

**ANNETTE WILLIAMS**

Candidate’s Legal Name: Annette Williams

Resource Title: Senior IA Consultant

Status Citizen/Visa: US Citizen

Clearance Type: DoD TS w/SCI eligibility, DHS EOD (Adj. 2/1/13)

Availability: Immediately

Summary of Skills / Fit: Over 10 years of experience as a Sr. Information Assurance Specialist and Senior Information Security engineer. Expertise at providing oversight and managing the facilitation of information security risk assessments and mitigation practices. Highly skilled at creating and maintaining Security Authorization Packages to include: Systems Security Plan (SSP), Contingency Plan (CP), Risk Assessment Reports (RAR), Security Assessment Reports (SAR), Plan of Action and Milestones (POA&M). CAP – Certified Authorization Professional. CISSP - Certified Information System Security Professional - (in progress), MCP, MCSE - Microsoft Certified System Engineer, CCNA - Cisco Certified Network Associate

**ANNETTE WILLIAMS**

**SUMMARY**

* Over 10 years of experience as a Sr. Information Assurance Specialist and Senior Information Security engineer
* Expertise at providing oversight and managing the facilitation of information security risk assessments and mitigation practices
* Proficient at conducting Assessment and Authorization (A&A) of an organization’s information systems and applications with a goal of achieving compliance
* Highly skilled at creating and maintaining Security Authorization Packages to include: Systems Security Plan (SSP), Contingency Plan (CP), Risk Assessment Reports (RAR), Security Assessment Reports (SAR), Plan of Action and Milestones (POA&M)
* Strong experience performing continuous monitoring activities on each system, ensuring it is compliant with FISMA and the organizational requirements
* Well-versed at performing security impact analysis prior to implementing changes to the information systems hardware, software, or configuration and providing system owners an analysis of impacted security controls and risk to the information systems security posture
* Expertise at reviewing, interpreting, and analyzing vulnerability/compliance scans to verify and validate changes, identify weaknesses and deficiencies, and ensure intended changes to the information system are operating as intended
* Proficient at recommending a plan of action to mitigate all weaknesses and vulnerabilities identified in the information system or application
* Skilled at providing management with regular reports on the activities and security posture of the information systems
* Successfully monitors and tracks all phases of projects and assessment, and performs QA of security packages before submission to Authorizing Official for ATO
* DoD TS w/SCI eligibility, DHS EOD (Adj. 2/1/13)

**CERTIFICATIONS**

* CAP – Certified Authorization Professional
* CISSP - Certified Information System Security Professional - (in progress)
* MCP, MCSE - Microsoft Certified System Engineer
* CCNA - Cisco Certified Network Associate

**TECHNICAL SKILLS**

* CSAM
* Tenable Nessus
* Trusted Agent Fisma Tool (TAFT)
* Resource Management System (RMS)
* AppDetective

**TECHNICAL EXPERIENCE**

**NCI, Inc. / FCC - Federal Communications Commission, Washington, DC 10/2014 - Present**

***Sr. Information Assurance Specialist***

As a Sr. Information Assurance Specialist, responsible for the Assessment and Authorization of all FCC’s information systems.

* Works closely with management and engineers in the planning and implementation of migrating their physical network to cloud/virtual.
* Ensures security is implemented in every aspect of the development and building of the network
* Ensures all connections are encrypted using FIPS 140-2 compliant protocols
* Ensures all servers, routers, and switches are configured according to NIST and the agencies requirements
* Requires scan be performed on all hardware/software for vulnerabilities and deficiencies, then analyzes the scans, informs management of results, and recommends plan of action and milestones for remediation
* Develops all documents, including Risk Assessments (RA), System Security Plan (SSP), Contingency Plan (CP), Plan of Action and Milestones (POA&M), FIPS 199, PTA, PIA, E-Authentication to obtain Authority To Operate (ATO)
* Performs continuous monitoring, and provides management with reports concerning the security posture of their information systems and applications.

**Engility/Kforce, LLC, Washington, DC 11/2013 – 08/2014**

**Department of Commerce - International Trade Administration (ITA)**

***Sr. Assurance Specialist (InfoSec)***

As a Sr. Information Assurance Specialist, responsible for the assessment and certification of ITA’s Next Generation Network (NGN), Infrastructure as a Service (IaaS), migration to the cloud.

