**678-925-9494** [**jay.jalil@engineer.com**](mailto:jay.jalil@engineer.com)

**OBJECTIVE: Senior Application Security Engineer/ DevSecOps Engineer**

**TOP SECRET /SCI via SSBI Clearance. DHS EOD Clearance.**

* **CERTIFICATIONS**

CISSP PMP AZ-900 AWS SYSOPS AWS ARCHITECT ASSOCIATE-C|CISO SPLUNK ADMINISTRATOR SPLUNK POWER USER CAP CEH SECURITY+CE SCRUM Master SCRUM Trainer SCRUM Product Owner CCNA ITILv3 NETAPP

Certificates of Completion: DevSecOps Essentials; Intro Azure DevSecOps; Intro Cloud DevSecOps.

Operations & Incident Response to CompTIA Security+. CompTIA CySA+.

EC-Council Certified DevSecOps Engineer.

* **PROFESSIONAL DEVELOPMENT**

Master of Science in Computer Science, Webster University, St. Louis, MO.   
Bachelor of Science in Computer Science, Devry University of Technology, Dallas, TX.   
Bachelor of Arts in Management, Saint Leo University, Atlanta, GA.

Program Manager and Project Manager experience handling multi-million dollar programs.

Warrant Officer Advance Course (Cyber Security & Information Security), Fort Gordon, GA.

Warrant Officer Basic Course (Information Security & Cisco Networking), Fort Gordon, GA.   
Warrant Officer Candidate Course, Warrant Officer Leadership Academy, Fort Rucker, AL.

U.S. Army Electronic & Communication Security Academy, Ft. Gordon, GA.   
U.S. Army Information Technology Systems Analyst Academy, Ft. Gordon, GA.

* **AREAS OF EXPERTISE**

|  |  |  |
| --- | --- | --- |
| * Cyber Threat Analysis * Security Architecture & Strategy * Network Security * Policy Development & Mgnt. * Database Management * Governance, Risk, Compliance * Security Incident Response * DevSecOps Architect | * Vulnerability/Risk Assessment * Project Management * Disaster Recovery Plan * Vulnerability Management * Strategic Planning * Cyber Threat Intelligence * Security Operations Center | * Security-Awareness * Application Security * Intrusion Detection * Executive Leadership * Vulnerability Testing * Data Privacy/Protection * SIEM Tools * Cyber Security Strategy |

* **QUALIFICATIONS**

-20 years experience in Information Technology & Cyber Security for Dept of Defense and Commercial.

-SonarQube; GitLab; Ansible; Docker; JIRA; ACAS; Nexus; Twistlock; Keycloak; Databricks; GitHub.

-Acunetix; Burpe Suite; MobaXterm; Terraform; GitLab Runner; Snyk; CI/CD Pipeline; DirBuster; Zenmap.

-Wireshark; OWASP ZAP; Qualys; AppDetectivePro; WebInspect; Fortify; Tenable Nessus; Prisma Cloud.

-StealthWatch; Cyber Kill Chain, Tipping Point; HP Service Manager; nGenuisOne; FireEye; Rapid7.

-Cisco IronPort; EnCase; Agent Ransack; SCAP; URLSnarf; Zero Trust Architecture; Azure.

-Splunk; McAfee ePoint Orchestra; McAfee WebWasher; McAfee SolidCore; McAfee ESM, PowerBI.

-NIST RMF; EMASS; SCCM 2012; HBSS; Xacta; Ubuntu; VMWare ESXi; Node.js.

-FedRAMP; AWS; FISMA; NIST 800-53r4; NIPSOM; DCID 6/9; DoD 8500 Series; FIPS.

-ISO 17799/27001/27002; Wireless LAN; TCP/IP; LDAP; DNS; WINS; DHCP; eGRC-10; HIPAA.

-MS Server 2012; Visual Studio 2012; SQL Server 2012; Active Directory; Exchange Server; Project 2010.

