at a hardware level, this task is handled by a physical chip called the Trusted Platform Module (TPM) which generates, stores, and limits the use of cryptographic keys. **Vulnerabilities** or attacks against the TPM can allow attackers to compromise these keys and gain trusted access to any number of assets. A firmware security platform can scan devices for vulnerabilities in the TPM that could put private keys at risk.

IR - Incident Response

Relevant Controls:

- IR-4 Incident Handling

Adversaries increasingly attempt to introduce malicious code into firmware as a way to establish persistence and evade higher-layer controls. The collection and analysis of unknown or malicious firmware during an incident can help reveal the tactics, goals, and identity of an adversary. Any changes to the firmware integrity of devices involved in a security incident should be closely analyzed for threats. This may require the collection and analysis of the firmware code running on the system or within system components. The incident handling requirements also extend to the supply chain with the standard calling out the need to "Coordinate incident handling activities involving supply chain events with other organizations involved in the supply chain."

As with any analysis of malicious code, any analysis of unknown firmware should be performed in a highly controlled manner. Firmware-specific tools can be used to collect firmware for forensic analysis either by internal staff or external service providers.

MA - Maintenance

Relevant Controls:

- MA-3 Maintenance Tools

Maintenance tools often require privileged access in order to properly address the needs of a system, and this is particularly true when it comes to firmware. MA-3 Maintenance Tools notes that such tools "can include hardware, software, and firmware items..."

There are several firmware-specific items that security teams will want to consider as it pertains to management tools. First, most laptops and servers contain built-in mechanisms to enable the out-of-band management of the device. In servers, this capability is provided by a dedicated baseboard management controller (BMC) which contains its own firmware, memory, processor, networking, and power that is completely independent of the host. **Attackers** have targeted these critical components in order to take control of or damage servers. In laptops, similar functionality is provided by separate firmware in the chipset such as the Intel Management Engine (ME) and Active Management Technology (AMT). Attackers such as the **PLATINUM** group have previously abused these capabilities to hide command-and-control from OS-level security controls.

It is important that security teams have the ability to monitor these management features for vulnerabilities or any signs of compromise.

RA - Risk Assessment

Relevant Controls:

- RA-3 Risk Assessment
- RA-5 Vulnerability Monitoring and Scanning
- RA-9 Criticality Analysis
- RA-10 Threat Hunting

Vulnerability and risk management are some of the most fundamental aspects of any organization's security practice. However, the tools that are traditionally used to assess software and operating systems lack the ability to reliably analyze firmware for weaknesses. This is due to the low-level nature of firmware, which often requires authenticated scanning and specialized drivers in order to gain the needed level of visibility.

There are also a wide range of low-level settings and protections that must be properly configured in order to properly secure a device. These risks are typically not detected by traditional vulnerability management scanners, which instead focus on specific vulnerabilities or CVEs. Just as importantly, many vulnerability management tools will rely on information provided by the operating system. As **recent attacks** have shown, an attacker with control over the firmware can report false information in terms of the version of firmware that is installed and even prevent the system from being updated.

Unsurprisingly, virtually all of these aspects apply to supply chain risk management as well. Many of the controls in the RA family call out this need specifically. The complexity and constantly changing nature of modern supply chains creates many opportunities for a vulnerability, misconfiguration, or threat to be introduced into a product. Only by being able to independently assess the risk of physical devices and their components will an organization be able to ensure the integrity of their technology supply chain.

Specialized firmware security tools can close these gaps and ensure that risk and vulnerability assessments go all the way to the firmware. This can include the detection of firmware vulnerabilities and misconfigurations and can use OS-independent mechanisms in order to truly verify the state of the firmware.

RA-10 Threat Hunting introduces another area where firmware will play an important role. Adversaries specifically target firmware in order to persist on a system without detection and to evade traditional security controls. Threat hunters should be able to hunt for threats or any unexpected code or anomalous behavior within the firmware of devices and their components.

