***Professional Summary***

A highly motivated solution-oriented 15 year Information Technology (IT) professional specializing in Information Security as well as Enterprise System Development and Deployment. An effective communicator with exceptional customer service skills that has demonstrated abilities to manage projects autonomously, coordinate and lead multiple teams of up to 18 professionals and develop robust IT solutions. Vast experience supporting DoD as well as Federal customers within the Information Technology arena, including but not limited to Health Care Reform. Also has a solid record of service as key team player in fast-paced and critical technical environments. Other highlights include:

* Secret Security Clearance
* B.S. Business Administration Degree
* FISMA, IRS Publication 1075, RMF, HIPPA, NIST Special Publications
* Information Technology Infrastructure Library (ITIL) v3, SANS Institute Network Penetration Testing and Ethical Hacking, CISCO (CCNA)
* CISSP Certified Information Systems Security Professional

***Employment***

Government Client via ADS – Washington, DC December 2014 – Present

*Senior Security Policy Analyst*

As an independent consultant working for the Office of the Chief Information Officer, my primary task was to develop policies that would bring the agency into and maintain compliance with Federal Tax Information regulations. In the process of developing policy, the foundation for an enterprise security program was laid. In addition to policy development, I guided SOP development, to ensure that procedures facilitated the implementation of the new agency policy. The guidance entailed group and individual knowledge transfer in compliance discipline. Also, I worked with the agency’s management, application, network, and security teams to update processes and procedures to ensure alignment with the new agency policy. Other duties included, but were not limited to:

* Worked with management to define granular policy requirements
* Developed security control SOP templates, to ensure documentation consistency for information systems
* Created security control plan, connection agreement, and accreditation package templates
* Guided SOP development
* Identified reoccurring compliance tasks and developed a schedule to complete tasks
* Member of the Change Control Board
* Identified process weaknesses and recommended improvements
* Developed and conducted Incident Response Training
* Assisted with non-security related policies
* Provided plan of action and milestone mitigation support for identified weaknesses

Federal Client via Beacon Hill Staffing Group - Bethesda, MD June 2014 – December 2014

*Senior Security Test Analyst*

As a member of the ISS LOB, Security Authorization & Testing Team (SA&TT) for a Federal Client, I was tasked with assessing the security posture of Government customers Information Systems, against the latest FISMA requirements. The effort involved evaluating the security controls of the Client’s system and their ability to ensure the confidentiality, integrity, availability, and accountability of the data and services it provides. Senior Security Test Analyst duties included, but were not limited to:

* Performed assessments of management, operational and technical security controls to determine the extent to which security controls are implemented correctly, operating as intended, and producing the desired outcome, with respect to meeting the security requirements governing enterprise protection
* Developed technical security assessments, of the customers various GSS and Major Applications (MA), that included the evaluation of security engineering and integration initiatives
* Assessed the development of system security documentation, such as System Security Plans, Contingency Plans and Information System Risk Assessments
* Composed Security Test Plans for all levels of testing, as well as maintain records of test progress, document test results, report preparation and presents results
* Produced Corrective Actions Plans, to correct deficiencies in the security controls and mitigate vulnerabilities discovered in the information systems
* Organized and lead security control assessments efforts in the assembly of data gathering activities, interviews, documentation reviews, and preparation of assembling final deliverable packages
* Prepared and participated in executive level briefings on the status of all security control assessment related activities

Radius Technology Group, Inc. – Washington, DC March 2013 – Jun 2014

*IT Policy Analyst*

As an IT Policy Analyst supporting a government costumer, I was part of a team that was responsible for all aspects of Cyber Security. A major accomplishment undertaken was consolidating a three General Support Systems (GSS) environment to a single GSS, with 10,000 plus users and 15,000 plus networked devices, all while ensuring that the information assurance of the GSS operates securely and complies with Federal mandates. Typical duties included but were not limited to:

* Developed and maintained Information System Interconnection Agreements to include Memorandum of Understandings and Interconnection Security Agreements, for the purpose of sharing data with other agencies
* Developed reports based on Incident Response Alerts and Notifications
* Produced quarterly/annual Federal Information Security Management Act (FISMA) Reports to satisfy Federal reporting requirement
* Conducted Contingency Plan Testing and created Contingency Plan After Action Report based on testing results
* Tracked Agency Role Based Training (RBT) activities to ensure agency training compliance
* Monitored, tracked and managed GSS resources using Cyber Security Assessment and Management (CSAM) tool
* Created Agency Annual Personal Identifiable Information (PII) Report to satisfy Federal reporting requirement
* Conducted Security Self Assessments to evaluate the effectiveness of implemented security controls
* Monitored Tivoli Endpoint Manager, as part of the Continuous Monitoring Program
* Reviewed and Approved Change Control Request (CCR) to ensure system modifications are in line with established security controls
* Performed POAM Analysis to assist in the mitigation of vulnerabilities in the Information System
* Provided interpretation of Security policies to the supported program offices
* Contributed to the writing of Security documentation, to include the System Security Plan, Incident Response Plan, Contingency Plan, other ATO Package artifacts as well as the Computer Security Handbook Revision 4 update
* Conducted monthly/quarterly/annual reviews in an effort to stay compliant with security policies and procedures
* Remediate Support Tickets

CMS via TMI Solutions, Inc. - Lanham, MD August 2009 – November 2012

*Senior Security Test Engineer*

While working the Centers for Medicare and Medicaid (CMS) effort, I was tasked with leading a team of security professionals to conduct Security Control Assessments with the goal of determining the agency’s systems compliance, by examining management, operational and technical security control against the customers defined Minimum Security Requirements for “HIGH” systems (based on NIST SP 800-53 for HIGH systems), ultimately providing the information needed to support the CMS’s Certification and Accreditation (C&A) Program and Federal Information Security Management Act (FISMA) reporting. This entailed determining the potential security risks to the customer’s critical information technology assets while validating that the confidentiality, integrity and availability of system data was securely implemented. Duties included, but were not limited to:

* Ensured that the underlying infrastructure including the confidentiality, integrity and availability of system data was securely implemented
* Performed assessments of management, operational and technical security controls to determine the extent to which security controls are implemented correctly, operating as intended, and producing the desired outcome, with respect to meeting the security requirements governing enterprise protection
* Developed technical and programmatic security assessments, of the customers various GSS and Major Applications (MA), that included the evaluation of security engineering and integration initiatives, as well as provide technical support to assess the customer’s security policies implementation, standards, and guidelines
* Assessed the development of system security documentation, such as Information System Risk Assessments, Contingency Plans and System Security Plans
* Composed Security Test Plans for all levels of testing, as well as maintain records of test progress, document test results, report preparation and presents results
* Produced POA&M Reports, to correct deficiencies in the security controls and mitigate vulnerabilities discovered in the information systems
* Organized and lead security control assessments efforts in the assembly of data gathering activities, interviews, documentation reviews, and preparation of assembling final deliverable packages
* Prepared and participated in executive level briefings on the status of all security control assessment related activities
* Performed technical vulnerability scans and assessed vulnerability reports for multi-platform, large enterprise environments; included Federal Desktop Core Configuration (FDCC), databases, servers, as well as network devices

MC4 via L-3 Communications - Landover, MD December 2008 - August 2009

*Integration Test Engineer*

As an Integration Test Engineer supporting the Medical Communications for Combat Casualty Care (MC4) program, which has helped capture more than 5 million health records to date, I was commissioned to ensure cutting-edge hardware, loaded with familiar software, that transcends military branches, could digitally capture and transmit battlefield medical records, from environments where Internet connectivity is intermittent to a worldwide-accessible database. Duties to accomplish this task included:

* Perform systems planning, testing, validation, and integration engineering to the MC4 Electronic Medical Record (EMR) system, to ensure a defect-free delivery of the IS
* Provide technical integration and evaluation support on all MC4 Project Builds, including the troubleshooting and resolving of software/hardware configuration and proprietary Army/GOTS software application issues
* Instrumental in the development of technical documentation to include creating/updating detailed test procedures and the System Administration Guide (SAG): consisting of Standard Operating Procedures (SOP), Trouble Shooting actions and Sustainment measures
* Contribute to the development and administration of the MC4 network architecture to include backup/recovery planning
* Report daily testing activities to include testing status, test progression and issue/defect identification/ classification
* Analyze and assess changes, additions, and reconfigurations of the MC4 EMR systems; for Laptops/Servers, Routers, Switches, Gateways
* Recommend, based on system research, upgrade growth and security strategies in an effort to enhance to MC4’s EMR Systems

Office of the Secretary of Defense via SkillStorm, Crystal City, VA June 2008 – September 2008