-Oracle DBA; SQL Server DBA. Cisco Network Security, Cisco Email Security; MDE.

-Python; Linux; Unix; SQL; Shell Scripting; SharePoint; ServiceNow; Group Policy.

* **PROFESSIONAL EXPERIENCE**

**10/2022-Present: DoD/USSOCOM: Senior Application Security Engineer/DevSecOps Engineer**

Senior Architect in building a Continuous Intergration/Continuous Deployment Pipeline for DoD.

Perform DAST, IAST, & SAST, and SSDLC to build DevSecOps CI/CD pipeline for IaC, Cloud, & Mobile.

Perform Source Code Repository using GitLab; Perform Build Orchestrator using GitLab Runner.

Perform Static Code Analysis (Quality and Security) using SonarQube; Perform Issue Tracking using JIRA.

Perform Artifact Manager & Container Registry using Nexus; Perform Documentation Wiki using Confluence.

Perform Container Security Scanning using Twistlock; Perform Container Auditing using Terraform/Kubernetes.

Perform Identity Management using Keycloak with IDP to Azure AD; Vulnerability Management with Nessus.

**Identify, measure, control & minimize security risks to information systems including application and host security.  
Evaluate the current methods in use by Early Warning to access and process data via Early Warning applications.  
Owns the development of repeatable application security architectures working with internal and external partners.   
Leads security efforts with architecture teams to implement new developed applications & infrastructure.**

Perform security automation within DevSecOps and CI/CD processes including vulnerability identification.

Perform automated provisioning scripts using Terraform and create heat maps using PowerBI.

Advises and approves of changes and architectures for assigned areas from a security perspective.  
Manage decisions on product business cases for functional & detail design specs for proper security standards.  
Assists & leads security incident response process as assigned & contribute towards risk mitigation efforts.  
Subject Matter Expert & contributor to the development of Early Warning security policy & procedures.  
Develops and owns architectural reference material to ensure that repeatable security practices are implemented.

Document and present risks and security issues that impact the confidentiality, integrity & availability of the business by assisting in documentation, tracking and creating solutions for mitigation.  
Coordinate internal/external organizations to coordinate application & network-based penetration testing.  
Lead efforts with Secure Software Development Lifecycle to perform SAST on all custom developed code.  
Perform tabletop testing for security vulnerabilities, review penetration testing findings, and mitigate controls.  
Support company's commitment to risk management & protecting the integrity & confidentiality of systems & data.

**05/2022-10/2022: DoD/NCIS, Remote: Sr. Application Security Engineer/Vulnerability Management**

Manage Defensive cybersecurity support along with Log management and analysis and SIEM support.

Creating the Incident Response Plan and performing Auditing on the enterprise network systems.

Perform Governance, Risk & Compliance (GRC) along with creating the Standard Operating Procedures (SOP).

Subject matter expert to provide GRC guidance and interpretation of rules, regulations, risks, and best practices.

Create & implement policies, procedures, communication of the new policies & procedures to support projects.

Document and escalate incidents that may cause ongoing and immediate impact to the environment.

Performed event correlation to gain situational awareness and determine the effectiveness of an observed attack.

Provided daily summary reports of network events and activity relevant to cyber defense practices.

Receive & analyze network alerts from various sources within the enterprise and determine possible causes of alerts.

Provided timely detection, identification, and alerting of possible attacks/intrusions and anomalous activities.

Use cyber defense tools for continual monitoring and analysis of system activity to identify malicious activity.

Analyze identified malicious activity to determine weaknesses exploited, exploitation methods, & effects on system.

Identify network mapping & operating system fingerprinting activities & analyze anomalies in network traffic.

Validate intrusion detection system (IDS) alerts against network traffic using packet analysis tools.

Develop the strategic plan and roadmap to assist management in the assessment of project risks and controls.

Leverage industry and technical expertise to assist management to address business risks more effectively.

Manage the strategic development and improvement of risk frameworks, methodologies, and limits.

Administrator using McAfee Enterprise Security Manager to investigate and respond to threats.

