eclypsium /FEDERAL

TECHNICAL BLUEPRINT_

HARDWARE SECURITY FOR AI INFRASTRUCTURE

Executive Summary_

This document details the necessary effort to implement the Eclypsium Hardware Supply Chain Security Platform to address critical hardware supply chain vulnerabilities, infrastructure integrity, and component-level security gaps within Department of War (DoW) information systems and high-performance computing AI environments.

Eclypsium is pleased to propose the Eclypsium Hardware Supply Chain Security Platform to provide proactive hardware supply chain security for critical AI hardware, firmware, and software infrastructure. The platform's key architectural features include:

- **Key Feature One:** Complete component-level visibility and automated generation of Software, Firmware, and Hardware Bills of Materials (SBOM/FBOM/HBOM) to maintain an uncompromised, verifiable inventory of device components, including GPUs, specialized AI accelerators, and high-performance networking devices. This directly fulfills Presidential and DoW mandates for absolute supply chain transparency before hardware is cleared for active deployment in sensitive AI environments.
- **Key Feature Two:** Agentless discovery and analysis combined with a powerful REST API for flexible integration with existing SIEM, SOAR, and ITSM tools without causing operational disruption. This allows rapid security verification without altering critical mission code bases, consuming costly GPU cycles, or disrupting long running, resource intensive AI model training runs.
- **Key Feature Three:** Firmware monitoring capable of discovering hidden rootkits, bootkits, and backdoors that evade traditional security tools. The platform validates cryptographic integrity against a database of 15 million and growing known good firmware images, intercepting adversarial tampering directly at the hardware layer before threat actors can exfiltrate proprietary models, manipulate training data, or silently hijack compute resources.

Mandates & Policies Specific to AI Infrastructure

AI data center hubs, specialized clusters, and high-performance computing "AI factories" have been designated as national-level strategic assets and critical infrastructure. Due to high data volumes and the continuous leasing or swapping of raw compute nodes between different classified and unclassified customer workloads, these environments face severe threats from data poisoning, model weight leaks, and hardware-level exploitation. Eclypsium delivers the low-level visibility needed to defend these networks while satisfying current DoW AI mandates:

- **White House Executive Order (Advanced AI Innovation and Security)**
  The June 2, 2026 EO explicitly directs the DoW, the NSA, and CISA to prioritize the cyber defense of National Security Systems hosting advanced AI. It also establishes a framework for evaluating "covered frontier models" via a classified benchmarking process, requiring early secure access for trusted federal partners. Eclypsium hardens the physical infrastructure hosting these evaluations, ensuring that the underlying servers, GPUs, and network switches are free from low-level vulnerabilities

- **National Security Presidential Memorandum 11 (NSPM-11)**
  Signed on June 5, 2026, NSPM-11 orders the national security enterprise to accelerate secure AI adoption while embedding strict assurance and accountability infrastructure. A primary directive of NSPM-11 is ensuring that no commercial entity or foreign adversary can unauthorizedly disable, degrade, or modify a fielded system that warfighters depend on. Eclypsium provides the independent hardware-level verification needed to guarantee that underlying systems cannot be covertly altered or disabled via firmware manipulation.

- **FY 2026 NDAA (Section 1513) Compliance**
  Congress has mandated a strict security procurement framework for all acquired AI/ML technologies, focusing specifically on mitigating supply chain vulnerabilities, counterfeit parts, data poisoning, and adversarial tampering. The law targets, including source code, software, and the underlying hardware/firmware methods used to develop or host AI. Eclypsium satisfies this mandate by continuously scanning and cryptographically verifying the foundational layers of the compute nodes running those models.

- **NIST SP 800-223 Standards**
  Eclypsium fulfills the specialized High-Performance Computing (HPC) guidelines detailed in NIST SP 800-223, specifically providing automated mechanisms to solve Compute Node Sanitization challenges between task runs on shared infrastructure.

Core Technical Capabilities for AI Infrastructure Security

The key technical pillars built into the Eclypsium architecture are tailored specifically for high-capacity AI environments:

AI Server & GPU Risk Analysis

- **Advanced Accelerator Mapping:** Discovers, inventories, and maps critical components deep within AI clusters, offering native support for advanced infrastructure such as NVIDIA GPUs.
- **Multi-Tenant Validation:** Continuously monitors the physical and cryptographic integrity of GPUs before and after they are leased or allocated to different missions, teams, or external defense contractors, preventing cross-tenant data contamination or persistent firmware modifications.

- **Automated Risk Reporting:** Generates comprehensive risk profiles detailing hardware vulnerabilities, outdated firmware, and component risks for individual accelerators or scaled across data center fleets.

