USING ECLYPSIUM TO PROTECT YOUR DATA AND ALIGN WITH NIST 800-171_

In the sometimes dizzying world of NIST publications, SP 800-171 plays an increasingly important role in modern information security. At a high level, there are two things that make 800-171 stand out from other NIST standards. First, it applies to non-federal organizations such as federal contractors, service providers, and research institutions that work with or handle federal data. Second, it applies to a class of sensitive data known officially as Controlled Unclassified Information or CUI. This includes an incredibly broad range of information that needs to be protected, yet is not officially Classified (e.g. “Secret” or “Top Secret”). As such, CUI can include data such as Personally Identifiable Information (PII), certain types of research, intellectual property such as design schematics, technical manuals, and many other forms of trade secrets.

At its heart, SP 800-171 is about how the U.S. Government protects sensitive data in its information and technology supply chains. For example, the U.S. Department of Defense mandates that all organizations that contract with the DoD, known collectively as the Defense Industrial Base (DIB), must comply with SP 800-171. However, the same is true for organizations that contract with other agencies such as NASA and GSA. It also applies to manufacturers that supply products and services to federal agencies. So while 800-171 can be seen as a data-centric standard with its focus on CUI, it is also a supply-chain-centric standard.

With this in mind, let’s look at some of the ways organizations can use a supply chain security platform to comply with 800-171 and better protect their data and assets.

Mapping Eclypsium to SP 800-171 Controls_

Access Control

3.1.3 - Control the flow of CUI in accordance with approved authorizations

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

How Eclypsium Helps: Allows organizations to analyze their network devices and directly determine their integrity and security posture down to the level of hardware and firmware with the devices.

3.1.7 - Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.

Privileged functions include establishing system accounts, performing system integrity checks, conducting patching operations, or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.

How Eclypsium Helps: Eclypsium can scan devices for vulnerabilities or missing protections that can allow non-privileged users (or malicious code with user privileges) to make unauthorized changes to the device and/or the underlying firmware and boot process.

3.1.15 - Authorize remote execution of privileged commands and remote access to security-relevant information.

A privileged command is a human-initiated...command executed on a system involving the control, monitoring, or administration of the system including security functions and associated security-relevant information...Note that the ability to affect the integrity of the system is considered security-relevant as that could enable the means to by-pass security functions although not directly impacting the function itself.

How Eclypsium Helps: Eclypsium allows organizations to monitor the security of physical out-of-band management controllers such as baseboard management controllers (BMCs) in servers or the Intel Management Engine in laptops. Vulnerabilities in these critical elements can easily allow attackers to take full control of a device and bypass security functions.

Awareness and Training

3.2.2 - Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.

...organizations provide system developers, enterprise architects, security architects, acquisition/procurement officials, software developers, system developers, systems integrators, system/network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation, security assessors, and other personnel having access to system-level software, security-related technical training specifically tailored for their assigned duties...Such training can include policies, procedures, tools, and artifacts for the security roles defined. Organizations also provide the training necessary for individuals to carry out their responsibilities related to operations and supply chain security within the context of organizational information security programs.

How Eclypsium Helps: Simple automated scans allow a wide range of teams to assess the supply chain security of their assets without the need for technical knowledge or expertise related to supply chain or firmware security.

Configuration Management

3.4.1 - Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

How Eclypsium Helps: Eclypsium automatically creates highly detailed baselines of devices, internal components, and critical code, and can alert staff to any unexpected changes to these baselines.

3.4.2 - Establish and enforce security configuration settings for information technology products employed in organizational systems.

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture or functionality of the system. Information technology products for which security-related configuration settings can be defined include mainframe computers, servers, workstations, input and output devices (e.g., scanners, copiers, and printers), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), operating systems, middleware, and applications.

How Eclypsium Helps: Eclypsium performs a system-level analysis of each asset to ensure that all available protections are properly configured and working together as intended.

3.4.3 - Track, review, approve or disapprove, and log changes to organizational systems.

Configuration change control for organizational systems involves the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications. Configuration change control includes changes to baseline configurations for components and configuration items of systems, changes to configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers, and mobile devices), unscheduled and unauthorized changes, and changes to remediate vulnerabilities.

How Eclypsium Helps: Eclypsium automatically alerts staff to any unexpected changes to system baselines down to the level of the firmware of the devices. When vulnerabilities are found, Eclypsium can help organizations to prioritize updates based on real-world threat intelligence and can facilitate the update process based on the approval of staff. When potential threats are found, Eclypsium can help organizations to validate the alert by providing context and help them to remediate through updates.

