Michael Williamson

8817 Fran Del Dr., Fort Washington, MD 20744

**Mywilli9@verizon.net**

Mobile: 202.360.1968

**On-Line Training:**

* Certificate for Cyber Fundamentals for Law Enforcement Investigations 1/2019
* Certificate for DNSSEC Training Workshop 1/2019
* Certificate for 101- Critical Infrastructure Protection 1/2019
* Certificate for Cyber Security Investigations 1/2019
* Certificate for CDM Module 2 Hardware Asset Management 1/2019
* Certificate for CDM Module 3 Software Asset Management 1/2019
* Certificate for CDM Module 4 Configuration Settings Management 1/2019
* Certificate for CDM Module 5 Vulnerability Management 1/2019
* Certificate for CDM Module 1 Overview 1/2019
* Wireless Network Security 1/2019
* Risk Management Framework Curriculum 5/2019
* CompTIA Advanced Security Practitioner (CASP) 11/2019
* CompTIA Cybersecurity Analyst (CySA+) Prep 11/2019
* CompTIA Security+ (SY0-501) Certification Prep 11/2019
* [Wireless Network Security (WNS)](https://fedvte.usalearning.gov/viewcourse_nf.php?group=1&course=22) 11/2019
* Mobile and Device Security 11/2019
* Mobile Forensics 11/2019

**In Class Training**

* Navy Qualified Validator (NQV), Training 2017
* **Products**

Nessus, Foundstone, Retina, Riverbed, Niksum Nmap, Metasploit, Nexpose, Qualys, Wireshark, WebInspect, OWASP Zap, Core Impact, AppScan, AppDetect, ASA, Checkpoint, Sidewinder, Stonegate, Netscreen, Rapter, Mars, Nitro, Proventure, IDSM-2, Tipping Point, Unix, Linux, Windows, Zscaler etc...

**Certifications:**

* (CCNP) Cisco Certified Network Professional # CSCO10019262, Cisco, 1/2004, expired
* (CCSP) Cisco Certified Security Professional # CSCO10019262, Cisco, 1/2005, expired
* (CISSP) Certified Information System Security Professional # 342173, ISC2, (1/2022)
* (CEH) Certified Ethical Hacker # ECC41824300973, EC-Council, (12/31/2022)
* (ECSA) E-Council Security Analyst # ECC93190653594, EC-Council, (12/31/2020)
* (CHFI) Certified Hacker Forensic Investigator # ECC75493699104, EC-Council, 12/31/2020
* (CISM) Certified Information Security Manager (Exam recipient), ISACA, December (2012)
* (CISA) Certified Information Systems Auditor # 14118702, ISACA, (10/2020)
* (CAP) Certification Authorization Professional # 342173, ISC2 (1/30/2019 - 1/31/2022)

**Education:**

University of the District of Columbia (UDC), 3 Years, No Degree

**Locations:**

DC General Hospital; DC Fire Department; Sprint; Department of Transportation (DOT); Department of State (DOS); Veterans Administration (VA), Transportation Security Administration (TSA); Federal Communication Commission (FCC); Department of Defense (DOD); Department of Justice (DOJ); United States House of Representatives, Department of Education (DOE), Pentagon

**Business Integra**

**Information Assurance Engineer (RMF)**

**4/6/2020 to 09/17/2021**

* Support planning and execution for certification and accreditation processes.
* Ensure risk assessment packages are compliant with accreditation requirements. Integrate information protection requirements into system designs.
* To utilize tools such as CSET, Vulnerator for evaluating controls.
* Reviewed all artifacts required to be submitted into eMass for BoE.
* Upload Security Compliance Check for all OS systems as required.
* Performed updating and verifying POAM finding as completed and accurate.
* Assessed NIST controls and CCI’s for accuracy.
* To utilize eMass management tool as a repository for body of evidence (BOE) for NIST (RMF) controls, POA&M’s and DoD (CCI’s)
* Work with lead specialist for the implementation of the NIST 18 control family Policy and Procedures required for A&A.