AI Infrastructure Integrity & Supply Chain Security

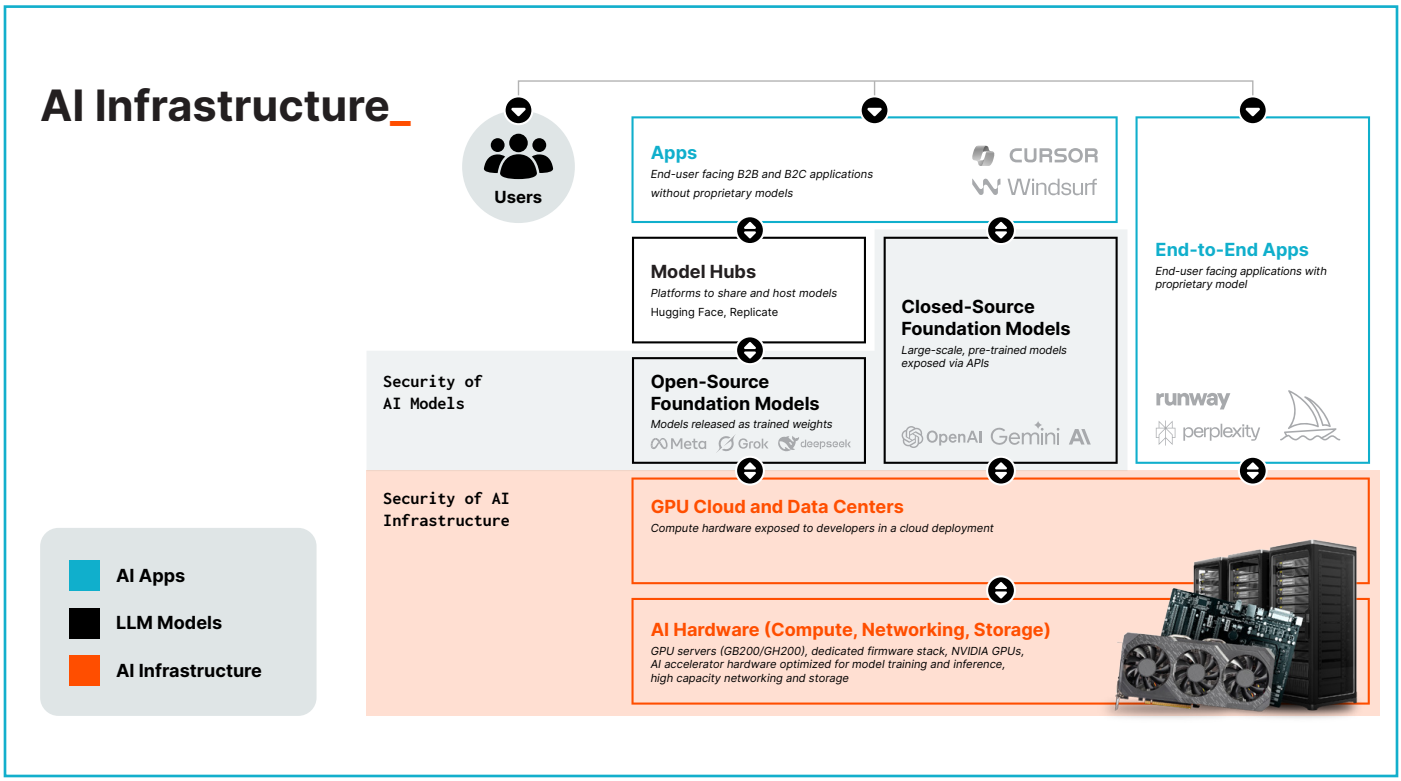
- **Firmware Verification:** Scans and verifies production GPUs, accelerators, and underlying silicon to guarantee that only authorized, "known-good" configurations are executing in the environment.
- **Anti-Drift Monitoring:** Instantly alerts security operations centers the moment an unauthorized modification, unexpected configuration drift, or unauthorized patch distribution is detected.
- **Automated xBOM Generation:** Continuously generates and updates SBOMs, FBOMs, and HBOMs for AI infrastructure assets to fulfill NDAA Section 1513 supply chain provenance requirements.

Deep Vulnerability Management & Threat Detection

- **Component-Level Vulnerability Finding:** Uncovers deep seated structural vulnerabilities that traditional network or operating system-level scanners overlook, including outdated firmware and vulnerable GPU drivers.
- **Low-Level Threat Interception:** Proactively catches backdoors, malicious hardware manipulation, and stealthy implants attempting to bypass EDR barriers to subvert high-performance compute nodes.

