Enhancing NERC CIP Compliance with the Eclypsium Platforms_

The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards are essential for safeguarding the Bulk Electric System (BES) against cyber threats. These mandatory requirements ensure the reliability and security of North America's electric grid by addressing key areas such as electronic access controls, system security management, configuration change management, vulnerability assessments, and supply chain risks. As cyber threats evolve, particularly those targeting firmware and hardware components, utilities face increasing challenges in maintaining compliance.

The Eclypsium platform, a leading solution for firmware and supply chain security, provides automated tools to detect, assess, and mitigate vulnerabilities at the hardware and firmware levels. This white paper explores how Eclypsium supports compliance with CIP-005 (Electronic Security Perimeter), CIP-007 (Systems Security Management), CIP-010 (Configuration Change Management and Vulnerability Assessments), and CIP-013 (Supply Chain Risk Management). By offering deep visibility, vulnerability remediation, and continuous monitoring, Eclypsium helps utilities reduce risks, streamline audits, and enhance overall grid resilience.

Summary of Key NERC CIP Controls Supported by Eclypsium

CIP-005	focuses on controlling electronic access to BES Cyber Systems through defined perimeters.
CIP-007	emphasizes technical and procedural measures for system security, including patch management and malware prevention.
CIP-010	addresses configuration change management and vulnerability assessments to prevent unauthorized changes to BES Cyber Systems.
CIP-013	focuses on cybersecurity risks in the supply chain for BES Cyber Systems, requiring entities to implement risk management plans.

Firmware and hardware vulnerabilities represent a growing blind spot in traditional security approaches, as they operate below the operating system and can evade endpoint detection tools. Eclypsium's platform scans hardware, firmware, and software components, providing inventory, vulnerability management, and threat detection. With features like automated integrity verification and zero-trust principles, Eclypsium aligns with NIST SP 800-53 controls, which underpin many CIP requirements. This integration enables utilities to meet CIP obligations while addressing sophisticated threats like supply chain compromises.

CIP-005: Strengthening Electronic Security Perimeters

CIP-005 requires entities to establish Electronic Security Perimeters (ESPs) to manage and monitor electronic access to high- and medium-impact BES Cyber Systems, preventing unauthorized entry that could lead to grid disruptions. Traditional security often overlooks firmware-level threats, such as rootkits or bootkits, which can bypass perimeter controls.

Eclypsium enhances CIP-005 compliance by providing continuous monitoring and protection of devices at the component level. The platform detects implants and backdoors in firmware that could compromise the ESP, ensuring no blind trust in vendors or manufacturers. For instance, Eclypsium verifies endpoints down to the device level, identifying outdated or vulnerable firmware that might allow unauthorized access. This visibility extends to processors, network interfaces, and UEFI firmware, filling gaps in traditional endpoint detection and response (EDR) tools.

In practice, Eclypsium's automated scans reveal firmware weaknesses, enabling utilities to harden perimeters by remediating vulnerabilities before they are exploited. By enriching SIEM systems with component-level data, Eclypsium supports real-time monitoring of access points, aligning with CIP-005's requirements for interactive remote access management.

CIP-007: Advancing Systems Security Management

CIP-007 mandates robust security management practices, including ports and services management, security patch application, malicious code prevention, and system access controls. Firmware and hardware components are critical here, as unpatched vulnerabilities can enable persistent threats that traditional patching overlooks.

Eclypsium supports CIP-007 by offering vulnerability management and threat detection at the hardware and firmware layers. The platform identifies and remediates insecure configurations, outdated firmware, and known vulnerabilities, hardening the environment against compromises. It integrates with existing ITSM and SIEM systems, providing component-level insights to automate patch prioritization and deployment.

For malicious code prevention, Eclypsium detects advanced threats like rootkits and implants that evade antivirus solutions, ensuring compliance with CIP-007's anti-malware requirements. Automatic firmware updates and integrity checks further align with patch management obligations, reducing manual effort. Eclypsium's research-driven database enables proactive vulnerability scanning across diverse vendors. This comprehensive approach not only meets CIP-007 but also prepares utilities for audits by documenting security controls.

CIP-010: Enabling Configuration Change Management and Vulnerability Assessments

CIP-010 requires entities to implement processes for baseline configurations, authorize changes, monitor for unauthorized modifications, and conduct regular vulnerability assessments for high- and medium-impact BES Cyber Systems. This includes verifying the identity and integrity of software sources prior to changes, particularly for operating systems, applications, and ports.

Eclypsium addresses CIP-010 through its Integrity Baselining functionality, which allows setting per-device baselines to monitor for configuration drift. It also enables applying baseline templates to groups of assets to monitor for asset drift and alert to configuration changes at scale. The platform maintains an up-to-date library of valid firmware and software, performing cryptographic checks to detect tampering or alterations.

For change management, Eclypsium's features ensure baselines are updated and deviations are documented, while integrating with SIEM tools for real-time alerts on unauthorized modifications. This aligns with CIP-010's requirements for testing changes in controlled environments and conducting assessments every 15-36 months. By automating these processes, Eclypsium reduces compliance burdens and enhances protection against misconfigurations that could lead to BES instability.

CIP-013: Mitigating Supply Chain Risks

CIP-013 requires entities to develop and implement supply chain cybersecurity risk management plans, focusing on vendor notifications, risk assessments, and verification of firmware integrity. Supply chain attacks, like SolarWinds, highlight the need for verifying component authenticity in BES Cyber Systems.

Eclypsium excels in CIP-013 compliance through its supply chain security features, including continuous monitoring of production assets and a searchable inventory of components. The platform inspects hardware and vendor-supplied firmware, as well as the underlying OS of network devices, addressing risks from third-party compromises. It performs cryptographic checks to verify software and firmware authenticity, meeting requirements like those in related CIP-010 for baseline configurations.

By applying zero-trust principles to devices, Eclypsium eliminates blind trust in suppliers, scanning for vulnerabilities and tampering across the supply chain. Features like GenAI assessments for hardware and models further enhance risk management for emerging technologies. Utilities can generate compliance reports, demonstrating adherence to CIP-013's periodic reviews and vendor coordination.

Conclusion_

The Eclypsium platform fulfills key requirements of NERC CIP that other tools can't, closing security gaps and rounding out existing NERC CIP programs for overall improved security posture. By addressing firmware and supply chain vulnerabilities, Eclypsium directly supports CIP-005's perimeter protections, CIP-007's security management, CIP-010's change and assessment processes, and CIP-013's risk mitigation. In an era where exploitation of edge network devices has grown 8x since 2024, according to the Verizon 2025 Data Breach Investigations Report, Eclypsium provides essential visibility and automation.

Utilities adopting Eclypsium can achieve cost savings, reduced audit burdens, and enhanced grid reliability. As threats continue to target critical infrastructure, integrating such platforms is not just compliant—it's imperative for national security.