**Validatek**

**USCG (ONI)**

**Information Assurance Engineer**

**1/27/2020 to 3/20/20**

* Provide technical, administrative, and security management services for the area of Assessment & Authorization (A&A) by conducting IT evaluations and assessments, and performing documentation support services.
* Review, update and publish all cyber security artifacts to support unclassified and classified cyber security efforts using prescribed tools and maintain any relevant security artifacts.
* Assess security controls and determine that controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements for systems using USCG, DoD, DHS, and/or the IC directives, regulations, instructions and procedures.
* Provide review and recommendation services on security architecture for new systems and systems that are upgraded to ensure that security is integrated throughout the lifecycle of the system.
* Work directly with appointed Government entities in support of maintaining the COOP.
* Provide services during a DR event for Notification/Activation, Recovery, and Reconstitution phases.
* As needed, serve as Assistant ISSO (AISSO) for the security posture of an IT system.
* Ensure the implementation of Security and Information Assurance (SIA) requirements of an IS throughout the system lifecycle, from concept phase through disposal to include serving as an active participant in the Security Authorization Process for their assigned system.

**Business Integra**

**DTIC**

**Information Assurance Engineer (RMF)**

**12/4/2019 to 1/24/2020**

* Support planning and execution for certification and accreditation processes.
* Ensure risk assessment packages are compliant with accreditation requirements. Integrate information protection requirements into system designs.
* To utilize tools such as CSET, Vulnerator for evaluating controls.
* Reviewed all artifacts required to be submitted into eMass for BoE.
* Upload Security Compliance Check for all OS systems as required.
* Performed updating and verifying POAM finding as completed and accurate.
* Assessed NIST controls and CCI’s for accuracy.
* To utilize eMass management tool as a repository for body of evidence (BOE) for NIST (RMF) controls, POA&M’s and DoD (CCI’s)
* Work with lead specialist for the implementation of the NIST 18 control family Policy and Procedures required for A&A.

**GDIT**

**3170 Fairview Park Dr, Falls Church, VA · 22042 (703) 641-2000**

**Information Assurance Engineer**

**May 2019 – 11/1/2019**

* To support **Authorizing Official Designated Representative**, **Enterprise Architect** and **Operation Manager** in provisioning of the Governance, Risk and Compliance assurance accuracy and completion.
* To perform **Subject Matter Expert** duties, **Department Transportation Safety Board** on IT Security issues. These matters would cover various issues pertaining FISMA requirements.
* To work with **Authorizing Official Designated Representative** in the creation of the Agency Security Policy.
* To work with **Authorizing Official Designated Representative** in the planning and the support for all systems requiring Assessment and Authorization.

**N-Link**

**550 NW Franklin Ave**

**Bend, OR 97701 (541) 617-0011**

**Senior Information Analysis**

**January 2018 – May 2019**

**Top Secret**

**Responsibility:**

* To support Senior Information Security Officer and Operation Manager in provisioning of the Governance, Risk and Compliance assurance accuracy and completion.
* To perform **Subject Matter Expert** duties, **Department of Commerce** on IT Security issues. These matters would cover various issues pertaining FISMA requirements.
* To work with Chief Information Security Officer in support of Annual Cyber Security Awareness training for all government and contract personnel as a requirement.
* To work with Chief Security Information Officer in the creation of the Agency Security Policy.
* To utilize **CSAM** management tool as a repository for body of evidence (BOE) for NIST (RMF) controls, POA&M’s.
* To work with Chief Information Security Officer in the planning and the support for all systems requiring Assessment and Authorization.

**Info Reliance**

**4050 Legato Rd Fairfax VA**

**703-246-0360**

**Senior Security Engineer**

**Oct. 2017 – November 30, 2017**

**Top Secret/SCI**

**Responsibilities:**

* To perform **Subject Matter Expert** duties for federal agency, **Department Homeland Security** on IT Security issues. These matters would cover various issues pertaining CNSS and FISMA requirements, physical and logical.

