Lead Cyber Security Analyst Lead Cyber Security Analyst Lead Cyber Security Analyst - SPAWAR Philadelphia Navy Yard Beaufort, SC Work Experience Lead Cyber Security Analyst SPAWAR Philadelphia Navy Yard June 2019 to Present Contract Lead for OSCedge. Prepare status reports, Technical Reports, POA&M reports, etc. Cyber Security Analyst II - Prepare RMF A&A package documentation IAW DoD/NAVSEA directives on Platform IT (PIT) determination package documentation, System Categorization form, Information System Continuous Monitoring Strategy (ISCM), Security Plan (SP), POA&M reports, Risk assessment Reports (RAR) etc. Ensures that all IACs within the Department of Navy (DON) systems are in compliance with NAVSEAINST 9400.2 guidelines by reviewing CT&E plans and procedures. Test and evaluationprocedures and reporting all findings to required stakeholders. Assess and validate the systems to ensure tha the syste as implemented the approved security control baselines. Act as a trusted agent to the SCA Security Control Assessor. Assessment & Authorization (A&A) Analyst SPAWAR Data Center August 2018 to May 2019 Act as a Certification Agent for the Certifying Authority. Conduct onsite/remote systems assessments on enclaves and programs. Authorization & Accreditation (A&A) Visits at DOD Facilities, within SPAWAR. Support the PM's in securing the equipment and services and infrastructure, validate the IA controls, brief upper management regarding what is expected (In brief) and what has resulted (Out brief) and future strategy. Preparing documentation/artifacts for obtaining an ATO, i.e., SAP, CONOPS, SAR, RAR, POAM's etc. Creating and running ACAS, SCAP and Vulnerator scans and applying remediation or creating POAM's on findings. Create Certification Recommendation Packages that are reviewed by the AO, implemented upon approval. Risk Management Executive (RME), Certification & Assessment Division Defense Information Agency (DISA) October 2013 to May 2018 2210 GS 13 $120,000 IT Specialist (INFOSEC) Team Lead, Certification Authoritative Representative, Security Control Assessor Representative (SCAR), RME/RE52 Ft Meade, MD Assisting Programs in transition from DIACAP to RMF, which involves, the requirements and processes to identify the categories, selection of controls, assessing and validating controls, assign risk and severity and identify the compelling evidence to validate controls. Preparing RMF artifacts to obtain the ATO. Moving forward with the ATO for AO approval.