Use McAfee ESM to find anomalies and malware to monitor data breaches and data loss.

Used Trellix and McAfee Solidcore (McAfee ESM) to conduct vulnerability management & troubleshooting.

Perform Splunk Administrator/Engineer activities for installation, engineering, and monitoring SIEM.

**12/2021-05/2022: Comerica Bank, Remote: Senior Vulnerability Management Consultant**

Identify, review and evaluate the solution requirements for business units, application teams, and vendors. Investigated and proposed strategic fits for virtualization, consolidation and rationalization solution opportunities.

Evaluated & align strategic solutions across infrastructure platforms and solutions specific to system technologies. Understand, participate, reviewed and influenced long term capacity planning and technology investments.

Provided Client consulting and planning guidance as applicable for moderate to large highly complex programs. Provided consultation for cross-functional infrastructure departments on multiple initiatives to meet objectives.

Identified & evaluated programs & design processes that enhance and rationalize existing & future solutions. Mapped requirements into standard services solution, identify opportunities for integrating technologies.

Provided cost effective solutions for moderate to large highly complex project/programs/initiatives.

Reviewed, identified & managed requirements for complex solutions & cost value, feasibility, and risk analysis.

Reviewed, develop and update architectural standards, guiding principles, rationales and strategies.

Evaluated, review & approve highly complex design solutions for business and infrastructure projects or programs.

Used Qualys VDMR to perform DAST and vulnerability risk management and web application security scanning.

**10/2020-10/2021: DOD/DCSA, Remote: Program Manager for Infrastructure Implementation**

Managed and Coordinated three classified projects under PMP/PMI guidelines, structure, and best practices.

Responsible for the performance of the work and act in the capacity of the Contractor Program Manager.

Operated with full authority on all contract matters related to daily operations of the contract.

Created and update all the major CDO artifacts and documents required for completion of the project.

Managed the timeline, budget, Risk Management Framework (RMF) requirements.

Managed the creation of an Incident Response plan for responding to various emergencies.

Developed and maintained an effective quality control program to ensure services are properly performed.

Created and operated under a quality control program (QCP) to ensure work complies to the contract.

Lead capability assessments and partner with program managers to help build business unit security roadmap.

Developed high-quality executive reports, including strategies and describing current and expected future state.

Present weekly and monthly reports to C-Level executive-level management with project progress and issues.

Actively recruited future companies to the contract and provided briefings on the overall concept of the plan.

Created all documents that are required for the project according to project management institute standards.

Conducted face-to-face sales meetings with clients on the purpose and benefits of government technical tools.

Accountable and Responsible for implementing FireEye hardware tools at over 32 external client sites.

Performed Threat Modeling for the client company to locate vulnerabilities and develop countermeasures.

**01/2018-12/2020:** **JCC-5/DHS, Remote: Project Manager/Senior Application Security Engineer**

Vulnerability Management Consultant in charge of Top Secret and Secret networks controlling 40 servers.

Perform Supply Chain Risk Management & Continuous Monitoring on 40 servers for classified network systems.

Performed Nessus scanning using Tenable.sc to manipulate data and create reports for management.

Identified & Documented risks, Monitor the risks, Institute Governance and regular review of the risks.

Analyzed Risk Management, Evaluate Data, Use Automation to Scan & Monitor, Integrate Supply Chain.

Performed DAST using Tenable.io/Nessus to detect Common Vulnerabilities and Exposures (CVEs).

Installed Tenable products (multiple Nessus scanners and Security Center) onto two classified network systems.

Performed Upgrades on Tenable products (multiple Nessus scanners and Security Center) for classified systems.

Defined/supported DHS vulnerability management and security assessment standards and metrics within a SOC.

Used Nessus Security Manager to conduct & maintain vulnerability scanning on networks, systems and applications.

Directed Recertification & Accreditation activities for IP-based networks & assist managing schedule for ATO.

Produced actionable, risk-based reports on security assessment results & assist with vulnerability remediation.