SA - System and Services Acquisition

Relevant Controls:

- SA-3 System Development Lifecycle
- SA-8 Security and Privacy Engineering Principles
- SA-10 Developer Configuration Management
- SA-10 Developer Configuration Management
- SA-11 Developer Testing and Evaluation
- SA-17 Developer Security and Privacy Architecture and Design
- SA-20 Custom Development of Critical Components
- SA-22 Unsupported System Components

The SA family is intrinsically connected to supply chain security and calls out firmware across many of the included controls. This section lays out the importance of considering firmware at the earliest stages of the technology lifecycle and establishes standards both for internal developers as well as outside technology vendors. Given that the vast majority of firmware is delivered by outside vendors, many of the requirements identified in SA will apply to any selected vendors.

However, security teams will need the appropriate tools both to evaluate prospective vendors and to verify that selected vendors are meeting their obligations in regard to developing and delivering secure firmware. A firmware security platform can arm staff to independently verify the state of all firmware both during the technology selection process and when verifying newly acquired assets.

SC - System and Communication Function

Relevant Controls:

- SSC-3 Security Function Isolation
- SC-37 Out of Band Channels
- SC-39 Process Isolation
- SC-51 Hardware-Based Protection

Firmware security is important to several SC controls, however, there are two important areas that are particularly significant and are often overlooked. SC-37 Out of Band Channels calls out the need to secure out-of-band channels, which can include "network paths physically separate from network paths used for operational traffic."

As discussed in the MA section, most servers and traditional systems such as workstations and laptops will include dedicated hardware used for out-of-band management. The baseboard management controllers within servers provide out-of-band management of the device and include their own independent network interfaces, memory, processing, and power. Any compromise to the BMC can allow an attacker to take control of the server or disable it entirely. More traditional laptops often include out-of-band management capabilities such as Intel's AMT which runs on the dedicated Management Engine (ME) chip. While these components will share access to the system's network interface, they typically have a dedicated connection to the interface that is independent of the operating system. These capabilities have been used by adversaries to establish **hidden command-and-control channels**.

Additionally, SC-51 Hardware-Based Protection calls out the need to " employ hardware-based, write-protect for organization-defined system firmware components." This requirement is particularly important based on active threats seen in the wild. Firmware threats such as **TrickBoot**, **MosaicRegressor**, and **LoJax** all target devices in which the system UEFI or BIOS firmware is not properly write-protected.

A firmware security platform can easily address these challenges by scanning out-of-band management firmware for vulnerabilities and threats, while also proactively identifying any devices that are not properly write-protecting their firmware.

SI - System and Information Integrity

Relevant Controls:

- SI-2 Flaw Remediation
- SI-3 Malicious Code Protection
- SI-4 System Monitoring
- SI-7 Software, Firmware, and Information Integrity

The SI family of controls is one of the most important in regard to firmware security. SI-3 Malicious Code Protection calls out the need for both signature and non-signature-based methods for detecting threats within code. Malicious code within firmware can have a very impact as it can allow attackers to control and subvert all other aspects of the system. Threats such as firmware rootkits/bootkits, implants, and backdoors have become increasingly common yet are often undetectable by traditional endpoint security and EDR tools that rely on the operating system in order to analyze the underlying firmware. It is critical for organizations to employ tools that can detect any changes to the integrity of firmware, detect known firmware threats, and detect anomalous firmware behavior that could indicate the presence of new or unknown threats.

SI-7 Software, Firmware, and Information Integrity goes into great detail regarding the need to verify and monitor the integrity of firmware within an organization's devices. This includes not only monitoring the firmware itself, but also the integrity of the boot process of the device. The control also specifies that organizations should:

- *Employ centrally managed integrity verification tools.*
- *Implement cryptographic mechanisms to detect unauthorized changes to software, firmware, and information.*
- *Employ automated tools that provide notification… upon discovering discrepancies during integrity verification.*

A firmware security platform provides all of these key capabilities, allowing organizations to verify the integrity of firmware, detect any changes, and automatically alert or other automated systems when problems are detected.

SR - Supply Chain Risk Management

Relevant Controls:

- SR-2 Supply Chain Risk Management Plan
- SR-3 Supply Chain Controls and Processes
- SR-4 Provenance
- SR-6 Supplier Assessment and Review
- SR-11 Component Authenticity

Physical devices and equipment are some of the most common and valuable assets within an organization, and these devices typically rely on highly complex supply chains involving dozens of suppliers and subsuppliers across many countries of origin. Since virtually every physical system and component relies on firmware, every part of the supply chain can potentially introduce vulnerable or malicious firmware components. The paper, Weak Links: Firmware Security for ICT Supply Chains (**PDF**) provides an in-depth analysis of how to integrate firmware into an organization's SCRM strategy.