Act as a Certification Agent for the Certifying Authority. As Team Lead I lead a team of Contractors and conduct onsite/remote visits for enclaves and programs and Authorization & Accreditation (A&A) Visits at DOD Facilities, Agencies and Theatres. Support the PM's in securing the equipment and services and infrastructure, validate the IA controls, brief upper management regarding what is expected (In brief) and what has resulted (Out brief) and future strategy. Create Certification Recommendation Packages that are reviewed by the AO, implemented upon approval. Risk Assessment Management of DoD programs to ID risks on Changes, Extensions, Reciprocity and A&A's. Team Lead on Security Audits on Classified and Unclassified Systems. CONUS/OCONUS Locations. Identify the security of the Confidentiality/Integrity/Availability (CIA) of the Systems. Support the ISSO's in Vulnerability Compliances and preparing Artifacts for the DIACAP Process and transition to the Risk Management Framework (RMF). Validated IA Controls in eMass. Assessed vulnerabilities via VMS through Oct 2015. DISA has transitioned to Assured Compliance Assessment Solution (ACAS) DISA and CONTINUOUS MONITORING (ConMon) REQUIREMENTS CMRS for validation of vulnerabilities since Oct 2015. I review stats from these tools and assess RISK. Perform Risk Assessments and brief the AO on Programs/Systems within the DOD arena. Communication Tasking Orders - Retina Scans, PKI, HBSS, Internal threats - evaluate systems for compliance. Contribute recommendations on existing and new security policies. Utilize Security Technical Implementation Guides (STIGs) and DoD Security Requirements Guides (SRGs during the auditing process. Tool: StigViewer Defense Information Systems Agency (DISA) - MA-PEO IA41 PKI Infrastructure Branch GS 13 2210 IT Specialist INFOSEC - Fort Meade, MD September 2012 to October 2013 Program Lead of Government employees and Contractors regarding PKI Projects that include develop statement of work, acquisition packages, deliverable evaluations, vendor performance, monitoring vulnerabilities and maintaining the schedule for components of Public Key Infrastructure (PKI), and other IA projects as necessary. Ensures the C&A DIACAP package is complete and ATO are issued prior to expiration, ensures that all security processes are in place and follow policy, and that the SSP is properly completed to include a thorough CONOPs. Ensure DOD and DISA security policies, procedures and practices are adhered to and in compliance with IA requirements. Conduct test of Commercial off the Shelf (COTS) and Government off the Shelf (GOTS) information assurance software. Research the applicability of new technological developments in the field to solve problems or meet future needs of the Defense Information Infrastructure. Task Manager of Contractor Activities Prepares and Maintains IMS Schedules in MS Project 2010, and serve as PM regarding various projects. Assists in the preparation of ATO Packages to include artifacts, populating eMass and VMS, and monitoring systems and creating POAMs. Prepare Senior Briefings in the area of Policy, Processes and IT Projects. Maintain Project Schedules utilizing MS Project and other Project Mgmt Tools. NOTE: There was realignment in August 2013. I was temporarily transferred to Cyber Integration Branch, which dealt with Knowledge Management and SharePoint. However, I was working on PKI projects during this period, working the NRRB (NetOps Readiness Review Board) requirement. On Oct 4th, 2013, I was transferred to FSO (Field Security Office), upon my own request. See present Job Description. RDECOM HQ October 2009 to September 2012 Division Chief Governance, Strategy and Enterprise Architecture Division - Aberdeen, MD May 2001 to June 2012 21005 RDECOM Duties/Accomplishments Division Chief (Acting): DETAIL: 120 Days. Guidance and Supervision of the Knowledge Management Staff and Governance, Strategy and Enterprise Division. Staff of seven employees, of which six are federal employees and one, is a contractor. Manage IT Projects, delegate tasks, maintain schedules and advise. IAM: Team Lead in IA Division. Provide guidance and support for the protection of IT systems and enclaves throughout the SubOrgs, to include Classified, Unclassified and SAP programs. Performs tech analysis to secure network operations per AR25-2, JAFAN 6/3, and DODI8510.01. POC for the Information Assurance Organizational Program (OIP) for RDECOM and the Installation Assessment Visits. Conducts site assessments and evaluations for the SAP (Special Access Programs) and Collateral Systems to reduce risk and vulnerabilities throughout the sub orgs of RDECOM. Participates in the development of hardware and software safeguards to reduce risks; and implement audit measures. Run vulnerability scans on workstations and networks. Audit Orgs for Information Assurance and recommend best practices. Runs IA Tools as a part of the Assessment Site Visits. Monitor IA Vulnerabilities thru Inspections and Validation via the DIAG IA Checklist to include Networks, Wireless, Security, Personnel Security awareness, Tempest validation, COOP, etc. Verify CTO's. Maintain and support the C&A of the REDECOM and SubOrg Systems via DIACAP and FISMA. COOP Officer G6: Coordinate, test and perform COOP exercises at alternate sites and DRP exercises. Incident Response Officer: Respond to Security Incidents and follow protocol to investigate and lock down pertinent systems. Enforces DOD, DA, AMC, RDECOM and NETCOM IA regulatory requirements and policies over existing/new HQ RDECOM IT resources. Evaluates and influences the mission definitions for IT/IM systems and system elements for assigned mission areas with regard to the AR IA Regs. Budgetary: Initiates and directs staff studies for IA resource problems or inadequacies. Ensures maximum dollar savings and economies by developing, monitoring, and enforcing cost avoidance or reduction programs within IA programs. Represents the RDECOM at meetings, which impact the IA on the network, for both current and future operations. Represents the RDECOM at symposiums, seminars and conferences where IA support and related matters are the topics of discussion. Serves as the general point of contact for all operations pertaining to IA in the HQs and assigns specific points of contact for individual areas. Presents Briefings to the ARMY CIO's regarding the findings and observations from the Site Visits. Prepared and published the TSP (Tenant Security Plan) for RDECOM HQ - Required IA Validations in all IA areas to include, Risk Assessment, COOP, COMSEC, CONOPS, and PIA etc. Created an Information Assurance Virtual Inspection Process that will decrease the cost to implement the evaluations, without decreasing the value and accuracy of the inspection. Implements and maintains security of the Information Systems to include hardening, testing, security scanning, reporting and security accreditation processes. IT Specialist - Development Directorate of Info Mgt/NETCOM September 2008 to October 2009 410-278-7488 Aberdeen Proving Ground, 21005 NETCOM Duties/Accomplishments Develop, support and acquire applications software programs to meet tech and functional requirements. Developing web pages with Dreamweaver/ColdFusion. Testing Websites/apps and ensuring security controls and OPSEC review. Developing Statistical Reports in Crystal Reports with SQL Server DB's. Developing and maintaining DB's using SQL Server 2005. DBA Admin for Oracle and SQL Server 2005. Ensure that APG automation infrastructure is maintained/operated in a manner that provides availability, confidentiality, and integrity of information. Maintain information technology security and ensure users and resources are protected IAW IA, OPSEC, and appropriate policies and regulations. I ensure web applications are secured with an AKO login. Resolved application and web page issues within 10 working business days of issue occurrence. Small Business Administration - GS12 2210 $78,000 IT Specialist - Network MGR Baltimore, MD August 1998 to September 2008 21201 SBA Duties/Accomplishments Administrator of Windows 2003 Server/Windows XP Pro Network, Windows 2000 for the Baltimore District office and a field office. Maintained functions in AD, to include User/computer administration, user support, group policy, and security templates and monitoring performance. Exchange Administrator with Outlook on the Client workstations. Installed, tested and supported all user workstations. Customer Support/Helpdesk tasks for clients and identified and resolves network, hardware/software conflicts/problems and provides support services and training. Analyze system requirements in response to business requirements and evaluates risks and costs related to systems development, to include Telecommunication systems. Analyzes service logs and identifies system enhancements as well as fine-tuning performance of the systems. We use Track- IT on the LAN, which logs changes, audits, and inventory logs as well. Maintained the backups/restores and our Internet site, which involved security and accessibility. Webmaster for the District's page. I coded in html and Dreamweaver. I used Stellent Content Manager to maintain the Baltimore District Web Page. Analyzed internet usage and functionality. Creates databases, and prepare ad hoc reports and marketing statistics. Security Officer for the Baltimore District. I ensured that security standards, federal policies and procedures are being followed throughout the Baltimore District. I prepared the Risk Assessment Model annually. Ensure that user interface and access to the SBA LAN remotely has security elements, installed within their systems. Ensure that the firewall is functioning and installed at all field offices. Communicate in writing and orally requests from other SBA authorities. Briefings on recommendations to the Systems, based on objectives, user requirements and functional changes. Project Mgr and led a team of contractors in the migration of our field office from Windows 2000 environment to a Windows XP and Exchange 2003 Environment. I led a team of contractors in the upgrade of the workstations and various other devices. Configured and troubleshoot laptops and remote SBA PC's with VPN connections and token authentication. Developed an IT plan that would enable staff to remotely access the LAN, email, both at the main site and at the pilot offices. This plan involved researching technologies, GSA pricing, software/hardware and training needs. I developed various configurations which differed in funds, performance and ease of use for the staff.