3.4.8 - Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.

Whitelisting is the stronger of the two policies for restricting software program execution. In addition to whitelisting, organizations consider verifying the integrity of whitelisted software programs using, for example, cryptographic checksums, digital signatures, or hash functions.

How Eclypsium Helps: Eclypsium employs both denylisting and allowlisting of critical supply chain code within devices. Eclypsium has the industry's most complete library of firmware, system code, and supply chain software that is used to proactively verify the integrity of devices and their components.

Incident Response

3.6.1 - Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.

Incident-related information can be obtained from a variety of sources including audit monitoring, network monitoring, physical access monitoring, user and administrator reports, and reported supply chain events.

How Eclypsium Helps: Eclypsium can proactively scan devices to verify that they have not been altered below the level of the operating system such as being compromised by backdoors or bootkits. In the case of a supply chain event, IR teams can quickly identify all systems that contain a potentially affected component.

Maintenance

3.7.1 - Perform maintenance on organizational systems.

This requirement addresses the information security aspects of the system maintenance program and applies to all types of maintenance to any system component (including hardware, firmware, applications) conducted by any local or nonlocal entity.

3.7.2 - Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

Maintenance tools can include hardware, software, and firmware items, for example, hardware and software diagnostic test equipment and hardware and software packet sniffers.

How Eclypsium Helps: In both of these cases, Eclypsium provides automated tools for the ongoing assessment and maintenance of critical assets down to the level of the firmware and hardware. Traditional IT and security tools typically lack visibility and expertise at this level, leading to unseen risk or requiring large amounts of time-consuming technical work from staff.

Risk Assessment

3.11.1 - Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.

Such risk assessments consider threats, vulnerabilities, likelihood, and impact to organizational operations, organizational assets, and individuals based on the operation and use of organizational systems. Risk assessments also consider risk from external parties (e.g., service providers, contractors operating systems on behalf of the organization, individuals accessing organizational systems, outsourcing entities).

How Eclypsium Helps: Eclypsium provides device-level risk assessments and prioritizes vulnerabilities that are known to be exploited by threat actors in the wild. Eclypsium specializes in supply chain risks and threats specifically, allowing teams to assess risks based on assets and code from external supply chain partners.

3.11.2 - Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.

How Eclypsium Helps: Eclypsium specializes in the detection of supply chain vulnerabilities and other low-level vulnerabilities that are often missed by traditional scans. Proprietary drivers allow Eclypsium to scan deeper into devices to detect underlying vulnerabilities. Alternatively, device fingerprinting capabilities enable teams to identify vulnerable devices without the need for an authenticated scan.

3.11.3 - Remediate vulnerabilities in accordance with risk assessments.

How Eclypsium Helps: Eclypsium assists staff with prioritizing and applying updates, including identifying the latest vendor-approved code, validating the integrity of the patch/update code, and that all low-level settings are working properly after an update.

Security Assessment

3.12.3 - Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. Automation supports more frequent updates to hardware, software, firmware inventories, and other system information.

How Eclypsium Helps: Eclypsium provides ongoing insight into the integrity and posture of critical assets. Dashboards allow staff to quickly identify any changes to the device whether in terms of integrity changes, new vulnerabilities, configuration problems, or unusual behavior.

3.12.4 - Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

This reduces the documentation requirements associated with security programs and maintains security-related information in other established management/operational areas related to enterprise architecture, system development life cycle, systems engineering, and acquisition.

How Eclypsium Helps: The need to understand security across the system development lifecycle and acquisition process requires that organizations have a way to assess and audit their supply chain. Eclypsium lets teams easily audit these relationships. Additionally, Eclypsium allows teams to verify the integrity of networking assets that by nature, provide connectivity across boundaries, which are often targeted by attackers.

System and Communication Protection

3.13.3 - Separate user functionality from system management functionality.

System management functionality includes functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. ...separation includes web administrative interfaces that use separate authentication methods for users of any other system resources. Separation of system and user functionality may include isolating administrative interfaces on different domains and with additional access controls.

How Eclypsium Helps: Eclypsium audits the posture and integrity of system management components such as server BMCs and Intel Management Engine in laptops. The platform can ensure that these components are free of vulnerabilities that could allow an entity with user-level permissions to take control of these administrative components.

3.13.10 - Establish and manage cryptographic keys for cryptography employed in organizational systems.

How Eclypsium Helps: Eclypsium audits the internal components of a device that are responsible for the protection and administration of cryptographic keys (e.g. Trusted Platform Module).

