SOLUTIONS_

SUPPORTING CROSS DOMAIN SOLUTIONS

U.S. Federal Agencies exchange sensitive information across boundaries to fulfill their mission objectives. Given the growing reliance on information exchange spanning multiple domains within operational contexts, cross domain solution (CDS) systems have emerged as vital elements of our national security framework. Warfighters need to have absolute confidence that the information that they receive has been transmitted securely and reliably.

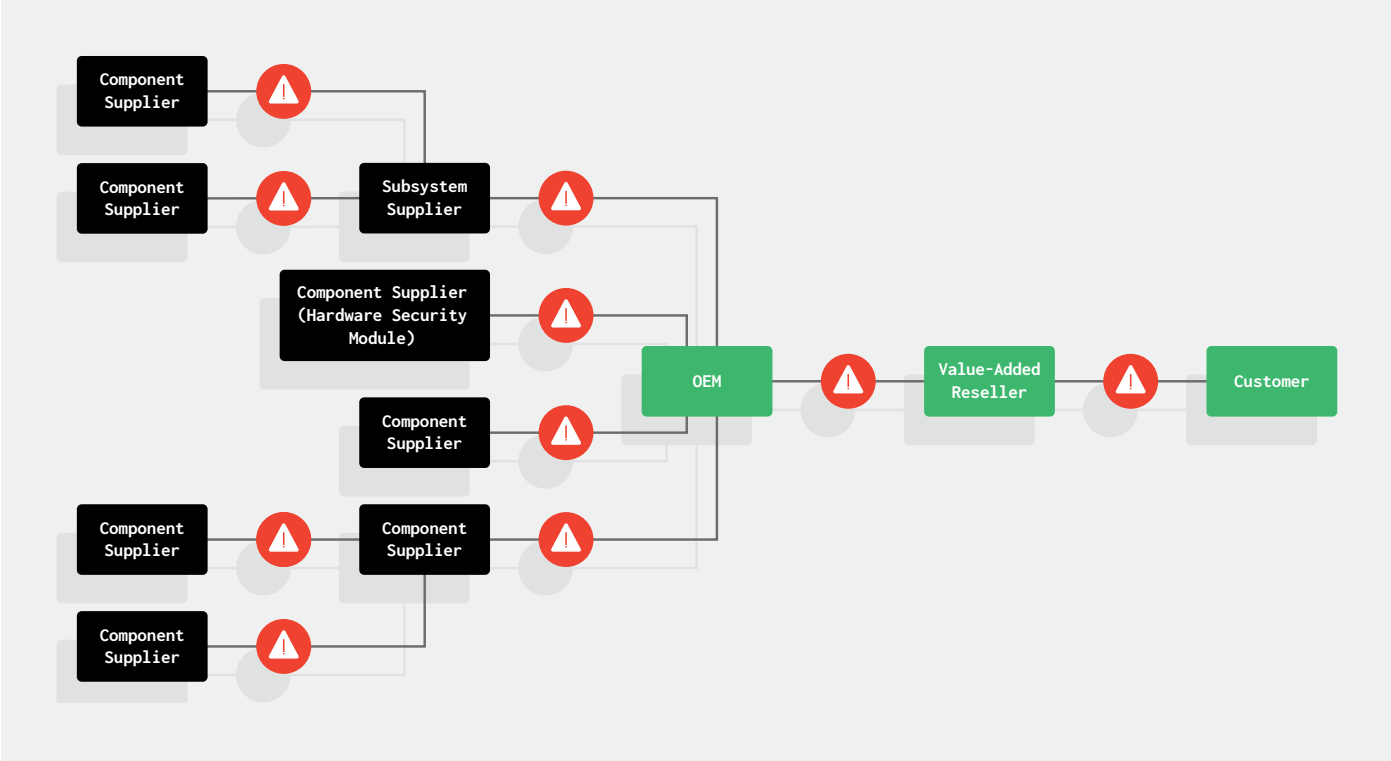
Recognizing the vulnerabilities inherent in systems handling classified data and the persistent threats posed by adversaries aiming to exploit cross-domain activities, the NSA established the National Cross Domain Strategy and Management Office (NCDSMO). The NCDSMO's main objective is to enhance the protection of vulnerable systems associated with cross-domain activities. In 2018, the NCDSMO released the Raise The Bar (RTB) initiative, the first set of security standards and requirements aimed at mitigating the risk of CDS systems experiencing failure, even in the face of persistent attacks. The RTB was created to enhance the security and functionality of cross-domain solutions over the entire duration of its existence, including design, development, assessment, implementation, and utilization. In 2022, the White House issued NSM-8, which establishes the NCDSMO as the authority overseeing CDS, including mandates for the controls on CDS systems.