*Software Systems Engineering Supervisor*

While working for the Chief Information Office (CIO) of the Office of the Secretary of Defense (OSD), I was responsible for leading the efforts to introduce new technologies throughout the organization. Projects included Application Virtualization/SoftGrid, which allows users to utilize application that have been streamed to their desktop as if they were locally installed; development of Remedy’s knowledgebase; and the upgrade to Microsoft Office 2007. These projects allow the OSD to be more productive, efficient and save monies by preserving valuable resources. Primary duties included:

* Lead user testing efforts
* Collected project requirements
* Gathered and analyzed raw data statistics then develop
* Produced project artifacts
* Provided daily testing activates and progress reports
* Presented status report presentations

SRA International, Inc. - Alexandria, VA December 2000 - March 2008

*Test Engineer IV - Information Assurance Engineer IV*

Throughout my tenure with SRA I had three primary responsibilities: Security Test Lead; Infrastructure Team Lead; and Sr. Infrastructure Test Engineer. The ultimate goal of each was to independently verify and validate our government client’s requirements were being met. Primary duties included:

* Security Testing Lead on the United States Patent and Trademarks Office, (USPTO) contract. Responsibilities included conducting Technical Vulnerability Assessments (TVA), which consisted of the review of previous assessment documentation and ensuring that the latest C & A documentation was consistent with the current project version, and included the development of TVA Plans, conducting system security vulnerability test execution and analysis, and creating TVA Reports, for each newly implemented designated Automated Information Systems (AIS). All while ensuring compliance, by using the latest Federal Government mandates, FISMA, HSPD, FIPS, and the NIST SP – 800 series.
* Team Lead for the Infrastructure Testing Team. Provided level of effort (LOE) estimates and burn rate matrix in an effort to support the customer’s budget tracking. Managed and tracked time allocated for each project to time used to ensure that there are no shortages. Delegated projects and responsibilities based on team member knowledge and expertise. Provide day-to-day assistance to team members to ensure that a high level of support is being provided to the customer as well as consistent on time delivery of documentation. Also reviewing documentation deliverables and ensuring conformance to established company/project standards and quality control procedures, to include CMM. (SRA is ISO 9001:2000 certified and also a CMM Level 4 assessed company). Managed test lab technicians to ensure workstations were available for baseline requests by, updating and tracking the request database, workstation request were complete in a timely fashion, and verified that the test server had the latest patches and applications. Additional duties involved supplying input as a member of the Process Review Team, interfacing with project teams, test managers, and Sr. project management. Furnished weekly team status reports to management.
* Sr. Infrastructure Testing Engineer Project Lead on USPTO AIS. Duties consisted of strict adherence to the SDLC process, test execution (including functional, product evaluation, regression system compatibility, system integration and 508), which included using automated testing tools as well as manual test, development of artifacts (consisting of Test Plans, Test Scenarios and Procedures, Test Reports), identify/track system defects using HP Quality Center, providing test data intelligence and Quality Assurance (QA) metrics to the customer as well as a Technical Review Board, (TRB). Provided support to the Configuration Management (CM) team to ensure CM builds were consistent with expected test environment. Conducted peer reviews when needed in an effort to define requirements. Projects supported that help the USPTO generate in excess of $1,000,000 per day and protect against unauthorized access included: Electron Filing System on the Web which eliminated the mail-in/paper application process and implemented a Portal/Web-based application filling process; the Firewall projects, Redesign, Consolidation, Upgrade and Bluecoat which increased the organizations security posture and efficiency; USPTO Network Upgrade-2 which was a complete network architecture restructure; the EDS project which upgraded the Enterprise Active Directory System; PKI projects with undertakings that resulted in Federal Bridge Certification Authority (FBCA) operational member approval, and Smart Card implementation that satisfies HSPD-12; Enterprise Application Integration – Hub which provided application translation/communication; the NAS projects which were Storage Management ventures; and the Continuity of Operations (COOP)/Disaster Recovery Plans.
* Training and Awareness Subject Matter Expert. Redeveloped the Defense Information Systems Agency (DISA) Level‑1 System Administrator (SA-1) Certification Examination, using the most current DoD Directives, DISA policies and learning objectives. Provided subject matter knowledge for DISA’s retooled Firewall and Router CBTs.
* Resale Engineer. Installed, configured, demonstrated the use of and provide technical support to clients and interested patrons for Tenix America, One-Way Data-Diode security products. The combination of the hardware appliances and software applications allow for a secure physical link to forward data between an unclassified and a classified network. The tools were displayed at DISA, as part of the Joint Warrior Interoperability Demonstration (JWID), multi-national / multi-agency War fighter exercise intended to highlight multi-level security. This product became the first product to have been awarded the highest security certification of EAL 7+ under the NIAP Common Criteria scheme.

