

IT Security Analyst/A&A Specialist IT Security Analyst/A&A Specialist IT Security Analyst/A&A Specialist - Sunrun Inc A seasoned leader in Cyber Security Engineer with 5 years hands on experience in Risk Management Framework (RMF), core Expertise in Cyber security, Risk Management, Testing, FISMA, ST&E, SCA, POAMs, Security Assessment & Authorization (A&A) SCAP, and the CDM process. Highly adaptive, and can work in a fast paced environment and still exceed 30% expectations in meeting program milestones. Ability to multi-task and analyze information, while providing sound recommendations to help the client. Well acquainted with the NIST SP 800 Series. Work Experience IT Security Analyst/A&A Specialist Sunrun Inc April 2016 to Present

NIST 800-37 risk management framework-categorize systems, privacy impact assessments, security impact assessments, interconnection security agreements, risk assessments, waivers. Develops and manages the contract/programs security documentation such as the System Security Plan (SSP), Security Risk Assessment Reports (SAR), test and evaluation reports, security policies, Contingency Plans, Plan of Action and Milestones (POAM), and Incident Response Plans. Guided various organizations through system categorizations, minimum controls baseline selections, Implementations of selected controls specified in the SSP, Assessing the effectiveness of the implemented controls, documenting the SAR as well as recommendation guide to identify deficiency in accordance to NIST SP 800 53 rev &53A, FIPS 199/200 and POA&Ms documentation

Assess and reviews privacy controls in compliance with Privacy Impact Assessments and Privacy Threshold Analysis using NIST 800-53. Conducts risk and vulnerability assessments of planned and installed information systems to identify vulnerabilities, risks, and protection needs. Develops and implements programs to ensure that systems, network, data users are aware of, understand and adhere to systems security policies and procedures and conducts systems security evaluations, audits and reviews. Ability to independently and effectively investigate, troubleshoot and analyze security-related problems, develop recommendations and collaborate with other OIS customer personnel to implement corrective actions. Maintains appropriate client and contract/program guidelines including required federal guidance/information within the application. Develops and maintains standard operating procedures (SOP) for the contract/program's application suite. Ability

to independently and effectively investigate, troubleshoot and analyze security-related problems, develop recommendations and collaborate with other OIS customer personnel to implement corrective actions. Information Security Analyst Hackensack Meridian Health April 2013 to March 2016 NJ

- * Determine security categorizations using the FIPS 199 and SP 800 60 as a guide in the risk management framework.
- * Worked effectively with all levels of management, staff and cross-functional security teams within the organization to identify and implement information assurance controls authorized by NIST SP 800-53.
- * Performed Privacy Threshold Analysis (PTA), E-Authentication with business owners and selected stakeholders.
- * Assisted System Owners and ISSOs through Security Assessment and Authorization (SA&A) Process, ensuring that Operational, management and technical control securing sensitive Security Systems are in place and being followed according to the Federal Guideline (NIST SP 800-53).
- * Performed NIST-based C&A activities using NIST 800-53 process for assessing federal agency IT systems; reviews implemented procedural and technical security controls; and provides recommendations to resolve identified deficiencies
- * Identified and advised major security incidents, which could impact day-to-day services and operations
- * Performed security testing and analyze results to identify vulnerabilities and violations of information security. Work to determine strategies and takes measures to mitigate risk
- * Prepared documentation and review System Security Plan (SSP), Security Assessment Report (SAR), Plan of Action and Milestones (POA&M), Authorization letter/memorandum (ATO)
- * On an on-going basis, coordinate with business process owners to ensure timely identification and remediation of jointly owned risk related issues and action plans (POA&M).

Network Administrator MTN October 2008 to November 2012 Ghana (Exceeded 45% over set goal before project milestone)

- * Supervised the day-to-day operation of computer networks including hardware/software support, training, in World Vision Ghana Head Office, Base Offices and ADPs and special projects
- * Established network specifications by conferring with all users; analyzing workflow, access, information, and security requirements; design router and switch administration, including interface configuration and routing protocols.
- * Planned, designed and implemented data and voice connectivity for local area network (LAN) and wide area network (WAN) systems. Assisted

in coordinating and implementing connectivity and infrastructure projects including network and related wiring plans, LAN/WAN hardware/software purchases, Partnership special projects: system installations. Manage network device configurations, backup/recovery, maintenance and problem-solving in the Head Office, Base offices, ADPs and special projects * Maintained existing anti-spam, anti-spyware and anti-virus systems. Define/recommend network and security policies and Implement approved policies to minimize risks. * Established network performance management processes to monitor Local Area Networks and WAN links in all projects. * Interacted regularly with the Service Desk Team, Administrator and GICT to ensure a good user experience of network services. * Planned for and maintained a call tracking system that enables proper tracking of and rapid response to user calls on all network related issues. Education Bachelor of Science University of Ghana May 2006 Skills SECURITY (5 years), INFORMATION SECURITY, NESSUS, NIST (6 years), FISMA (6 years), INFORMATION ASSURANCE, VULNERABILITY ASSESSMENT, CONTINGENCY PLANNING, EXCEL (10+ years), MICROSOFT OFFICE (10+ years), OUTLOOK (10+ years), WORD (10+ years)

Name: Travis Fuller

Email: glittle@example.net

Phone: 863.444.7563x179