The SR section specifically calls out the need to verify the authenticity and provenance of all firmware and components within a system as well as the ability to perform independent testing of technology suppliers.

A firmware security platform provides the critical ability to independently verify and assess all critical firmware components within a device throughout all phases of the supply chain. Prospective equipment can be evaluated to identify supply chain problems during the selection process. Additionally, staff can quickly verify the authenticity of newly acquired devices, while verifying that they have not been tampered with prior to delivery. Teams can likewise analyze that updates are valid and monitor the behavior of firmware following an update to identify threats potentially introduced into "approved" vendor updates.

CONCLUSIONS AND NEXT STEPS

Firmware security plays a critical role throughout SP 800-53 rev 5. This paper seeks to introduce some of the most important examples with a focus on the most common technical and procedural gaps facing organizations today.

However, it is important to note that as threat actors continue to shift their focus to firmware, new security tools are also available that can help security teams incorporate and automate firmware security into their existing practices."Firmware security", for our purposes, means giving organizations the ability to identify, verify and fortify firmware wherever it exists in their infrastructure:

Identify - Automate device discovery and provide ongoing visibility into each device's firmware, from individual firmware configurations to an inventory of the dozens of unique firmware components on every device. Quickly zero in on important components, attributes, or changes that can impact your security posture.

Verify - Proactively identify risks from outdated or vulnerable firmware or device misconfigurations. Verify the integrity of all firmware and detect known and unknown firmware threats including rootkits, implants, and backdoors.

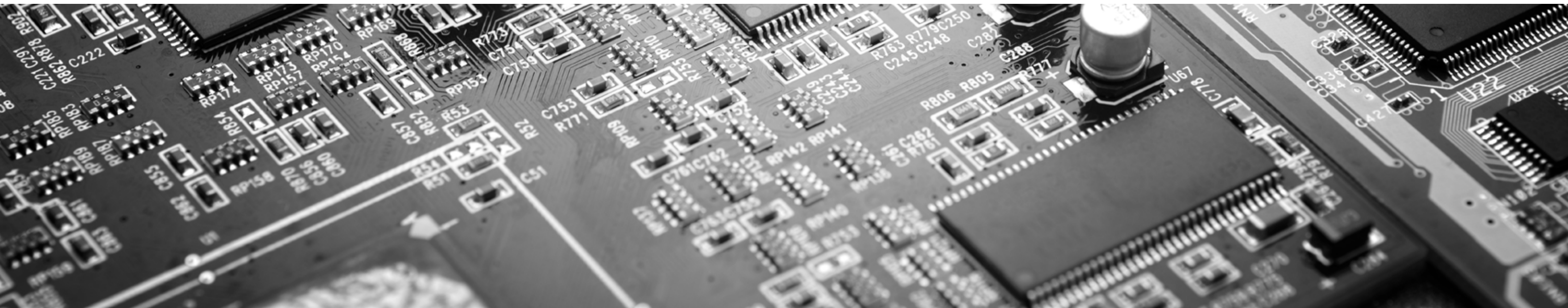
Fortify - Remotely apply patches or updates to proactively mitigate device risks. Receive automated alerts to any firmware integrity changes and drive automated responses via integration with your existing IT and security tools with pre-built integrations with leading SIEMs, vulnerability management, and device management tools.

Built on industry-leading expertise and research, the Eclypsium firmware security platform makes it easy for organizations to integrate firmware security into all phases of their security and risk practices. With a single automated solution organizations can identify and inventory their devices and firmware, find and prioritize vulnerabilities, detect firmware level threats, and take action to fortify their devices and mitigate risks. If you would like to learn more, we recommend the following resources:

To learn more about firmware security, we recommend the **Definitive Guide to Firmware Security**.

To stay up to date with latest firmware security news, please subscribe to the **Below the Surface Threat Report**

To learn more about Eclypsium, please contact our team at **info@eclypsium.com**.



APPENDIX A - SUMMARY OF FIRMWARE CONTROLS

Firmware related controls are designated with an asterisk (*).

