

Zineb Crowe

CYSE 368 CRN 25090

Date: 01/28/2026

ODU Spring 2026

NNWC Department / AERMOR LLC

Professor name: Teresa Duvall

TA name: Joshua Russell

Reflective Paper 1

My first 50 hours as Cloud Engineer for Endpoint Transport in the NNWC department at AERMOR LLC delivered hands-on experience supporting the U.S. Navy's migration from NMCI (Navy Marine Corps Intranet) machines to Nautilus endpoints. This PEO Digital initiative maintains operational readiness for Nautilus Virtual Desktops (NVD) and Endpoints (NEP), impacting thousands of users. The DoD security classifications prevent me from sharing particular project information, but my duties focus on endpoint configuration, routing diagnostics via Microsoft Intune and Azure VPN, FlankSpeed Microsoft 365, and BMC Helix ticketing, directly applying my ODU coursework in cybersecurity policy, network security, and Linux administration to real Navy IT challenges.

The NMCI-to-Nautilus shift upgrades outdated hardware to cloud-based platforms with zero-trust security, scalable infrastructure, and remote access. Unlike NMCI's rigid structure, Nautilus integrates FlankSpeed's Microsoft 365 for superior endpoint control and secure .mil/.gov websites access, enabling vital military operations.

My role emphasizes four core areas: enforcing configuration updates and security

policies; resolving routing issues in hybrid environments; co-authoring incident reports with security recommendations; and creating user knowledge articles. All align with NNWC's mission to minimize disruptions while meeting DoD standards.

Intune administrator access is critical for routing table management, as users frequently lose .mil/.gov connectivity post-transition due to Nautilus's distinct gateways versus NMCI's legacy paths. My process is reviewing tables to trace traffic, confirming if destinations fall outside our environment, then coordinating with the site's networking POC for gateway fixes. BMC Helix documents actions for audits, while Global Reader aids Tier IV escalations, safeguarding operations without power interruptions. These tasks mirror ODU training: Troubleshooting subnets, IPsec, and protocols draw from networking/Linux labs (e.g., scripting traffic simulations); Intune policies echo zero-trust/STIG concepts from policy classes; and knowledge articles support technical writing for ethical cybersecurity, bridging theory to practice.

The high number of military and government-related tickets requires immediate security-based assessment which restricts the ability to monitor the process and needs exact transfer of contact information between teams. The process of achieving fast results while following rules has proven to be extremely challenging because of the hybrid NMCI-Nautilus system which I must handle while working full-time and studying as a single mother. The implementation of batch resolution through specific modifications has proven that enterprise diagnostic systems can be trusted.

In conclusion, the first 50 hours I spent in the NNWC department brought me a life-changing experience which proved that ODU delivers challenging academic work that leads to meaningful Navy modernization projects. The combination of routing disruptions has developed my ability to be resilient while my cloud security technical abilities have been proven through my achievements. The position has shown me which path to follow for achieving DoD infrastructure leadership positions and advanced certifications while demonstrating that practical experience improves national service cybersecurity education for national service.