Broad Lifecycle & Ecosystem Support

- **Technology Agnostic:** Delivers uniform security coverage across an array of technology stacks, from x86 and ARM server architectures to firewalls, core switches, and data center networking routers.
- **Full Lifecycle Protection:** Can be deployed fluidly at any infrastructure phase: before installing the gear, between heavy AI model training runs, or during final asset disposition.



info@eclypsium.com
eclypsium.com

Objectives & Key Problems Solved

The Eclypsium platform serves as an enterprise-grade Hardware Supply Chain Security solution engineered to anchor the physical trust layer of critical AI infrastructure. By securing the underlying hardware, microcode, and firmware, Eclypsium directly protects the integrity of advanced machine learning models and heavy compute resources. This operational implementation explicitly addresses the following strategic objectives and operational gaps within the defense enterprise:

- **Benefit 1 (Hardware-Enforced Model Integrity and Supply Chain Provenance):** Eradicates operational blind spots at the hardware layer to prevent data loss, unauthorized access, and low-level tampering targeting proprietary AI model weights, hyper-parameters, and sensitive training datasets. Because traditional security tools cannot see down to the GPU or baseboard management controller (BMC) firmware, adversaries can persist in these components, leveraging them to silently exfiltrate models or poison data directly in memory. Eclypsium stops this by cryptographically verifying the infrastructure, ensuring the physical hardware and component firmware has not been manipulated to leak sensitive information or alter model behavior. This guarantees continuous compliance with federal supply chain risk management standards, specifically enforcing the strict hardware/software provenance and anti-tampering directives mandated under the June 2026 White House Executive Order on AI, NIST SP 800-53, NIST SP 800-223, and the FY 2026 NDAA (Section 1513).
- **Benefit 2 (Optimized Multi-Tenant Compute & Accelerated AI Deployment Timelines):** Eliminates manual vendor compliance tracking by providing automated, continuous scanning and vulnerability analysis of complex AI hardware clusters, including GPUs, TPUs, and high-performance interconnects without requiring specialized firmware engineers. This shortens implementation timelines, enabling cyber defense and data science teams to rapidly validate high-performance compute infrastructure. This accelerates safe multi-tenant compute environments, allowing infrastructure to be quickly cleared, sanitized, and redeployed for different classified workloads without introducing cross-contamination risks.

Vendor Qualifications

Eclypsium has a proven track record of providing Hardware Supply Chain Security solutions to various U.S. Government agencies and organizations, addressing critical needs related to operational continuity, risk reduction, and compliance with stringent cybersecurity mandates. As an established market leader included on CISA's Continuous Diagnostics and Mitigation Approved Products List, Eclypsium serves as a trusted partner across global defense networks, intelligence agencies, and major federal cloud providers to protect critical infrastructure and high-performance AI compute clusters. The platform delivers targeted security for modern AI factories by continuously inventorying, managing, and scanning AI infrastructure and NVIDIA GPU hardware down to the component level. By delivering low-level visibility and automated vulnerability analysis below the operating system layer, the Eclypsium platform hardens defense networks and data science pipelines against advanced persistent threats, proactively identifying outdated firmware, unpatched GPU drivers, and hardware-level risks that traditional scanners miss. Backed by an extensive and growing database of over 15 million cryptographic firmware hashes, Eclypsium provides the real-time threat intelligence needed to counter sophisticated state-sponsored supply chain exploits. This ensures foundational hardware remains resilient against unauthorized modifications, adversarial tampering, or low-level exploits targeting proprietary AI models.

Procurement Guidance

The Eclypsium Hardware Supply Chain Security Platform is widely accessible through Carahsoft and our authorized reseller network and their multiple Government-wide Acquisition Contracts (GWACs), including GSA Multiple Award Schedule (MAS), NASA SEWP V, and ITES-SW2 vehicles. Additionally, Eclypsium is on the CISA CDM APL.

There is established precedent for a brand name procurement of Eclypsium by U.S Government agencies. While other commercial products offer limited hardware security, none possess the comprehensive hardware security capabilities required to secure high-performance AI infrastructure and fulfill specific mission requirements.

Summary_

Eclypsium appreciates the opportunity to offer this modernized AI Infrastructure security capability blueprint. We are entirely confident that the Eclypsium Hardware Supply Chain Security Platform will allow the U.S Government to achieve unprecedented speed, cryptographic validation, and process optimization across its ongoing operations while answering the nation's call to secure critical AI infrastructure.

Eclypsium provides the essential technical ecosystem required to fulfill this operational requirement: a unified, supply chain security platform that automatically scans, maps, and analyzes firmware binaries across servers, endpoints, networking assets, and AI accelerators, such as GPUs.

By continuously inspecting hardware against its proprietary vulnerability database, the platform detects configuration drift, flags malicious implants, and automatically manages firmware patches directly through a centralized console. These capabilities allow the DoW to sanitize compute nodes and continuously audit its high-value AI hardware assets throughout their active operational lifecycles.

How to Buy Eclypsium_

Federal Agencies

Eclypsium is available through Federal VARs and Carahsoft on the following contracts:

GSA Multiple Award Schedule (MAS) and SCRIPTS BPA

GSA Schedule | NASA SEWP V | ITES-SW2

Eclypsium is also on the CDM APL.

State and Local Governments
Carahsoft for Eclypsium SLED Contracts

Canadian Federal Government
Carahsoft Canadian Cyber Security Procurement Vehicle

Vendor Information
Eclypsium, Inc.
Address: 919 SW Taylor Street | Portland, OR 07205
DUNS/CAGE: 081023218| 8GXX1