* Worked closely with management and engineers in the planning and implementation of migrating their physical network to cloud/virtual
* Ensured all transmission were encrypted using FIPS 140-2 compliant protocols
* Ensured all servers, routers, switches, checkpoints were configured using FISMA compliant and organizational required approved baselines
* Performed vulnerability and compliance scanning on all devices and applications, then reviewed and analyzed scans and made recommendations to the system owner or engineers for remediation strategies to correct any deficiency
* Created and updated all system security documents in reference to the security assessment package, including System Security Plan (SSP), Contingency Plan (CP), Plan of Action and Milestones (POA&M), Security Assessment Report (SAR), Risk Assessment Report (RAR), FIPS 199, Privacy documents if required (PTA), PIA, and E-Authentication
* Performed continuous monitoring of the security packages to ensure an annual re-authorization was received
* Maintained all SAP documentation on SharePoint and in CSAM.

**Missing Link Security/Sure Secure Solutions, Alexandria, VA 02/2013 – 09/2013**

**Department of Commerce - US Patent and Trade Office (USPTO)**

***Sr. Cyber Security Analyst***

As a Sr. Security Analyst, was responsible for daily continuous monitoring of all financial systems, ensuring all security control requirements were met to protect the confidentiality, integrity, and availability of the information systems and applications.

* Prepared all Assessment and Authorization packages to include the following major deliverables: System Security Plan (SSP), Security Test and Evaluation (ST&E), Plan of Action and Milestone (POA&M), and Contingency Plans (CP), Privacy Analysis (PTA), and annual system assessments
* Coordinated with the technical leads and the system owner to determine system categorization and information types using FIPS 199
* Assessed the system or application using NIST 800-53 r3 controls
* Tracked vulnerabilities and weaknesses in POA&Ms, and verified and validated all artifacts used as supporting evidence in POA&M closure
* Reviewed and monitored logs, accounts, SDLC documentation
* Maintained a current inventory of all hardware and software assets on each system in the organization
* Maintained and updated system SDLC documentation
* Conducted Risk Assessments, ran vulnerability scans on systems using the Nessus scanning tool
* Conducted and advised in meetings with management concerning the security posture of the information systems, provided recommendations and guidance when assisting in audits or annual assessments, and provided input in mitigating weaknesses and vulnerabilities
* Maintained all system documentation and artifacts on the SharePoint repository and CSAM.

**AMDEX/Sure Secure Solutions, Alexandria, VA 03/2012 – 01/2013**

**Department of Homeland Security - Customs and Border Protection**

***Information System Security Officer***

Responsible for performing Assessment and Authorization (A&A) for the Customs and Border Protection (CBP) general support systems and major applications, including Virtualization Servers, UNIX Servers, and Windows Servers. Provided support for all application systems supporting SQL, Oracle, SANS in obtaining an Authorization to Operate (ATO).

* Prepared all Assessment and Authorization packages to include the following major deliverables: System Security Plan (SSP), Security Test and Evaluation (ST&E), Plan of Action and Milestone (POA&M), and Contingency Plans (CP), Privacy Analysis (PTA), and annual system assessments
* Coordinated with the Engineering team, System Owner, Certifying Agent and the CISO to determine system categorization and information types using FIPS 199
* Assessed the system or application using NIST 800-53 r3 controls
* Verified and validated artifact for POA&M closure or control evidence
* Reviewed and monitored logs, accounts, SDLC documentation
* Developed and maintained a current inventory of all hardware and software assets on each system in the organization
* Conducted Risk Assessments, ran vulnerability scans on systems using the Nessus scanning tool
* Tracked all weaknesses in POA&Ms until remediated
* Tracked weakness and vulnerabilities found in Nessus scans, or via security advisories or vender to apply the necessary plugins to correct or remediate the weakness
* Used the Nessus reporting tool to produce a report identifying the risk levels (High, Moderate or Low), and recommended solution for resolution
* Provided configuration management reviews prior to approving/disapproving any application coding or system configuration changes to ensure all policies and procedures were followed and vetted through the Configuration Management Board
* Ensured that proposed changes did not adversely affect or impact the security posture of the information system negatively
* Ensured all documents and artifacts associated with the A&A packages were complete and uploaded into Trusted Agent FISMA (TAF) Tool and RMS repositories.