System and Information Integrity

3.14.1 - Identify, report, and correct system flaws in a timely manner.

Organizations identify systems that are affected by announced software and firmware flaws including potential vulnerabilities resulting from those flaws and report this information to designated personnel...Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors including the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types of remediation.

How Eclypsium Helps: Eclypsium provides fully automated system-level assessments of critical assets down to firmware, hardware, and integrated supply chain code. Teams can quickly identify any flaws, and the Eclypsium platform facilitates the update process.

3.14.2 - Provide protection from malicious code at designated locations within organizational systems.

Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include logic bombs, back doors, and other types of cyber-attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended.

How Eclypsium Helps: Eclypsium specializes in the detection of low-level hardware, firmware, and software threats which are often able to evade traditional security controls. This includes supply chain backdoors, rootkits/bootkits, and other threats used for attacker evasion and persistence. The system uses a combination of known threat detection, proactive integrity checks of all supply chain code, as well as behavioral monitoring of code in order to detect highly advanced threats. Additionally, Eclypsium leverages OS-independent detection methods in order to detect low-level threats that may try to manipulate information that is passed up to the operating system.

3.14.3 - Monitor system security alerts and advisories and take action in response.

For example, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) generates security alerts and advisories to maintain situational awareness across the federal government and in non-federal organizations... Examples of response actions include notifying relevant external organizations, for example, external mission/business partners, supply chain partners, external service providers, and peer or supporting organizations.

How Eclypsium Helps: CISA, NSA, FBI, and other agencies have consistently provided detailed guidance on the protection of supply chain assets and the need to secure network devices, servers, and other computing infrastructure down to the level of the hardware, firmware, and underlying components. Eclypsium gives teams the tools they need to respond to these and future alerts and advisories. Along with our internal research, Eclypsium also monitors alerts from these and other agencies in order to prioritize specific vulnerabilities and techniques known to be used by threat actors.

3.14.5 - Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.

How Eclypsium Helps: Eclypsium regularly scans critical code to verify its integrity. This ensures that code has not been altered or tampered with either in the supply chain or after deployment. Eclypsium applies this same analysis to all update code, allowing staff to verify it is valid and authentic before it is deployed onto a device.

3.14.6 - Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

Unusual or unauthorized activities or conditions related to inbound/outbound communications traffic include internal traffic that indicates the presence of malicious code in systems or propagating among system components, the unauthorized exporting of information, or signaling to external systems. Evidence of malicious code is used to identify potentially compromised systems or system components.

How Eclypsium Helps: Eclypsium can perform behavioral analysis of underlying code and components including detection of unusual outbound communications. This can include the detection of communications from out-of-band management components that often have their own independent network stacks and hardware, which can be missed by a host operating system.
3.14.7 - Identify unauthorized use of organizational systems.
Unusual/unauthorized activities or conditions related to inbound and outbound communications traffic include internal traffic that indicates the presence of malicious code in systems or propagating among system components, the unauthorized exporting of information, or signaling to external systems. Evidence of malicious code is used to identify potentially compromised systems or system components.
How Eclypsium Helps: As in the prior case, attackers can often abuse internal system components to exfiltrate data or establish ongoing command and control of an attack. Eclypsium can audit these systems for vulnerabilities or threats to prevent unauthorized use.

CONCLUSIONS AND NEXT STEPS_

SP 800-171 clearly lays out the cybersecurity ground rules for organizations that do business with federal agencies or handle sensitive government information. However, it should also serve as an example even for organizations that are not contractually obligated to comply with the standard.

Ultimately, SP 800-171 is about setting clear expectations for how an organization's data should be protected by its partners and supply chain. All organizations have partners and supply chains, and likewise, all organizations have the equivalent of CUI in the form of intellectual property and trade secrets. While these partnerships have benefits, they also introduce risks. SP 800-171 provides a ready-made framework that can help address these risks.

It's no surprise that supply chain security controls are a major focus of SP 800-171. Organizations must be able to validate the integrity of their assets and infrastructure and proactively detect and remediate vulnerabilities that could lead to problems. This includes protecting key infrastructure such as networking gear, gateways, servers, and cloud infrastructure. And all assets must be protected down to the most fundamental levels including the hardware components, integrated firmware, boot processes, and other integrated supply chain software. Eclypsium turns these potentially complex tasks into simple, automated scans that allow staff to quickly identify potential problems and take corrective action. To learn more, contact the Eclypsium team at info@eclypsium.com.