

Senior Information Security Analyst Senior Information Security Analyst Senior Information Security Analyst Darnestown, MD Work Experience Senior Information Security Analyst Consultation Services (Private) - Germantown, MD January 2018 to Present Followed NIST RMF guidelines, FISMA/OMB standards, and industry best practices in performing information security assurance responsibilities for Federal Contractors. Lead in deliverables package and documentation reviews and updates for various systems Lead in security control assessment exercise (ST&E) for various systems Completed CompTIA CASP, ISSE, Cryptography, and CISSP Training Wrote a nonfiction book (currently in review) to be published Focused, resilient, detail, team, and goal oriented, work well with both lower and upper management for the accomplishment of a designated task and or achieve a goal Senior Information Security Analyst IQ Solutions, Inc - Rockville, MD March 2017 to September 2017 Followed NIST SP 800 53 Revision 4 guidelines, FISMA/OMB and industry best practices in performing information security certification and assurance responsibilities for various systems Lead information system certification and accreditation and responsible for deliverables package for various systems Lead system documentation, reviews, and updates (including SSP, CM, CP, RA, E-Authentication, PIA, ST&E etc.) Lead information system security policies draft, reviews, and updates (gap analysis) Participated in the implementation of system security controls for various systems Lead in the assessment of system security controls and continuous monitoring efforts in establishing controls effectiveness for overall system security for various systems. Lead the implementation of a successful company-wide security awareness and training program Lead as a POC for all assigned information systems Lead in tracking and updating system status - POA&Ms, Milestones, and Artifacts Security Team Lead in working with system personnel - Infrastructure, network, help desk to provide to maintain secure systems posture. Lead in interacting with vendors in determining efficient and effective security system automation tools to enhance efficiency performing system audits and artifacts retention, reviews and updates. ' Information Security Analyst InScope International - Silver Spring, MD September 2016 to November 2016 Follow NIST SP 800 53 Revision 4 guidelines in performing information security assurance responsibilities for various systems via CSAM POC for all assigned information systems

under Led in tracking and updating system status - POA&Ms, Milestones, and Artifacts in CSAM Coordinated with system personnel - ISSOs to provide ITSOs with accurate system reports regarding Milestones, POA&Ms, AORs and Artifacts Engaged in Front-End Documentation Reviews and write-ups - Kick-Off, SAP, SCA setup for assigned systems Engaged in Back-End Documentation Reviews and write-ups - completed SCA, VAR, SAR, Out-Brief Slide Deck etc. write-ups Engaged in Draft POA&M Approval Request and POA&M Close Request Reviews and write-ups. Systems Security Analyst Microsoft Corporation - New York, NY November 2013 to February 2016 Led in coordinating and guiding system owners and security system administrators through the C&A Identified security controls types for system using NIST SP 800 60 as a guide I participated in Categorizing of controls using FIPS 199 as a guideline Used NIST SP 800 53 as a guide in the selection of security controls identified for the system Used FIPS 200 to define minimum security control baseline for info and information system Led in the security controls assessment using NIST SP 800 53A as a guide to provide information necessary to determine their overall effectiveness Led in the development and maintenance of C&A documentations - SSPs, CPs, Risk Assessment Reports and evaluation of existing documentation for accuracy using NIST SP 800 series and ISO 27000 & 27001 respectively Led on the creating POA&Ms, developed required mitigation strategies As a team lead, worked with C&A team members, senior executives to establish and define programs, risks, and resources IT Security Analyst Microsoft Corporation - Germantown, MD September 2010 to September 2013 Conducted system risk assessment and documentation of key controls using NIST SP 800 30 as a guide Developed audit plan and performed system controls testing and assessment of information security using NIST SP 800 115 & 800 53A as a guide. Guided system administrators and system owners through the certification and accreditation process using NIST SP 800 37 Develop and reviewed System Security Plan by NIST SP 800 18 guidelines Involved in planning, and preparation for contingency and disaster recovery operations and Business Impact Analysis (BIA) using NIST SP 800 34 Ensured management, operation, and technical controls to secure sensitive security system are in place according to NIST SP 800 53 control selection guidelines and FIPS 200 control baseline

establishment and tailoring/enhancement guidelines    Assessment of security controls using NIST SP 800 53A to receive System Security Authorization    Involved in continuous monitoring of security control procedures using NIST 800 137, SP 800 128 & SP 800-30/39 as a guide    Worked in a self-motivated environment with strict project deadlines involved in security team meetings for implementing IT system security requirements Education Bachelor of Business Administration in Corporate Finance Zicklin School of Business, Baruch College, City University of New York 2002 Certification Skills Information Security, Information Assurance, Fisma Certifications/Licenses CERTIFIED AUTHORIZATION PROFESSIONAL (CAP) Present ISC2 CERTIFIED AUTHORIZATION PROFESSIONAL (CAP)

Name: Donna Allison

Email: jonesyolanda@example.net

Phone: (809)937-6572x77353