**IBM/Base Technologies, Inc., Springfield, VA 12/2008 – 02/2012**

**Department of Homeland Security - Customs and Border Protection**

***Information System Security Officer (ISSO)***

Responsible for performing Assessment and Authorization (A&A) for the Customs and Border Protection (CBP) general support systems and major applications, including Virtualization Servers, UNIX Servers, Windows Servers.

* Provided support for all application systems supporting SQL, Oracle, SANS to obtain an Authorization to Operate (ATO) for the systems
* Performed Assessment and Authorization (A&A) for the Customs and Border Protection (CBP) general support systems and major applications, including Virtualization Servers, UNIX Servers, and Windows Servers
* Provided support for all application systems supporting SQL, Oracle, SANS to obtain an Authorization to Operate (ATO)
* Prepared all Assessment and Authorization packages to include the following major deliverables: System Security Plan (SSP), Security Test and Evaluation (ST&E), Plan of Action and Milestone (POA&M), and Contingency Plans (CP), Privacy Analysis (PTA), and annual system assessments
* Coordinated with the Engineering team, System Owner, Certifying Agent, and the CISO to determine system categorization and information types using FIPS 199
* Assessed the system or application using NIST 800-53 r3 controls
* Verified and validated artifact for POA&M closure or control evidence
* Reviewed and monitored logs, accounts, SDLC documentation
* Developed and maintained a current inventory of all hardware and software assets on each system in the organization
* Conducted Risk Assessments, ran vulnerability scans on systems using the Nessus scanning tool
* Tracked all weaknesses in POA&Ms until remediated
* Tracked weakness and vulnerabilities found in Nessus scans, or via security advisories or vender to apply the necessary plugins to correct or remediate the weakness
* Used the Nessus reporting tool to produce a report identifying the risk levels (High, Moderate or Low), and recommended solution for resolution
* Provided configuration management reviews prior to approving/disapproving any application coding or system configuration changes to ensure all policies and procedures were followed and vetted through the Configuration Management Board
* Ensured that proposed changes did not adversely affect or impact the security posture of the information system negatively
* Ensured all documents, artifacts associated with the A&A packages were complete and uploaded into Trusted Agent FISMA (TAF) Tool and RMS repositories.

**Bearing Point, Inc., Suitland, MD 09/2008 – 12/2008**

**US Bureau of Census**

***Sr. Information Assurance Consultant (ISSO)***

As an ISSO, performed C&A for multiple Major Applications (MA) and General Support Systems (GSS).

* Performed the C&A process on all systems and applications using the NIST 800-37 guidelines; after completing C&A package and obtaining an ATO, continuous monitoring was performed
* Performed monthly scanning, reviewed and analyzed scans, made recommendations to the system owners on solutions to remediate and correct the weaknesses
* Provided briefings and presentations to management on the overall security posture of the organization’s information systems, and recommended resolutions to implement the necessary security controls to protect the applications and/or information systems
* Managed a team of security engineers ensure to all necessary patching was implemented
* Maintained and uploaded all documentation to the organization’s repository Trusted Agent FISMA Tool (TAFT) and RMS.

**Kforce/STG, Inc., Reston, VA 10/2007 – 08/2008**

**Department of Veterans Affairs**

***Sr. Network Security Engineer***

Performed the Certification and Accreditation of the organization’s general support systems and major applications

* Developed, reviewed, and updated all system documentation relative to the C&A process
* Performed testing and verification of all security controls to determine their effectiveness, and verified they were protecting the information systems and applications as intended
* Performed scans of the information systems, analyzed scans, and made recommendations to management for remediation of weaknesses found
* Created presentations for management detailing the security posture of the information systems and applications
* Performed continuous reviews and updates to the System Security Plans, Contingency Plan, POA&Ms, and all documentation was maintained on the organizations SharePoint repository.

**Lockheed Martin / DCR, Washington, DC 07/2005 – 102007**

**Federal Aviation Administration (FAA)**

***Sr. Network Engineer/Security Engineer***

Performed Certification and Accreditation for all of FAA’s Major Applications and General Systems using FISMA guidelines. Assessments were administered following the NIST 800-37 C&A process and assessing the information systems following the 800-53A, as well as FIPS199 for system categorization.

