ANDREW S. GALLEGOS

Westbrook, CT | 203-312-3511 | AndySGallegos@gmail.com | T**op Secret (TS) Clearance**

PROFESSIONAL SUMMARY

Core Competencies

- **Communication and Collaboration Tools:** Teams (chat and VOIP, policy and administration), Exchange Hybrid, On-premises, and Online, Mimecast (policy and administration).
- **Email Security:** Hardening DMARC policies via DKIM and SPF alignment to prevent domain spoofing and phishing.
- **Communication Platforms:** SharePoint, OneDrive, Egnyte, Jira.
- **Tenant Migration:** Executed and coordinated multiple Microsoft 365, Active Directory, Exchange Online, On-Premises, and Hybrid environments.
- **Automation & Scripting:** Advanced PowerShell (compliance checks, account auditing, task automation, daily checks, server monitoring).
- **Identity & Access Management:** Microsoft Entra ID (Azure AD), Active Directory OAuth Scopes, RBAC, MFA Enforcement, Conditional Access, User Lifecycle Management, Auditing, and Automation.
- **Governance, Risk & Compliance (GRC):** NIST 800-53, RMF, DISA STIGs, POA&M Management.
- **Infrastructure & Virtualization:** Windows Server (2016-2022), VMware, Hybrid Cloud Deployments, Patch Management (SCCM/Tanium, Intune, JAMF).
- **Security Tools:** Tenable/Nessus (ACAS), Splunk, Sophos and Trellix EDR.
- **ITSM:** Ticketing, change management requests, documentation, SOP and KB.

PROFESSIONAL EXPERIENCE

GENERAL DYNAMICS ELECTRIC BOAT | Sr Systems Administrator | ***Dec 2023 – Present***
Supports mission-critical, virtualized Windows environments within a DoD Secret space, ensuring strict adherence to Authorization to Operate (ATO) requirements.

- **Compliance Automation:** Developed and deployed PowerShell automation to manage multiple manual processes, improving accuracy, auditability, and reproducibility of tasks. Refactored numerous scripts to improve logging, error catching, and debugging.
- **Vulnerability Management:** Lead security hardening efforts by interpreting CVEs and ACAS (Tenable/Nessus) scans, mapping risks to NIST 800-53 controls, and

executing remediation across the server estate. Collaborated with engineers and administrators to validate changes.

- **RMF & Audit Support:** Executed Risk Management Framework (RMF) assessments by compiling security artifacts and validating technical controls for annual security reviews.
- **Risk Tracking:** Streamlined POA&M management by designing a ticket workflow for risk tracking and remediation validation, ensuring transparency across IT teams.
- **Infrastructure Maintenance:** Managed the deployment and troubleshooting of patches via SCCM and Tanium, maintaining high availability for virtualized Windows servers.
- **Email and Communication:** Manage and improved Exchange Server environment, scaled up to become highly available and resilient following Microsoft best practices.

BUYERS EDGE PLATFORM | IT Manager & Systems Administrator | ***Nov 2019 – Dec 2023***
Progressed from SysAdmin to IT Manager, overseeing a modern, cloud-first environment and providing strategic technical leadership in a fast paced start up environment.

- **SaaS Identity Management:** Managed the complete user lifecycle within Microsoft 365 and Entra ID (Azure AD), including provisioning, deprovisioning, and configuring conditional access policies,
- **Email Management:** Managed hybrid Exchange environment for **1000** users, led migrations from on-premises and cloud acquisitions to our environment. Enforced email security policies via Mimecast gateway and hardened our DMARC/DKIM/SPF alignment to move us towards a secure "reject" policy, including monitoring and auditing during the transition period.
- **Cloud Security & Governance:** Deployed endpoint protection (Sophos EDR) to mitigate threats in a distributed remote workforce.
- **Device Management (MDM/MAM):** Deployed a secure End-User Compute environment using Intune and JAMF, enforcing BYOD policies and ensuring secure connectivity for remote staff via VPN, Windows 365, and AWS WorkSpaces.
- **ITSM Leadership:** Championed ITSM best practices using Jira/Confluence to optimize change control, improve incident resolution times, and document system configurations.
- **Team Development:** Coached and mentored junior staff on infrastructure support, endpoint management, and standard operating procedures.

POWERPHONE (TOTAL RESPONSE) | Client Technician | *Oct 2016 – Nov 2019*

- Provided advanced troubleshooting for proprietary 911 emergency response software on client Windows Server environments.
- Conducted log analysis to identify root causes of critical system failures, collaborating with development teams for resolution.

EDUCATION & CERTIFICATIONS

Master of Science, Cybersecurity & Information Assurance
Western Governors University | *Expected May 2026*

- *Capstone Focus:* GRC Engineering and Compliance Automation.

Bachelor of Arts, Communications

Central Connecticut State University

Certification: CompTIA Security+ and CySA+