CELINE TANNOUS

CYBER SYSTEMS ENGINEER | ACTIVE TS/SCI

San Diego, CA | 720-318-3311 | linkedin.com/in/celine-tannous-34a44a1a7 | github.com/ObsidianNull | celinetannous.com

CLEARANCE & CERTIFICATIONS

Active TS/SCI | CompTIA Security+ | PenTest+ - In Progress | CySA+ - In Progress | Available Early 2027

PROFESSIONAL SUMMARY

Active TS/SCI-cleared U.S. Navy Lieutenant and cybersecurity professional with a B.S. in Cyber Operations and direct experience securing mission-critical DoD systems across Windows, Linux, virtualized, network, application, and standalone environments. Led ACAS vulnerability analysis, STIG control assessment, POA&M remediation, ATO sustainment, configuration governance, enterprise infrastructure support, and cybersecurity inspection readiness. Also qualified and currently stand watch as an A4W Propulsion Plant Watch Officer, combining cyber systems experience with high-reliability engineering leadership, technical decision-making, and casualty-response execution.

TECHNICAL SKILLS

Cyber Systems Engineering	Security Baselines; Security Control Assessment; Security Architecture Support; Technical Analysis; Configuration Governance; Root Cause Analysis
DoD Cyber / RMF	NIST/RMF-Aligned Processes; ATO Sustainment; POA&M Management; Risk Acceptance Documentation; Inspection Readiness; Continuous Monitoring
Assessment / Hardening	ACAS; STIG Checklists; CAT I/II/III Findings; HBSS Oversight; Vulnerability Remediation; Remediation Validation
Systems / Infrastructure	Windows; Linux; Active Directory; VMware; Virtualized Systems; CANES; Network Devices; Applications; Standalone Systems
Security Tools / Code	Wazuh; Atomic Red Team; MITRE ATT&CK; Wireshark; Nmap; Burp Suite; Metasploit; Git; Python; C; C++; Java; JavaScript

PROFESSIONAL EXPERIENCE

UNITED STATES NAVY | 2021-PRESENT

Assistant Reactor Electrical Assistant (A-REA) - USS CARL VINSON (CVN-70) – May 2026 to Present

- Support reactor electrical maintenance planning, engineering readiness, technical review, and department-level coordination for A4W nuclear propulsion electrical systems.
- Review maintenance work packages, tag-outs, testing requirements, equipment status, and corrective actions before execution in a high-reliability environment.
- Coordinate ship's-force and contractor maintenance priorities during Planned Incremental Availability while tracking equipment readiness and emergent work.
- Brief senior engineering leadership on system status, maintenance risk, troubleshooting progress, and corrective-action execution.

Reactor Electrical Division Officer - USS CARL VINSON (CVN-70) – Aug 2024 to May 2026

- Led a 20-person technical division responsible for operation, maintenance, troubleshooting, and readiness of nuclear propulsion electrical systems.
- Managed preventive and corrective maintenance, personnel qualifications, technical training, work controls, and divisional readiness across deployed and in-port operations.
- Directed fault isolation, casualty response, and restoration efforts for electrical distribution and supporting equipment under time-critical conditions.
- Coordinated engineering work across operations, maintenance, quality assurance, and senior reactor department leadership while balancing mission requirements and equipment risk.
- Prepared personnel, programs, and equipment for Operational Reactor Safeguards Examination and other formal engineering assessments.

A4W Propulsion Plant Watch Officer (PPWO) - USS CARL VINSON (CVN-70) – Aug 2024 to Present

- Qualified and currently stand watch as an A4W Propulsion Plant Watch Officer with delegated authority for safe propulsion plant operation.
- Supervise engineering watch teams, direct reactor and propulsion plant evolutions, evaluate plant conditions, and coordinate casualty response during deployed and in-port operations.
- Integrate operational requirements, maintenance status, procedural compliance, and engineering risk to make time-sensitive watchstanding decisions.
- Served as one of eight ORSE-qualified Propulsion Plant Watch Officers during deployment in support of Operation Rough Rider.