Continuous Monitoring to deliver results based on appropriate FISMA score category targets for system risks.

Managed, trained and mentored junior team members and assisted other security life cycle activities.

Developed & maintained security plans & security testing plans & improve risk models, metrics, reports, processes.

Splunk Administrator creating alerts, rules and advanced logic within Splunk Enterprise.

Splunk Administrator where develop automated searches and applications using Python scripting.

Use Single Sign-on (SSO) protocols and tokens (OAuth, OpenID, and JWT) for user access.

Performed Threat Analysis by defining scope, building processes, defined rating system & performing analysis.

**09/17-01/2018: JCC-5/DISA, Fort Meade, MD.: Senior Cyber Security Manager – Contractor**

Performed Threat Modeling for the client company to locate vulnerabilities and develop countermeasures

Performed DAST/SAST using HP Fortify, WebInspect, & AppDetective to scans networks, databases & endpoints.

Performed ISSM and ISSO tasks for IT systems in accordance with NIST SP 800-37 & 800-53 Rev4 requirements.

Performed system administration functions to create SSP, SCTM and documenting the security architecture.

Reviewed security threats and implement effective countermeasures IAW established policies/regulations/directives.

Analyzed network or system changes/reconfigurations for security impacts (performs risk analysis/assessment).

Performed functions as required in support of the DoD Instruction 8510.01 Risk Management Framework (RMF).

Performed privacy impact assessments and provide PII data security and monitoring and migration strategies.

Identified potential vulnerabilities to cyber and information security using penetration testing and red teams.

Provided technologies for identification, modeling, and predictive analysis of cyber threats.

Provided recommendations to the Information System Security Managers to bring their systems into compliancy. Analyzed and document deficiencies in POA&Ms or requests prepared for Acceptance of Risk (AoR).

Maintained security posture status in the Government systems of record which is reviewed by Approval Authorities.

Performed assessments of security controls, identify weaknesses, and track remediation activities in POA&Ms.

Worked with technical teams to mitigate security control deficiencies for assigned IT systems.

Advise system owners on all matters, technical and otherwise, involving the security of assigned IT systems.

Performed NIST RMF SP 800-37 RMF and DIACAP Assessment & Authorization processes.

Performed presentations to the ISSM staff concerning the status of each project under my responsibility.

Provided Single Sign-on (SSO) access using protocols and tokens (OAuth, OpenID, and JWT) for users.

**05/17-09/2017: JCC-5/DHA, Falls Church, VA.: Senior Cyber Security Engineer - Contractor**

Performed ISSO tasks for IT systems in accordance with NIST 800-53, NIST 800-53A & NIST SP 800-37.

Performed information assurance certification and accreditation analysis, security assessments.

Performed DAST/SAST using HP Fortify, WebInspect, & AppDetective to scans networks, databases & endpoints.

Analyzed and document deficiencies in POA&Ms or requests prepared for Acceptance of Risk (AoR).

Maintained security posture status in the Government systems of record where this information was reviewed by Approval Authorities or other external IA organizations when necessary.

Perform assessments of security controls, identify weaknesses, & track remediation activities in POA&Ms.

Coordinated with technical teams to mitigate security control deficiencies for assigned IT systems.

Advised system owners on matters, technical and otherwise, involving the security of assigned IT systems.

Conducted scans of networks, databases and endpoints using Fortify, WebInspect and App Detective.

Used industry testing tools to include, Tenable.io Nessus, WebInspect, AppDetective, DBProtect and XACTA.

Assessed security findings, develop testing plans, develops Security Assessment Reports (SAR).

Answered the RTM management, operational and technical questions and support findings to the system.

Validated client documents that are then presented to DHS-ISD department for approval.

Interfaced the client, providing information system security engineering support for system security configuration.

Created SAR, SCAP, RTM, along with editing the SSP and validating POAMs for ongoing assessments.