**General Dynamics**

**3170 Fairview Park Dr, Falls Church, VA · (703) 641-2000**

**Senior Principal Security Analyst**

**Oct 2016 – September 7, 2017**

**Top Secret/SCI**

**Responsibilities:**

* Providing technical knowledge and support to system owner and program manager for systems that we are responsible, performing completion of A&A documentation process and the System Development Life Cycle (SDLC).
* To continue support through the system self-assessment process following the agency requirements, and the change from DIACAP to Risk Management Framework (RMF).
* To analyze and support staff in the Nessus Security scanning and compliance process and the DISA (STIG) process, meeting the NIST 800-53v4, CM-6 requirements.
* Responsible for ensuring the implementation and maintenance of security controls in accordance with the SSP of all systems designated.
* Review system control requirement accordingly to system categorization implementation obtained by DIACAP & FIPS199/NIST800-60, and FIPS200/NIST800-53v4, 800-30,800-34, 800-37, 800-39, 800-59, 800-61, 800-64, 800-137; review standard operating procedures maintain by agency NIST and STIGS for Compliance and benchmark aim at services and systems.
* To support the risk assessment and re-assessment as required for any significate changes and formally notified ISSM/AO when changes occur that might affect accreditation.
* Review documentation to include System Security Plans (SSPs), Risk Assessment Reports, Accreditation and Authorization (A&A) packages.
* To utilize **eMass** and **Xacta** management tool as a repository for body of evidence (BOE) for NIST (RMF) controls, POA&M’s and DoD (CCI’s)
* To perform duties in supporting the deployment to the cloud infrastructure.

**SecureStrux, LLC**

**July 2016 – Oct 2016**

**Security Control Assessor**

**Contractor DOD**

**Top Secret**

**Responsibilities/Accomplishments:**

* Providing technical knowledge and support to system owner and program manager for systems that we are responsible, performing completion of A&A documentation process and the System Development Life Cycle (SDLC).
* To continue support through the system self-assessment process following the agency requirements, Risk Management Framework (RMF).
* Responsible for ensuring the implementation and maintenance of security controls in accordance with the SSP of all systems designated.
* To follow internal policy requirements doing an incident, notifying information security staff and SOC.
* Review system control requirement accordingly to system categorization implementation obtained by DIACAP & FIPS199/NIST800-60, and FIPS200/NIST800-53v3&v4; review standard operating procedures maintain by agency NIST and STIGS for various operating system platforms.
* To support the risk assessment and re-assessment as required for an significate changes and formally notified ISSM/AO when changes occur that might affect accreditation.
* To utilize **eMass** and **Xacta** management tool as a repository for body of evidence (BOE) for NIST (RMF) controls, POA&M’s and DoD (CCI’s)
* Review documentation to include System Security Plans (SSPs), Risk Assessment Reports, Accreditation and Authorization (A&A) packages

**Sun Management**

**March 2016 – June 2016**

**Resident Deployment Engineer**

**Responsibilities/Accomplishments:**

To support the deployment of Palo Alto devices in the Health Human Services entire agency. This would include all required components for the networking infrastructure (Firewall, Central Management, Logging apparatus) to each sub agencies.