* Maintained a close working relationship with the Business/System Owner
* Updated and verified information relevant to compiling the authorization package to ATO
* Reviewed scan results and findings to determine all areas of system vulnerabilities, sensitivity levels, and overall exposure to threats and weaknesses
* Developed POA&M reports from findings and recommended corrective actions to System Owners for remediation
* Assessments were completed using the following guidelines: FIPS 199, NIST 800-53rev3, 800-53A, 800-37, 800-30, 800-34.

**Siemens Government Services, Washington, DC 10/1999 – 06/2005**

**Department of Homeland Security - Immigrations and Customs Enforcement**

***Sr. Network Engineer***

As Sr. Network Engineer, worked as a Team Lead to configure, troubleshooting, and monitor the Department of Homeland Security (ICE) WAN/LAN

* onfigured, installed, troubleshot, and resolved all WAN connectivity issues to ensure network stayed operational
* Configured interfaces using the following protocols: TCP/IP, frame-relay, ATM, RIP, OSPF on T1, T3, ISDN circuits
* Used monitoring tools, HP Openview, Cisco Works, ProactiveNet to improve network performance issues
* Worked on LAN configuring and troubleshot servers, workstations, laptops, printers, hubs, and ensured LAN stayed operational; WAN/LAN consisted of 2500 nodes and approximately 20,000 users
* Configured, troubleshot Cisco 7200, 2600, 2500 routers and Catalyst switches
* Troubleshot servers in Windows/Novell LAN/WAN environment
* Troubleshot, resolved connectivity issues with Telco’s T1, T3, OC3/12, ISDN, Frame Relay, ATM, circuits
* Monitored network using Enterprise Tools; HP Openview, and CiscoWorks
* Used Remedy problems tracking system to track all problems
* Served as a Team Lead for Change Management Group
* Responsible for IOS upgrades and password recovery on Cisco routers/switches
* Managed Vlan, spanning tree, port security to ensure network security is effective
* Acted as Administrator for Novell Netware and Windows NT/2003 servers, and for Exchange Mail servers
* Remotely troubleshot routers, switches, and servers
* Made recommendations for corrective measures for improvement of network performance
* Configured DNS, WINS and proxies for connectivity of users to Internet
* Installed server patches/upgrades
* Created/deleted user accounts, profiles, groups, mail
* Administrator for Proactive Net Tools and HP Openview.

**Getronics Government Solutions, LLC, Washington, DC 06/1997 – 09/1999**

**Department of Commerce**

***Sr. Systems Analyst***

Responsible for the configuration and management of the network routers, switches, and servers connecting to the Dept. of Commerce LAN/WAN. Duties included the migration of Banyan Vines to Windows NT installation, configuration of Windows NT, Banyan Vines servers.

* Performed work as a Network Administrator for Windows NT, Banyan Vines, and Lotus Notes
* Added/deleted user accounts and mail accounts, managed profiles, installed print servers, configured PCs, laptops, and servers
* Performed backup/recovery of all files and data
* Added/deleted and managed user accounts and profiles
* Created and managed mail accounts
* Ghosted workstations, transferred and reconfigured all users for migration
* Managed over 1100 node network with 15000 users
* Installed NIC cards, printers, workstations, servers.

**Department of the Army, Washington, DC 09/1980 – 09/1997**

**Director of Information Management**

***Computer Specialist***

Responsible for the design, planning, and architecture of the Cabletron/Cisco based network using Banyan Vines and Windows NT servers

* Provided support as Network Administrator, managed user accounts, mail accounts, and installed and inventoried all network applications and licenses
* Troubleshot all network LAN/WAN problems with routers, servers, hubs, switches, cables, and software
* Conducted site surveys for upcoming LAN connectivity to the ordering of the equipment, coordinated circuit installation with the Telco, and installed PCs until customer was operational

Technical Environment: Cisco routers/switches, hubs, csu/ds, Windows NT/2000, Novell Netware servers, TCP/IP, IPX/SPX, ATM, Frame Relay, OSPF, EIGRP, RIP, T1, T3, ISDN, OC3/12, Ethernet, Fast Ethernet, Cisco Works, Remedy, HP Openview, Proactive Net Tools