Access Control	
AC-4 Information Flow Enforcement	Organizations also consider the trustworthiness of filtering and/or inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement.
AC-6 Least Privilege	Authorize access for organization-defined security functions (deployed in hardware, software, and firmware)
Assessment, Authorization, and Monitoring	
CA-2 Control Assessments	The required skills include general knowledge of risk management concepts and approaches as well as comprehensive knowledge of and experience with the hardware, software, and firmware system components implemented.
CA-7 Continuous Monitoring	The terms "continuous" and "ongoing" imply that organizations assess and monitor their controls and risks at a frequency sufficient to support risk-based decisions. Automation supports more frequent updates to hardware, software, and firmware inventories, authorization packages, and other system information.
CA-8 Penetration Testing	Authorize access for organization-defined security functions (deployed in hardware, software, and firmware)
Configuration Management	
CM-2 Baseline Configuration	Automated mechanisms that help organizations maintain consistent baseline configurations for systems include configuration management tools, hardware, software, firmware inventory tools, and network management tools. Retaining previous versions of baseline configurations to support rollback include hardware, software, firmware, configuration files, configuration records, and associated documentation.
CM-3 Configuration Change Control	Changes to systems include modifications to hardware, software, or firmware components and configuration settings defined in CM-6.
CM-5 Access Restrictions for Change	Changes to the hardware, software, or firmware components of systems or the operational procedures related to the system can potentially have significant effects on the security of the systems or individuals' privacy. Therefore, organizations permit only qualified and authorized individuals to access systems for purposes of initiating changes.

CM-6 Configuration Settings	Identify, document, and approve any deviations from established configuration settings
CM-7 Least Functionality	Code execution in protected environments applies to all sources of binary or machine-executable code, including commercial software and firmware and open-source software.
CM-8 System Component Inventory	System components are discrete, identifiable information technology assets that include hardware, software, and firmware. Detect the presence of unauthorized hardware, software, and firmware components within the system…
CM-14 Signed Components	Prevent the installation of software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.
Contingency Planning	
CP-9 System Backup	Security-related information includes inventories of system hardware, software, and firmware components.
Identification and Authentication	
IA-5 Authenticator Management*	(a) For public key-based authentication: (1) Enforce authorized access to the corresponding private key;
Incident Response	
IR-4 Incident Handling*	Analyze malicious code and/or other residual artifacts remaining in the system after the incident. Coordinate incident handling activities involving supply chain events with other organizations involved in the supply chain.
Maintenance	
MA-3 Maintenance Tools	Approve, control, and monitor the use of system maintenance tools; Maintenance tools can include hardware, software, and firmware items and may be pre-installed, brought in with maintenance personnel on media, cloud-based, or downloaded from a website.

Risk Assessment	
RA-3 Risk Assessment*	Conduct a risk assessment, including: 1. Identifying threats to and vulnerabilities in the system; 2. Determining the likelihood and magnitude of harm… Assess supply chain risks associated with organization-defined systems, system components, and system services and Update the supply chain risk assessment when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain.
RA-5 Vulnerability Monitoring and Scanning*	a. Monitor and scan for vulnerabilities in the system and hosted applications Enumerating platforms, software flaws, and improper configurations; Measuring vulnerability impact; Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.
RA-9 Criticality Analysis	The functional decomposition includes the identification of organizational missions supported by the system, decomposition into the specific functions to perform those missions, and traceability to the hardware, software, and firmware components that implement those functions, including when the functions are shared by many components within and external to the system.
RA-10 Threat Hunting*	Establish and maintain a cyber threat hunting capability to: 1. Search for indicators of compromise in organizational systems; and 2. Detect, track, and disrupt threats that evade existing controls;
System and Services Acquisition	
SA-3 System Development Lifecycle	Acquire, develop, and manage the system using organization-defined system development life cycle Technology refresh planning may encompass hardware, software, firmware, processes, personnel skill sets, suppliers, service providers, and facilities.
SA-8 Security and Privacy Engineering Principles	Organizations can apply systems security and privacy engineering principles to new systems under development or to systems undergoing upgrades…given the current state of hardware, software, and firmware components within those systems.