**SSI, LLC, December 2015 – February 12, 2016**

**Dept. of Commerce (Contractor)**

**Cybersecurity/Information Engineer**

**Secret Clearance:**

**1534 Dunwoody Village pkwy, suite 100, Atlantic, GA 30338**

**Mr. Keith Cornegay, Tel: 7703993000**

**Responsibilities/Accomplishments:**

* Requirements and responsibilities were performed in a cloud environment and provided by a major CSP. Primary function to perform assessment for IT system controls during ATO renewal/new. Serve as the principle advisor to the System Owner, Business Process Owner and the Task Manager on all matters, technical and otherwise, involving the security of an information system.
* Providing technical knowledge and support to system owner and program manager for systems that we are responsible, performing completion of C&A documentation process and the System Development Life Cycle (SDLC).
* To continue support through the system self-assessment process following the agency requirements, Risk Management Framework (RMF).
* Responsible for ensuring the implementation and maintenance of security controls in accordance with the SSP of all systems designated.
* Review system control requirement accordingly to system categorization implementation obtained by FIPS199/NIST800-60, and FIPS200/NIST800-53v3&v4; review standard operating procedures maintain by agency NIST and STIGS for various operating system platforms.
* To assist and provide support in the development of the System Security Plan and Contingency Plan for systems which are designated.
* To support the risk assessment and re-assessment as required for any significate changes and formally notified ISSM/AO when changes occur that might affect accreditation.
* Review documentation to include System Security Plans (SSPs), Risk Assessment Reports, Certification and Accreditation (C&A) packages
* To review and implement (FedRamp) A&A package within the AWS environment and services at various levels (IaaS, PaaS and SaaS).
* Review reporting results from scanning application Nessus, Web and communicate with system owners to verify the completion of findings.

**FEMA Computer Technology Consultant, September 2015 – October 2015**

**Top Secret**

**7404 EXECUTIVE PL STE 225**

**LANHAM, MD 20706**

**240-547-0076**

**Lead Security Engineer**

**Responsibilities/Accomplishments:**

Security team lead amongst a group of four teams leads for the FEMA agency throughout the USA deployment. Primary assignment was to perform IA function during and after deployment of present and new devices. Was not able meet FEMA security requirement after 7-week assignment at Washington, D.C. location.

**Provideo, LLC June 23, 2015 – July 31, 2015**

**Dept. Health Human Service (Contractor)**

**Position: Information Assurance Engineer**

**Secret Clearance:**

**21740 Beaumeade Circle, Suite 148, Ashburn, VA 20147**

**Bob Hass Tel:703.625.7776**

**Responsibilities/Accomplishments:**

* Perform system security assessment and system security testing on assign systems.
* To create system documentation for all system ATO both new and existing, the documentation would include all artifacts required for System Control Assessment (SCA) and the FISMA and RMF requirements.
* Conduct vulnerability assessments on networks, servers, websites, databases, and assist with other assessment activities.
* Plan and perform security controls assessments in accordance with NIST SP 800-53A, to include interviews, examinations, and vulnerability testing.
* Identify organizational security weaknesses in personnel controls, training, incident and emergency response, logical security controls, physical security controls, operational security and with the integrity of software applications and data.
* Utilize Nmap, Netcat, Nipper Studio, Microsoft Baseline Security Analyzer, Tenable Nessus, Security Center, Wireshark, Core Impact, IBM Appscan Standard, Burp Suite Professional, Application Security AppDetective Pro, HP WebInspect.
* Providing technical knowledge and support to system owner and program manager for systems that we are responsible, performing completion of C&A documentation process and the System Development Life Cycle (SDLC).
* To follow internal policy requirements doing an incident, notifying information security staff and SOC.
* To assist and provide support in the development of the System Security Plan and Contingency Plan for systems which are designated
* To support the risk assessment and re-assessment as required for any significate changes and formally notified ISSM/AO when changes occur that might affect accreditation.
* To continue support through the system self-assessment process following the agency requirements, Risk Management Framework (RMF).
* The following documents were used for both implementation and clarification.
* To perform and review report resulting from various scanning application Nessus, Web Inspect, Appdective, Nmap, Foundstone, communicate with system owners to verify the completion of findings.
* Confirm and provide assurance in support Health Insurance Portability Accountability Act (HIPAA) for all systems assigned by Health and Human Services.
* Review documentation to include System Security Plans (SSPs), Risk Assessment Reports, Certification and Accreditation (C&A) packages