Completed security assignments for NIST RMF Revision 4, AWS, FISMA and FEDRAMP environments

**01/17-05/17: JCC-5/U.S. Army, Atlanta, GA.: Senior Cyber Security Officer/Project Manager**

Project Manager on $200-million budget for Department of Defense Information Technology network systems.

Information Technology officer for 500 personnel on computer networks and satellite & radio communications.

Performed DAST/SAST using HP Fortify, WebInspect, & AppDetective to scans networks, databases & endpoints.

Used Zenmap for vulnerability scanning, port scanning and network mapping prior to assessing the network.

Spearheaded creation of strategic road maps instrumental in executive team planning for IT departments.

Implemented security using DoD Information Assurance DIACAP, FISMA, FIPS, NIST and IAVA.

Managed & installed IAVA update patches to the servers and network using proper DOD procedures and security.

Performed vulnerability checks using DoD intrusion detection tools Nessus, AR 25-1, AR 25-2.

Provided system security for electronic data communications, network and data security, electronic commerce.

Interfaced with government agencies to implement best practices on information system security systems.

Configured & installed servers on the LAN network and in correct zones and assigned IP addresses.

Assisted in implementing RAID architect onto the servers, proper disk space for number of drives required on SAN.

Designed Disk Groups, assign Failover/Failback per Virtual Disks & assigned port connections for SAN.

Used industry testing tools to include, Nessus, Tenable, WebInspect, AppDetective, DBProtect and XACTA.

Assessed security findings, develop testing plans, develops Security Assessment Reports (SAR).

Answered the RTM management, operational and technical questions and support findings to the system.

Interfaced the client, providing information system security engineering support for system security configuration.

Created SAR, SCAP, RTM, along with editing the SSP and validating POAMs for ongoing assessments.

Completed security assignments for NIST RMF Revision 4, AWS, FISMA and FEDRAMP environments.

**12/15-01/17: JCC-5/NSR, Atlanta, GA.: Senior Application Security Consultant & Splunk Contractor**

Used Threat Modeling to design & build a defense-in-depth cybersecurity program for Norfolk Southern Railroad.

Designed & maintained enterprise deployment of server anti-virus and host intrusion prevention software.

Lead Engineer in the Information Security Operations team in building the critical security infrastructure.

Lead Engineer in developing and integrating the company’s Automated Information Security program.

Performed Threat Modeling to locate vulnerabilities and develop countermeasures and activate mitigations.

Experience with Windows and Linux operating systems and performing deep packet network analysis.

Worked with data loss prevention tools, web browsing filters, email filters, vulnerability scans, SIEMs, and IPSs.

Used various tools to detect, deny disrupt, degrade, deceive and contain information for cyber chain kill.

Prevented reconnaissance, weaponization, delivery, exploitation, spread, command & control by remote attackers.

Used Wireshark to capture packets of and analyze network traffic from partner company’s networks.

Used Tipping Point for Intrusion Detection deep packet inspection, threat reputation, and malware analysis.

Used FireEye to proactively detect Advanced Persistent Threats (APTs), DAST and SAST to isolate the threat.

Used FireEye for Endpoint Threat Detection by tracing alerts directly to compromised devices.

Used HP Fortify to assist Java and Jenkins Developers by building VM processes along with installation boxes.

Used HP Fortify Software Security Center (SSC) to manage developers access credentials and project information.

Used Qualys to perform dynamic scanning of endpoint inventory and web application.

Used HP Fortify for SAST scan of source code for the developers to build better program modules.

Used Splunk to perform SIEM Intrusion Detection and read logs and write Windows scripts and alerts.

Used IronPort (Cisco Email Server & Cisco Management Server) to manage email and TLS access request.

Used Active Directory to manage the authorization for user permissions and credentials.

Used Wireshark to analyze network traffic prior to allowing external networks to connect to NSR network.

Used McAfee ePO Web Washer firewall for department access and deciding on which URLs to approve.

Used StealthWatch to track network flow, user-identity tracking and perform analysis for malicious behavior.