Cyber Officer / Automated Data Processing Officer - USS HARPERS FERRY (LSD-49) – Oct 2021 to Apr 2023

- Oversaw STIG compliance across Windows and Linux workstations, Windows servers, virtualized systems, network devices, applications, and standalone systems; reviewed CAT I/II/III findings and manually validated controls through STIG checklists, Group Policy, registry settings, services, and implementation evidence.
- Managed ACAS vulnerability remediation by prioritizing critical and high findings, reviewing affected hosts, CVEs, and recommended patches, directing corrective action, and personally verifying closure through scan and rescan results.
- Created and maintained POA&Ms documenting severity, affected systems, remediation plans, completion dates, and status; identified stalled or approaching-due findings and drove technical personnel toward closure.

- Managed STIG exceptions by documenting operational constraints and risk acceptance for Commanding Officer concurrence, coordinating required exceptions with TYCOM N6, and tracking temporary deficiencies through POA&Ms.
- Co-led quarterly Configuration Change Boards for the CO, XO, and CSO, briefing proposed cybersecurity configuration changes, affected systems, patching and availability constraints, and recommendations to improve cyber posture.
- Reviewed ATO authorization artifacts and routed documentation to TYCOM N6; supported recurring authorization renewals and continuous package maintenance as systems and configurations changed.
- Prepared for and facilitated Basic Phase Cyber Certification, continuing certification events, INSURV cyber assessments, COMSEC inspections, and a Fleet Cyber evaluation; coordinated inspectors and technical personnel and directed corrective actions through closure.
- Directed a 14-person IT team supporting cybersecurity readiness and enterprise services for approximately 300 permanent users and up to 600 users during embarked operations; served as the Commanding Officer's designated cybersecurity representative and Top Secret Control Officer.
- Supported CANES Version 3 infrastructure with approximately 60 VMware virtual servers and 100 workstations across NIPRNet and SIPRNet environments, Active Directory, network devices, firewalls, TACLANE, and SATCOM systems.
- Recovered enterprise services following CANES backbone failures by restoring VMware snapshots, rebuilding virtual machines, coordinating external maintenance support, and validating restored functionality.
- Developed a ship-wide bandwidth management strategy that balanced mission requirements, command priorities, and constrained satellite communications capacity.
- Supported a command cyber program that passed all inspections, performed above average during INSURV cyber assessment, received positive COMNAVSURFPAC N6 feedback, and became the first ship to pass a limited Fleet Cyber evaluation.

CYBER SYSTEMS ENGINEERING PROJECTS

Detection Engineering Lab

- Engineered a virtualized enterprise lab using VMware with Active Directory, Windows endpoints, Sysmon telemetry, and Linux-based Wazuh SIEM infrastructure.
- Created and validated custom Wazuh detection rules against Atomic Red Team simulations mapped to MITRE ATT&CK techniques, including PowerShell abuse, persistence, and lateral movement.
- Analyzed process trees, parent-child relationships, command lines, process identifiers, and Sysmon events to distinguish adversary behavior, telemetry, and detection logic.
- Diagnosed DNS, VM networking, domain-join, service, and agent-enrollment failures to restore end-to-end detection-pipeline functionality.

EARLIER TECHNICAL EXPERIENCE

GENERAL ELECTRIC AVIATION - Cyber Security Intern

- Performed indicator-of-compromise research to support identification of malicious activity and emerging threats.
- Analyzed emails for indications of phishing, malware, or compromise and escalated confirmed threats.
- Gained exposure to incident response, digital forensics, malware analysis, and secure development workflows in an enterprise environment.

JOHNS HOPKINS UNIVERSITY APPLIED PHYSICS LABORATORY (JHUAPL) - Software Engineering Intern

- Developed JavaScript functionality and integrated the Google Maps API for software supporting critical-infrastructure and national-security analysis.
- Created Python automation to support technical research and data-processing workflows.
- Produced technical documentation and collaborated in a mission-focused engineering research environment.

EDUCATION

UNITED STATES NAVAL ACADEMY - Annapolis, MD

B.S., Cyber Operations (Honors Program), 2021 | Graduated with Merit | CAE-CO Designated Program