THE CHALLENGE_

The stock hardware powering CDS devices is composed of dozens of underlying components that are essential to the function of the device. These systems and their components all depend on millions of lines of software code ("firmware") developed by a myriad of equipment manufacturers that not only govern how each component functions, but also pose a risk to the system's integrity and the security of its data when compromised. Threats at the firmware level can provide an attacker with complete control over a system, while easily avoiding higher-level security tools that run at the operating system level. To compound the supply chain risk, CDS vendors introduce an extra layer of complexity by customizing the hardware to align with their specific requirements. Throughout its lifespan, the CDS appliance remains vulnerable to a myriad of supply chain and firmware attacks.

In order to mitigate risk from the infrastructure supply chain, a CDS needs to do the following:

- Identify and provide firmware patches for the CDS solutions
- Verify that all hardware and firmware resources are patched to components such as CPU microcode, UEFI/BIOS, baseboard management controller (BMC), etc.
- Provide a mechanism to assess the current state of the CDS while in operation. This includes the ability to update the CDS periodically.
- Utilize a commercially supported hardware and firmware scanning tool



The supply chain for CDS solutions is complex and difficult to secure.

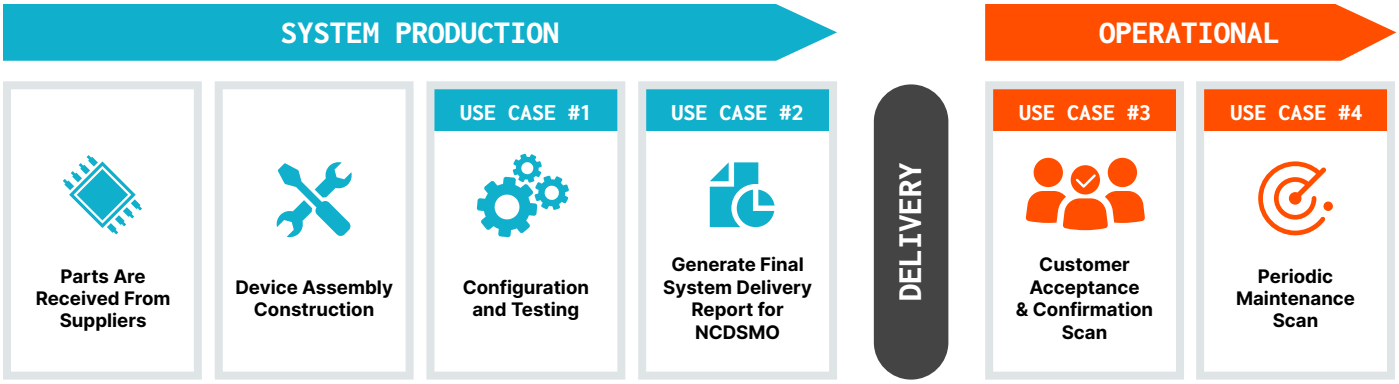
THE SOLUTION_

Eclypsium provides a simple, automated way to verify the integrity and posture of CDS systems during System Production and through operation. Built on decades of firmware vulnerability research, the Eclypsium Platform delivers enterprise-grade assurance for firmware and hardware. A basic scan verifies that the current state of assets and all of its components are authentic and have not been tampered with either in the field or in the supply chain. The scan will also validate that the equipment is using the latest supported version of the firmware and is free from vulnerabilities. The technology identifies the presence of known threats and monitors the behavior of the firmware and other critical code to detect the presence of unknown threats. These tests require no firmware expertise, pose no risk to the systems themselves, and can be performed fully offline.

Out of the box, Eclypsium can verify the following components:

- UEFI and BIOS
- Processor and Chipset
- Baseboard Management Controller
- Trusted Platform Module
- Intel Management Engine
- Network Interface Controllers
- MBR/Bootloader
- Storage

Eclypsium can be leveraged across four distinct use cases throughout the CDS lifecycle, with the initial two occurring during the System Production phase. At this stage, CDS vendors can conduct scans on the CDS appliance as it undergoes configuration and assembly, ensuring the incorporation of the latest firmware versions. Once the appliance is completed, a baseline scan can be set, generating a final artifact of record to validate the absence of vulnerabilities in the newly created CDS appliance and the application of the latest firmware version. This baseline scan serves as a benchmark during the customer's acceptance of the CDS, documenting compliance with the ordered specifications. Subsequently, the same baseline scan can be employed in scheduled scans throughout the lifespan of the CDS to verify that no changes have occurred.



Eclypsium offers unique support in satisfying the requirements of the RTB, particularly during the crucial System Production phase. By facilitating scans during the configuration and assembly process, Eclypsium validates the integrity of the device prior to delivery and acceptance by the customer.

ABOUT ECLYPSIUM_

Eclypsium is an established leader in supply chain and firmware security and is a contributor to the National Cybersecurity Center of Excellence (NCCoE) and SP 1800-34B, Validating the Integrity of Computing Devices. Eclypsium's cloud-based or offline platform provides digital supply chain security for critical hardware, firmware and software. Eclypsium defends enterprises and government agencies from the deep implants and exploits that have become the vector of choice for modern adversaries. For more information, visit eclypsium.com.