**SusanCousines, LLC April 2015 – June 3, 2015**

**FDA (Contractor)**

**Position: Information Security Engineer**

**Secret Clearance:**

**5100 Paint Branch Parkway, College Park, MD 20740**

**Mr. Edward**

**Responsibilities/Accomplishments:**

* Serve as the principle advisor to the System Owner, Business Process Owner and the Task Manager on all matters, technical and otherwise, involving the security of an information system.
* Responsible for ensuring the implementation and maintenance of security controls in accordance with the SSP of all systems designated.
* To follow internal policy requirements doing an incident, notifying information security staff and SOC.
* To assist and provide support in the development of the System Security Plan and Contingency Plan for systems which are designated Providing technical knowledge and support to system owner and program manager for systems that we are responsible, performing completion of C&A documentation process and the System Development Life Cycle (SDLC).
* To support the risk assessment and re-assessment as required for any significate changes and formally notified ISSM/AO when changes occur that might affect accreditation.
* To continue support through the system self-assessment process following the agency requirements, Risk Management Framework (RMF).
* Provide guidance oversight, expertise and develop security documents or implement any security controls. Perform vulnerability assessment on assign systems.
* To follow internal policy requirements doing an incident, notifying information security staff and SOC.
* Confirm and provide assurance in support Health Insurance Portability Accountability Act (HIPAA) for all systems assigned by Federal Drug Administration.
* Review documentation to include System Security Plans (SSPs), Risk Assessment Reports, Certification and Accreditation (C&A) packages

**Phacil, INC., October 2014 – January 2015**

**Dept. of Education (Contractor)**

**Position Title: Information Assurance Analysis**

**Secret Clearance:**

**800 N Glebe Rd, #700, Arlington, VA 22203**

**Mr. Naveed Tel:703. 526.1800**

**Responsibilities/Accomplishments:**

* Life Cycle (SDLC).
* To support the risk assessment and re-assessment as required for any significate changes and formally notified ISSM/AO when changes occur that might affect accreditation
* To review the risk assessment and re-assessment as required for any significate changes and provide independent analysis.
* Review documentation to include System Security Plans (SSPs), Risk Assessment Reports, Certification and Accreditation (C&A) packages Perform security assessment for Federal Enterprise agency Department of Education, (Major/Minor and GSS) systems, Generating Security Assessment Report/Plan, Risk Management Report, Security Control Assessment, etc.
* To establish presentation slides for each system needing kick-off documentation assessment procedures and time scheduling requirements by system owner, program manager, staff team for each manage system/systems.
* To review system documentation for all system ATO both new and existing, the documentation would include all artifacts required for System Control Assessment (SCA).
* To review and provide support in the development of the System Security Plan and Contingency Plan for systems which are designated Providing technical knowledge and support to system owner and program manager for systems that we are responsible, performing completion of C&A documentation process and the System Development

**General Dynamic, June 2014 – September 2014**

**Disa, Fort Meade (Contractor)**

**Position Title: Principle Analyst, Information Security**

**Top Secret/SCI:**

**3211 Jermantown Road, Fairfax, VA 22030**

**Mr. Salaz Tel:703. 995.8700**

**Responsibilities/Accomplishments:**

* Perform certification and accreditation in support of a family of systems, networks, and sites. Conducting Security Test and Evaluations as required.
* Conducting peer reviews of Certification conducted by other technicians. Review certification and accreditation policies and directives for the DIACAP.
* Assist the Certification Official in the oversight, inspection, review, and accreditation of Information Systems.
* To evaluate the self-assessment of system safeguards and program elements for C&A system.
* To support the risk assessment and re-assessment as required for any significate changes and formally notified ISSM/AO when changes occur that might affect accreditation
* Review documentation to include System Security Plans (SSPs), Risk Assessment Reports, Certification and Accreditation (C&A) packages

**Blue Canopy, LLC, Sept 2013 – Jan. 2014**

**US Capital (Contractor)**

**11091 Sunset Hills Road, Suite 777, Reston, VA 20190**

**Mr. Riddick Tel: 703.896.4000**

**Position Title: Senior Information Assurance Analyst**

* Perform Security Program Evaluation of the General Support System (GSS) Network Segment, Active Directory (AD) implementation, and various Financial Systems in support of multiple certification and authorization.
* To review Oracle HR database and confirm security requirements were mitigated and all default authentication are being mitigated.
* To assist and provide support in the development of the System Security Plan and Contingency Plan for systems which are designated.
* To continue support through the system self-assessment process following the agency requirements, Risk Management Framework (RMF).
* To support the risk assessment and re-assessment as required for any significate changes and formally notified ISSM/AO when changes occur that might affect accreditation
* Evaluated systems, networks, sites for compliance to Information Security standards and policies.
* Review documentation to include System Security Plans (SSPs), Risk Assessment Reports, Certification and Accreditation (C&A) packages