I prepared the Budget and prepare cost benefit analysis to evaluate information systems interfaces, processes, requirements that will provide IT solutions. I was the Purchasing Agent for acquiring all IT equipment, as well as Office Equipment. Systems Analyst - Network Mgr Army - Baltimore, MD April 1992 to August 1998 21201 COE - Duties/Accomplishments LAN Administrator for a Novell Network/NT Network. Email administrator with cc:Mail installed on the clients. System Administrator for various Government Oracle-based databases. Developed ad hoc reports utilizing Oracle SQL. Developed and implemented system changes by determining required information needs of all levels of staff. Researched the collection, storage, transmission and usage of data, telecommunication systems and advised supervisors of my recommendations. Recommended, procured and installed hw/sw. Develop proposals for improved and cost efficient automation systems. Annually prepare the ADP budget needs for the Division. Prepare Statements of Work for service contracts for the field office and ensure that the service is acceptable. Prepare cost benefit analysis for various IT scenarios to provide IT solutions throughout the COE. Security Officer for the Baltimore District. Configuration Management of all IT/COMSEC Equipment. Provided customer support/help desk to all levels of staff in the use of word processing, graphics, spreadsheets, databases, and telecommunications, LAN connections, remote access. Installed, configured and tested communication software on the server, laptops and client stations. Project Manager for a Nation-wide Information System, of which I represented our District in MD. It was the REMIS (Real Estate Management Information System). Which involved working on teams to analyze the performance and accuracy of the systems and testing with a sample group of users. I used TimeLine Project Software for this project. I have successfully deployed, installed and maintained this database system with the DBA for the mainframe that the system resides on. I coordinated a REMIS Committee. Committee member of the Network Administrators Committee for Corps of Engineers and a subcommittee member of the Information Resource Management Committee. Volunteer on the Strategic Information Management Plan Committee for Corps of Engineers, Baltimore District to aid in the development of a plan that provides the framework to manage information technology in our District for the next 10 years. I received a Special Act Award. The Corps was in the process of converting to a new database system, which involved everyone in the Division, (CEFMS) Corps of Engineers Financial Management System. I was on several committees that are involved in deploying this system throughout the Corps. Developed RE LAN Training Courses and instructed all levels of staff. Management Information Supervisor Occupational Medicine & Safety - Baltimore City Gov - Baltimore, MD April 1987 to April 1992 21201 OM&S Duties/Accomplishments Supervised a computer staff, to include delegation, scheduling, evaluation and discipline of staff. Interviewed and recommended staff selections. Train operators in the operation of the Systems. Schedule and review all computer operations. Produced ad hoc reports on a daily basis. Developed and implemented database procedures through automation of previous manual operations. Participated in all computer acquisitions and development. Utilized desktop publishing for various reports and presentations. Statistical and report forecasting in the Worker's Compensation area. Was credited with accomplishing multiple tasks on a consistent basis through my ability to find solutions and push myself and my subordinates to succeed. Aided in a migration to a more advanced system, and developed Training sessions that greatly decreased the learning curve. Education National Defense University July 2012 to August 2012 Harford Community College Security May 2008 MS in MIS University of Baltimore 1995 Bachelor's Degree in MIS University of Baltimore 1992 AA Degree in Computer Science Community College of Baltimore 1985

Name: Joyce Ramirez

Email: cwyatt@example.org

Phone: (894)961-1045x66256