SA-10 Developer Configuration Management	Require the developer of the system, system component, or system service to enable integrity verification of software and firmware components. The integrity checking mechanisms can also address counterfeiting of software and firmware components. Organizations verify the integrity of software and firmware components, for example, through secure one-way hashes provided by developers. Delivered software and firmware components also include any updates to such components.
SA-11 Developer Testing and Evaluation	Require the developer of the system, system component, or system service to perform attack surface reviews. Attack surfaces include any accessible areas where weaknesses or deficiencies in the hardware, software, and firmware components provide opportunities for adversaries to exploit vulnerabilities.
SA-17 Developer Security and Privacy Architecture and Design	Require the developer of the system, system component, or system service to produce…a formal top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of exceptions, error messages, and effects. Require the developer of the system, system component, or system service to structure security-relevant hardware, software, and firmware to facilitate controlling access with least privilege.
SA-20 Custom Development of Critical Components	Reimplementation or custom development of such components may satisfy requirements for higher assurance and is carried out by initiating changes to system components (including hardware, software, and firmware) such that the standard attacks by adversaries are less likely to succeed.
SA-22 Unsupported System Components	Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer Discussion: Support for system components includes software patches, firmware updates, replacement parts, and maintenance contracts.
System and Communication Function	
SC-3 Security Function Isolation	The isolation boundary controls access to and protects the integrity of the hardware, software, and firmware that perform system security functions. Systems implement code separation in many ways, such as through the provision of security kernels via processor rings or processor modes.
SC-37 Out of Band Channels*	Out-of-band channels include local, non-network accesses to systems; network paths physically separate from network paths used for operational traffic;
SC-39 Process Isolation	Maintaining separate execution domains for executing processes can be achieved, for example, by implementing separate address spaces. Process isolation technologies, including sandboxing or virtualization, logically separate software and firmware from other software, firmware, and data.
SC-51 Hardware-Based Protection	a. Employ hardware-based, write-protect for system firmware components

System and Information Integrity	
SI-2 Flaw Remediation	Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation. The need to remediate system flaws applies to all types of software and firmware.
SI-3 Malicious Code Protection	Malicious code protection mechanisms include both signature- and nonsignature-based technologies.
SI-4 System Monitoring*	System monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at external interfaces to the system. Internal monitoring includes the observation of events occurring within the system.
SI-7 Software, Firmware, and Information Integrity	Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: Firmware interfaces include Unified Extensible Firmware Interface (UEFI) and Basic Input/Output System (BIOS). Perform an integrity check of software, firmware, and information] (one or more): at startup; at transitional states or security-relevant events or organization-defined frequency. Security-relevant events include the identification of new threats to which organizational systems are susceptible and the installation of new hardware, software, or firmware. Transitional states include system startup, restart, shutdown, and abort. Employ automated tools that provide notification to organization-defined personnel upon discovering discrepancies during integrity verification. Employ centrally managed integrity verification tools. Implement cryptographic mechanisms to detect unauthorized changes to software, firmware, and information. Verify the integrity of the boot process of organization-defined system components. Implement cryptographic mechanisms to authenticate the following software or firmware components prior to installation
Supply Chain Risk Management	
SR-2 Supply Chain Risk Management Plan*	Develop an organization-wide strategy for managing supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services;
SR-3 Supply Chain Controls and Processes	Supply chain processes include hardware, software, and firmware development processes; shipping and handling procedures; personnel security and physical security programs; configuration management tools, techniques, and measures to maintain provenance; or other programs, processes, or procedures associated with the development, acquisition, maintenance and disposal of systems and system components.

SR-4 Provenance	Establish and maintain unique identification of the following supply chain elements, processes, and personnel associated with the identified system and critical system components: Supply chain processes include development processes for hardware, software, and firmware; shipping and handling procedures; configuration management tools, techniques, and measures to maintain provenance; personnel and physical security programs; or other programs, processes, or procedures associated with the production and distribution of supply chain elements.
SR-6 Supplier Assessment and Review	Employ (one or more): organizational analysis; independent third-party analysis; organizational testing; independent third-party testing] of the following supply chain elements, processes, and actors associated with the system, system component, or system service: Supply chain processes include supply chain risk management programs; SCRM strategies and implementation plans; personnel and physical security programs; hardware, software, and firmware development processes
SR-11 Component Authenticity	Train organization-defined personnel to detect counterfeit system components (including hardware, software, and firmware).