**HTA, Jan 2013 – Apr 2013**

**Dept. of Justice (Contractor)**

**30 South Wacker Drive, 22nd Floor Chicago, IL 60606,** **Tel:312-466-5728**

**Top Secret/SCI:**

**Information System Security Representative**

* Edited, created, reviewed and evaluated System Security Plans, System Security Authorization Agreements, systems and network diagrams, Security Requirements Traceability Matrices, Risk Assessments, and Associated Information Systems Certification and Accreditation (C&A) documents in accordance with Intelligence Community, National and Agency standards Observed, evaluated, and documented IS security certification testing and prepared Security Certification Test Reports (SCTRs) with findings and recommendations regarding systems' certifications.
* To assist and provide support in the development of the System Security Plan and Contingency Plan for systems which are designated.
* To continue support through the system self-assessment process following the agency requirements, Risk Management Framework (RMF).
* Advise the system owner regarding security considerations in applications systems procurement or development, implementation, operation and maintenance, and disposal activities.
* Assist in the determination of an appropriate level of security commensurate with the impact level
* Assist in the development and maintenance of system security plans and contingency plans for all systems under their responsibility
* To support the risk assessment and re-assessment as required for any significate changes and formally notified ISSM/AO when changes occur that might affect accreditation
* Evaluated systems, networks, sites for compliance to Information Security standards and policies.
* Review documentation to include System Security Plans (SSPs), Risk Assessment Reports, Certification and Accreditation (C&A) packages

**AAC Inc., Nov. 2011 – September. 2012**

**Federal Communication Commission (Contractor)**

**8470 Tyco Rd, Vienna, VA 22182, Tel: 703-918-6300**

**Position Title: Lead Security Engineer**

* Lead computer security operations engineer performing product evaluation, selection and procurement in Federal government context.
* To utilized various security monitoring applications SIEM, Packet Analyzer, Flow Analyzer, enCase. To performed malware analysis and forensic investigations.
* To maintained firewalls, IDS/IPS and VPNs. Led incident response activities.

**Secure Mission Solutions, Sept 2011 – Nov 2011**

**DOD, Fort Belvoir (Contractor)**

**5875 Trinity Parkway, Suite 300 Centreville, Virginia 20120**

**Top Secret:** 703-988-8500

**Position Title: Information Assurance Analyst**

* Performed System Test and Evaluation (ST&E) activities on a variety of hardware and software systems (Windows, UNIX and Cisco IOS) using the latest Navy-approved vulnerability scanning tools (eye Retina, Nmap, Windows Production Gold Disk and DISA Security Readiness Review (SRR) scripts.
* Write C&A documents per DIACAP and Navy Afloat PIT standards, including System Security Plans (SSPs), Risk Assessment (RA) Plans, Plans of Actions and Milestones (POA&M), Security Test and Evaluation (ST&E) Plans, and Contingency Plans (CP. Review Army Information Regulation documentation AR-1 and AR-2.
* To assist and provide support in the development of the System Security Plan and Contingency Plan for systems which are designated
* To support the risk assessment and re-assessment as required for any significate changes and formally notified ISSM/AO when changes occur that might affect accreditation

