Security Analyst/ IT Auditor Security Analyst/IT Auditor Security Analyst/ IT Auditor - Eagle Solutions Landover, MD IT Security Analyst/ IT Auditor- IT Security Analyst/ IT Auditor with 6 years' experience in high impact IT security/audit assignments with specialty in risk assessments, security architectures, Certification and Accreditation (C&A) process including; vulnerabilities of programs, and countermeasures in support of infrastructures following; FISMA, NIST and OMB standards Technical IT skills, in INFOSEC, Firewall, Switches, Routers, CSAM, FISCAM and C&A tests, experience with security information and event management (SIEM) tool, implementation of security standards, policies, procedures, compliance and test procedures. Skilled in SOX assessment and internal control frameworks such as COBIT and FISCAM, Windows servers, Linux, virtual machines (VMware), creating System Security Plans, Cybersecurity, security assessment and Authorization (A&A), vulnerability scanning, penetration testing and payment card industry Security standards, security protocols, software and security architectures, design and implementation of security controls and protocols, including networking concepts and services, such as, VPNs, IPSec, PKI and TCP/IP. Proficiency in the following government regulations and standards: National Institute of Standards and Technology (NIST), Federal Information Security Management Act (FISMA), Gramm Leach Bliley Act (GLBA), HUD Handbook, Sarbanes Oxley (Sox), National Housing Act, etc. Extensive experience with managing client expectations and communicating effectively with senior management and regulatory officials. Experience in managing strategic and/or cross-organizational projects and planning and tracking multiple complex projects or programs. Authorized to work in the US for any employer Work Experience Security Analyst/ IT Auditor Eagle Solutions - Reston, VA January 2010 to Present subcontractor) Reston, VA- .January 2010 - Date Maintain policies, procedures and standards required for information security compliance in accordance with FISMA regulatory mandate (SAR, SSP, SCA, FIPS-199-and NIST SP 800-53) Perform assessments of IT General Controls (ITGC) such as Access Control, Change Management, IT operations, Disaster recovery and Job Scheduling. Provide status briefing on IT security compliance program, plan, develop, finalize, and review key deliverables in each stage of the SA&A process. Execute development of System Security Plans for all applications, access controls and access certification

to network, providing guidance and instruction to system owners on FIPS -199 control -categorization, data types selection and risk framework implementation. Experienced in the selection, implementation, assessment, authorization and monitoring of security controls. Perform system vulnerability scanning and analyze discovered infrastructure and software vulnerabilities to determine risk, impact and remediation strategies. Maintain Security compliance activities including client and server patching, endpoint protection, configuration management, and assist with providing documentation on security practices and vulnerability mitigation reports. Perform testing of internal controls under Section 404 of the Sarbanes Oxley Act (SOX) and performing walkthroughs of controls and evaluating operating effectiveness of controls, using applicable frameworks such as FISCAM, COBIT and COSO. Also performed OMB circular A-123 audit. Provide daily, ongoing security oversight of assigned systems as to the security impact of proposed modifications, additions, and technology refresh evolutions via analysis. IT Security Consultant Cowrie Consulting Inc - Las Vegas, NV January 2008 to December 2009 subcontractor) Las Vegas, NV- January 2008 to December 2009 Served as Lead Security Officer in the implementation of Federal security Standards for Authority to operate (ATO). Thorough knowledge of mandatory federal standards in response to FISMA NIST SP 800-53A, SP 800-37, SP 800-42, NIST 800-115, Gramm Leach Bliley Act (GLBA), HUD Handbook, Sarbanes Oxley (Sox), National Housing Act, and FIPS 199. Responsible of the following: Design and implementation of government computer security programs; security policy documentation, maintenance of systems and infrastructure Security Plan, Policies and procedures agency wide; Risk assessment, System security Plan, Contingency Plan, Configuration Management Plan, System Test & Evaluation Maintenance of POAM execution, (CSAM) network security, baselines, network boundaries, risk management, TCP-IP services, DNS, firewall security, patches, vulnerabilities and logs, router and switch configuration, network security architecture and design. Conducted in depth security reviews (ArcSight and Nessus-ePO) for network vulnerabilities, and mitigation strategies in accordance with Federal guidelines; NIST, OMB A-130. Performed system vulnerability scanning and penetration testing of systems and network environment. Worked directly with internal IT personnel and clients

to establish IT security best practices, protection objectives, process improvements and effective IT security controls Served as IT security consultant to clients for the implementation of ISO 27001 security standards, risk assessment, system security, data protection, and policy implementation. Reviewed system-wide security practices, disaster recovery, and network security plans. Improved efficiency and awareness of enterprise-wide security concerns, maintenance concepts, as well as data and resource protection activities Provided training of security and data recovery instruction to five-member team of experts in medium scale administration for Andean Pacific export group Participated in system reviews to include hardware and software, in-house development and provide recommendations for securing these systems Proactively supported the certification and accreditation activities, and analyzed and coordinated IT security incidents and perform documentation and reporting Design, implement and support security-focused tools and services Support of current security products and initiatives, including PKI and encryption solutions. Develop security policies and procedures Participate in security compliance efforts (e.g., PCI-DSS) Evaluate new and emerging security products and technologies. Provide expert judgment that contributes to design, development and implementation of security infrastructure projects Education Bachelor of Science Imo State University 2000 to 2002 University Of Ibadan 1990 to 1995 Masters in Business Administration in Information Technology California Intercontinental University Additional Information CORE COMPETENCIES Testing and Documenting, Telecom and Network Security, Process Improvement, System, Security Risk, Assessment, Sarbanes Oxley Compliance, Technology Risk Management, PDCII.HIPAA, Strategic Planning, Application Development, Computer Room Controls, Disaster Recovery, Data Integrity, Regulatory Compliance, Project Management, User Access Controls, SAS 70 Type II(now SSAE 16), Vulnerability Assessment, Business Continuity. TECHNICAL PROFICIENCIES ISO 27001, COBIT, FISCAM, NIST, PeopleSoft, UNIX / Solaris / AIX - True 64 HP, IBM MVS O / S 390, Windows 2008, z / OS, UNIX, RACF, CISCO Firewall and Router Security

Name: Victoria Miller

Email: michaeldiaz@example.com

Phone: 768-825-6280x723