Used StealthWatch for real-time network monitoring and detection of Advance Persistent Threats (APTs).

Used McAfee ePO Orchestrator to allow external customers to enter the network firewall to conduct business.

**04/15-03/16: JCC-5/DHS, Washington, DC: Senior Cyber Security Engineer - Contractor**

Developed Security Assessment scripts for vulnerability scans and assess automated vulnerability scan.

Discussed requirement descriptions, weaknesses, affected elements, severity levels, and recommended remediation.

Used industry testing tools to include, Nessus, Tenable.io, WebInspect, AppDetective, DBProtect and XACTA.

Assessed security findings, develop testing plans, develops Security Assessment Reports (SAR).

Answered the RTM management, operational and technical questions and support findings to the system.

Validated client documents that are then presented to DHS-ISD department for approval.

Interfaced the client, providing information system security engineering support for system security configuration.

Created SAR, SCAP, RTM, along with editing the SSP and validating POAMs for ongoing assessments.

Completed security assignments for NIST RMF Revision 4, AWS, FISMA and FEDRAMP environments.

Used Wireshark to analyze network traffic prior to approving the Authorization-to-Operate and access to enclave.

Used Zenmap for vulnerability scanning, port scanning and network mapping prior to assessing the network.

**10/14 – 04/15: SuprTEK (DHA), Falls Church, VA: Senior Cyber Security Engineer Contractor**

Assisted the IA Manager (IAM) in meeting their duties and responsibilities outlined in DoDI 8500.2.

Initiated protective or corrective measures when an IA incident or vulnerability is discovered.

Performed DAST/SAST using HP Fortify, WebInspect, & AppDetective to scans networks, databases & endpoints.

Confirmed IA-enabled software, hardware, and firmware comply with appropriate security configurations.

Ensured DoD information system recovery processes are monitored & IA components are properly restored.

Implemented & enforced DoD information system IA policies & procedures as defined by C&A documentation.

Supported the DHA in RMF lifecycle support for twenty health care systems/applications.

Performed risk assessments, annual reviews, ATOs and sustained ATOs, and Branch Service Accreditation.

Used eMASS, POAMs, DIACAP/RMF packages, remediation, mitigations, risk assessments and security analysis.

Performed scans and vulnerability assessments using AppDetective, WebInspect, HP Fortify and Nessus.

Managed DISA Security Readiness Reviews (SRR) and provide technical leadership/consulting support to staff.

Developed Security Test Reports, POA&Ms, Certification&Accreditation security packages and documents.

Evaluated security vulnerabilities and mitigation strategies for networked and non-networked systems.

Evaluated information security principles, DoD STIGs, and C&A processes for technical systems.

Used Zenmap for vulnerability scanning, port scanning and network mapping prior to assessing the network.

**06/14 – 10/14: NSSPlus (DHA), Falls Church, VA.: Senior Cyber Security Engineer - Contractor**

Conducted NIST Risk Management Framework (RMF) validation for Department of Defense clients.

Performed scans and Manual Reviews using AppDetective, WebInspect, HP Fortify, Tenable Nessus, SCAP.

Developed Security Test Reports, POA&Ms, Certification&Accreditation security packages and documents.

Evaluated security vulnerabilities and mitigation strategies for networked and non-networked systems.

Evaluated information security principles, DoD STIGs, and C&A processes for technical systems.

Interfaced the client, providing information system security engineering support for system security configuration.

Perform testing and analytical activities, including security administration, vulnerability assessments.

Conducted application security, client reporting, authoring documentation and A&A preparation.

Provided information protection needs via system security, security CONOPS, and security development.

Analyzed functional architectures, design constraints, life cycle support needs and gave recommendations.

Reviewed vulnerability scans to identify false positives, mitigation strategies, and system fixes.

Develop technical documentation e.g. network diagrams, inventory control, data flows and perform reviews.

Used Zenmap for vulnerability scanning, port scanning and network mapping prior to assessing the network.