Electronic Data Systems (EDS)March 1999 – December 2000

National Guard Bureau (NGB), Army Computer Emergency Response Team (ACERT). - Arlington, VA

*Firewall Engineer*

Primary responsibilities included the administration of the Army National Guard’s 100‑plus Point‑of‑Presence firewalls located in each state and US Territory. I assessed business needs, configured and implemented unique security policies for each, updated rule bases, added patches and replaced damaged equipment was a daily occurrence. Other duties included:

* Managed preventive and corrective action processes
* Monitored sites Intrusion Detection Systems
* Provided Disaster Recovery support efforts
* Performed security audits and used security forensics to troubleshoot and resolve reported security related incidents

Air National Guard (ANG), Network Operations Security Center (NOSC**). -** Crystal City, VA

*Information Assurance Engineer*

While working in the NOSC, I maintained operational network security devices and related system services which included actively responding to and resolving enterprise security events for each of the Air National Guard’s 250 plus units located throughout the United States and US Territories. Other duties included troubleshooting as well as:

* CISCO router configuration
* Performed WAN/MAN monitoring and optimization
* Firewall configuration and administration
* Exchange server administration/virus inoculation (Melissa, Bubble Boy and Love Bug)
* Assisted site unit with DITSCAP support
* Developed network performance metrics model and presented weekly reports

Riggs Bank, NA. - Riverdale, MD March 1996 - March 1999

*Information Security Systems Analyst*

While at Riggs Bank, currently known as PNC, I was responsible for all aspects of security for the corporate offices as well as the branches through metropolitan DC area. Duties included:

* Provided administrative support on ACF2, Novell and OS/2 platforms to ensure employees access systems
* Performed system monitoring
* Conduct internal audits
* Defined and developed network policy
* Detection and resolution of network intrusions and misuse
* Supported efforts to improve Information Security awareness programs and education
* Administered Gauntlet firewall
* Enterprise Anti-Virus management

***Education***

B.S., Business Administration from the University of Maryland Eastern Shore May 1994

***Professional Affiliations***

Certified Information Systems Security Professional (CISSP)

Information Technology Infrastructure Library (ITIL) v3

SANS Institute

Cisco Certified Network Associate (CCNA)

Microsoft Certified Professional (MCP)

ACF2 East Coast Users Security Group

***Skills***

Tivoli Endpoint Manager, Nessus, nCircle Suite 360, AppScan V8.5, Secutor Prime, Internet Security Systems (ISS) Internet Scanner, Computer Security Assessment Management (CSAM) Tool, NMAP, Theater Medical Information Program Composite Health Care System Caché (TC2), Defense Medical Logistics Standard Support (DMLSS), DMLSS Customer Assistance Module (DCAM), Theater Army Medical Management Information System (TAMMIS), Electronic Post Deployment Health Assessment (ePPDHA), Armed forces Health Longitudinal Technology Application – Theater (AHLTA-T), Business Objects, Microsoft Desktop Optimization, Microsoft Application Virtualization, Microsoft SoftGrid, SharePoint, Quality Center, Test Director, Rational Tool Suite, HP Open View, ELRON Internet Manager, Gauntlet Firewall, Raptor Firewall, Check Point Firewall, Sidewinder Firewall, Stone Beat Load Balancer, Blue Coat Proxy SG, Microsoft Widows Server 2003 Active Directory Infrastructure, Datakey Card Management System, Datakey CIP, Entrust Security Authority Manager, Entrust Enteligence, EMC Control Center (ECC), Enterprise Storage Network (ESN) Manager, IBM TotalStorage™ Network Attached Storage 300G, What’s Up Gold network monitor, IBM TotalStorage FAStT200 HA Storage Server IBM LAN Manager and CT/2 Security Administration Monitors - Tandem (VLX) Computer System {Main-Frame}, Tandem 9-Track Turbo Tape Drives, SQL Server, TANDEM, XEROX {3700,4050} OS/2, Lotus 1-2-3, COBOL, CICS, RAS servers, Netfinity, VAX

***Clearance Level***

Secret