**KCG, Jan. 2011 – Mar. 2011**

**Transportation Security Administration (Contractor)**

**11710 Plaza America Dr, Reston, VA 20190**

**Secret:**

**2000 Edmund Halley Drive, Suite 500, Reston, VA 20191**

**Tel: 703. 467.2000**

**Position Title: Information System Security Officer**

* Developed and maintained overall system security documentation, Information System Security Plan (SSP), which contained all necessary security procedures, instructions, operating plans and guidance.
* Participated in the development or revision of System-specific security safeguards and local operating procedures that are based on the above regulations.
* Providing technical knowledge and support to system owner and program manager for systems that we are responsible, performing completion of C&A documentation process and the System Development Life Cycle (SDLC).
* To continue support through the system self-assessment process following the agency requirements Risk Management Framework (RMF).
* To assist and provide support in the development of the System Security Plan and Contingency Plan for systems which are designated
* To support the risk assessment and re-assessment as required for any significate changes and formally notified ISSM/AO when changes occur that might affect accreditation
* To follow internal requirements doing an incident, notifying information security staff and SOC as required.
* Ensuring Configuration Management (CM) for security-related IS software, hardware, and firmware is maintained and documented.
* Advise the system owner regarding security considerations in applications systems procurement or development, implementation, operation and maintenance, and disposal activities.
* Assist in the determination of an appropriate level of security commensurate with the impact level
* Assist in the development and maintenance of system security plans and contingency plans for all systems under their responsibility
* Prepare and review documentation to include System Security Plans (SSPs), Risk Assessment Reports, Certification and Accreditation (C&A) packages

**Skypoint Decisions, Inc., Apr. 2010 – Oct. 2010**

**Department of State (Contractor)**

**45240 Business Court, Suite 160, Dulles, VA 20166**

**Top Secret:**

**Tel: 703.234.7880**

**Position: Senior Firewall Engineer**

* Supported the building and testing the Firewall / PKI / DMZ infrastructure in sustaining the consolidation and the client’s IT Security Architecture.
* To maintained Network Stateful and Application Firewall technologies (Stonegate, Sidewinder G2).

**Verisolv Technologies, Jan. 2008 – Sept. 2009**

**Veterans Administration (Contractor)**

**2035 Headlands Cir, Reston, VA 20191**

**Position Title: Senior Security Engineer**

* To perform Security Engineer with the Project Management Office team for Veterans Affairs Agency to meet OMB mandate June 2008, IPv6 compliant.
* Reviewed Veterans Affairs security handbook and verify IPv6 testing meets internal agency policies requirements and National Institute Standards Technology guideline, policies, and standards.

**AETEA Information Technology, May 2006 – Aug 2007**

**Department of Transportation**

**1445 Research Blvd. Suite 210, Rockville, MD 20850**

**Mr. Tercy Tel: 301.721.4200**

**Position Title: Security Engineer**

* Worked with the security design group on the design of the enterprise infrastructure and deployed network security devices as requested by customer.
* Deployment of Cisco (FWSM) and Checkpoint Firewalls
* In support maintaining requirements for NIST 800 series for, 800-30 for Risk Management, 800-34 for Contingency Planning, 800-37 NIST 800-53v2 Security Minimal Baseline Requirements, NIST 800-53Av1 Security Baseline

**Sprint, Aug 2005 – May 2006**

**12524 Sunrise Valley Dr Reston VA 20191**

**Position Title: Firewall Security Engineer**

* Performed administration, maintained and monitored security RSA accounts on ACE server.
* Maintained and performed administration duties for users on LDAP server.
* Worked on administration, configuration and troubleshooting of issues on Checkpoint, Cisco Pix firewall, Netscreen and Raptor firewall.

**DC Fire Department, Apr 2004 – Aug 2005**

**2000 14th Street, NW, 500, Washington, DC 20009**

**Position Title: Network Engineer**

* Designed, planned, configured, updated and maintained the network and information systems to ensure the 24-hour per day, 7 days per week availability required to support the Department's mission-critical service delivery operations.

**DC General Hospital, Feb 1984 – May 2002**

**1900 Mass. Ave. SE, Washington, DC, Closed**

**Position Title: Supervisor Biomedical/ System Engineer**

* To Assisted in the Planning and Formulation of an effective patient medical information program by researching material, equipment manuals and brochures, medical equipment repair and concepts.
* Worked directly with Chief Biomedical Engineer and presented plans of operations, to include techniques, scheduled preventive major damage and down time of equipment.
* Confirm and provide assurance in support Health Insurance Portability Accountability Act (HIPAA) and District of Columbia Regulatory Agency (DCRA) for all medical devices with DC General Hospital.