**10/12-06/14: Engility, (Dept of VA) Charleston, SC: Senior Cyber Security Engineer & Splunk Administrator**

Performed Systems Analysis, Systems Architecture, Systems/Equipment Support, Test and Evaluation.

Conducted NIST SP 800-53, FIPS 140-2, DIACAP, ISO 27001, Disaster Recovery Planning and Policies.

Managed NIST Risk Management Framework (RMF) process and standards for Dept of Veteran Affairs.

Researched, designed, developed, tested and validated information assurance mitigations via SOA.

Lead Engineer for monitoring and documenting system threats, vulnerabilities and security mitigations.

Monitored and documented risk factors (i.e. operational criticality of the system & associated security environment).

Designed, configured & managed security within iCloud environment concerning servers, databases files.

Provided security solution/mitigation development and validation testing for iCloud Information System.

SPLUNK Administrator for performing Audit Logging on both Windows and Linux servers and operating systems.

Created alert scripts and dashboard scripts to function on the Linux and Windows server operating systems.

Designed incident response planning and management of security incidents & to protect enterprise-wide IT.

Designed Single Sign-on (SSO) for users to access the network environment using SAML, OAuth, & OpenID.

**06/12 – 10/12: CSC (SPAWAR), Charleston, SC: Senior Cyber Security Engineer - Contractor**

Team Lead for government project for Department of the Navy where budget was at $55-million.

Provided engineering analysis, design and support for firewalls, routers, networks and operating systems.

Performed vulnerability scans & Audit Log monitoring to detect system and network anomalies.

Enforced the information security configuration management and configuration management procedures passwords.

Developed technical and programmatic assessments, evaluated engineering and integration initiatives.

Implemented, enforced & delivered security policies for software, hardware & communications systems.

Performed Threat Modeling via product evaluations, risk assessment and implemented vendor products/services.

Validated & tested security architecture and design solutions to produce detailed engineering specifications.

Developed, tested and operated firewalls, IDS, IPS, enterprise anti-virus systems and software tools.

Recommended installation, modification of hardware/software components and all configuration changes.

Provided enforcement of security directives, orders, standards, plans and procedures at server sites.

Ensured system support personnel receive/maintain security awareness and training.

Advised management on business relations caused by theft, destruction, alteration or denial of access to information.

Monitored user access process to ensure operational integrity of the system.

Used SOA Principle to support integration and consolidation activities within the Navy/DoD enterprise systems.

Used industry testing tools to include, Nessus, Tenable, WebInspect, AppDetective, DBProtect and XACTA.

Assessed security findings, develop testing plans, develops Security Assessment Reports (SAR).

Answered the RTM management, operational and technical questions and support findings to the system.

Created SAR, SCAP, RTM, along with editing the SSP and validating POAMs for ongoing assessments.

Completed security assignments for NIST RMF Revision 3, FISMA and FEDRAMP environments

**06/11-06/12: JCC-5, Vandenberg AFB, CA: Senior Cyber Security Engineer - Contractor**

Project Manager for $200-million budget for four Department of Defense projects for Information Security.

Project Manager for scheduling, managing DIACAP projects to the DoD and the U.S. Air Force.

Performed as Risk Management Framework for five projects and manage their progress toward IATT/ATO.

Applied effective information assurance procedures and policies including change management.

Managed security policies, disaster recovery, release management, systems maintenance and operations.

Created packages for IATT and ATO to complete government contracts for DoD and U.S. Air Force.

Conducted PowerPoint presentations to DAA/A6 and IAM to attain approval for receiving five ATOs.

Participated in design review of systems and system modifications for impact to security using DoD 8500.

Planned and managed Security Test and Evaluations (ST&E) to ensure compliance with DoD IA controls.

Performed vulnerability analysis using Defense Information Systems Agency (DISA) vulnerability tools.

Designed Security Readiness Review (SRR) Scripts & perform technical analysis system scans.

Assisted SLRSC Range/System Engineers in closing open vulnerabilities to harden systems for network security.

Defined and recommended security requirements concerning EMSEC and testing communications (ST&E).

Used SOA Framework for integration and consolidation activities within the Air Force and DoD enterprise systems.

**06/10-6/11: Telecommunication Systems, Suwanee, GA: Senior Information Security Engineer - Contractor**

Project Manager of $50-million budget developing policies and plans for information security and network systems.

Performed IA Engineering support (design, architecture, development, integration, certification and accreditation).

Achieved and maintained Government IA certification and accreditation requirements using DoD 8500 series.

Established an IA training program for the ongoing education and indoctrination of network engineering staff.

Effectively and independently performed gap assessments, plan mitigation strategies, and implement accordingly.

Developed & created security policies, disaster recovery, release management, systems maintenance and operations.

Developed annual information security budget for capital infrastructure improvements using DCID 6/9.

Designed and Writing packages and templates for Risk Management Framework (RMF) on IATC/ATC project.

Provided DISA Security standards including the Gold Disk, SRR, STIGs, IAVA and IAVB.

Designed and created packages to meet ISO 27001 policies concerning security standards and compliance.

**09/09-06/10: Georgia Army National Guard, Atlanta, GA.: Brigade Chief Information Technology Officer.**

Project Manager on $250-million budget for Department of Defense Information Technology network systems.

Information Technology officer for 500 personnel on computer networks and satellite & radio communications.

Created two-year strategic road maps instrumental in executive team planning for IT departments.

Implemented security using DoD Information Assurance DIACAP, FISMA, FIPS, NIST and IAVA.

Managed & installed IAVA update patches to the servers and network using proper DOD procedures and security.

Performed vulnerability checks using DoD intrusion detection tools Nessus, AR 25-1, AR 25-2.

Provided system security for electronic data communications, network & data security, electronic systems.

Interfaced with government agencies to implement information system security mechanisms & requirements.

Configured & installed servers on the LAN network and in correct zones and assigned IP addresses.

Assisted in implementing RAID architect onto the servers, proper disk space for number of drives required on SAN.

Designed Disk Groups, assign Failover/Failback per Virtual Disks & assigned port connections for SAN.

Performed Audit Logging using Oracle Performance Monitor and Audit Trail.

**09/08 –09/09: BoozAllenHamilton, Atlanta, GA.: Information Technology Manager/Engineer.**

Project Manager over $25-million budget for DIACAP Risk Management Framework (RMF) projects for DoD.

Implemented security using DoD 8500 Series, NIST 800-53, NIST 800-53A, FISMA, FIPS-199, 800-39.

Prepared technical documents Risk Assessments, Security Plans, POA&M, MOA and Configuration Plans.

Security Certification Agent to monitor and assess all phases of NIST Risk Management Framework.

Managed database systems using Data Definition Language & Data Manipulation Language, SSIS & SSRS.

Performed Audit Logging using SQL Server Audit and Database Audit Specification.

**01/08 – 08/08: DataPath, Atlanta, GA.: Senior Information Security Analyst.**

Project Manager of $20-million budget for Department of Defense information security and network systems.

Implemented security using DoD 8500 Series, DIACAP, FISMA, FIPS-199, NIST 800-53, and IAVA.

Managed & installed IAVA update patches on servers & network using proper DOD procedures & security.

Performed vulnerability checks using DoD intrusion detection tools eEye-Retina, Nessus and SMS.

Installed Cisco routers and switches on the network to provide security for LAN & WAN networks.

Performed software updates on DOD servers, laptops and SATCOM equipment for satellite networks.

Conducted building network system for the internal and external network system along with pix firewall.

Provided system security for electronic data communications, network and data security, electronic commerce.

Interfaced with government agencies to implement information system security mechanisms & requirements.

Assisted in building NIPERNET and SIPERNET networks and tunneling network for CENTCOM.

Built and lockdowned Supermicro servers and admin laptops using Windows XP/2003 Local Security Policy.