IT Security Analyst IT Security Analyst IT Security Analyst - United States Department of Homeland Security Work Experience IT Security Analyst United States Department of Homeland Security October 2017 to Present Analyze and update System Security Plan (SSP), Risk Assessment (RA), Privacy Impact As- sessment (PIA), System Security test and Evaluation (ST&E) and the Plan of Actions and Milestones (POA&M) Designate systems and categorize its C.I.A using FIPS 199 and NIST SP 800-60 Conduct interviews with selected personnel, document and evaluate business processes, and execute audit test programs to determine the adequacy and effectiveness of internal controls and compliance with regulations Conduct cloud system assessments, primarily with AWS (Amazon Web Services) by utilizing FedRAMP and NIST guidelines Evaluate the effectiveness of internal control systems and identify areas of improvement, best practices, and lessons learned Document findings within Requirements Traceability Matrix (RTMs) and Security Assess- ment Reports (SARs). Review and analyze Nessus Vulnerability and Compliance scans, WebInspect scans, Burp Suite and DbProtect scans for possible remediation. Assess systems of varying scope and complexity and comprised of various technologies. Provide weekly status reports on ongoing tasks and deliverables IT Security Analyst United States Custom and Border Patrol April 2015 to October 2017 Assisted in conducting cloud system assessments Helped in updating IT security policies, procedures, standards and guidelines according to department and federal requirements Worked with client in safeguarding CUIs by performing the necessary assessments which pri- marily deals with 14 control families. Support Cyber Security analyst in conducting Vulnerability Management, Security Engineering, Certification and Accreditation, and Computer Network Defense. Perform risk assessments, update and review System Security Plans (SSP) using NIST 800-18 (Guide for Developing Security Plans for federal information systems) Plans of Action and Mile- stones (POA&M), Security Control Assessments, Configuration Perform vulnerabilities scan and monitor continuously using NIST 800-137 as a guide with the aid of Nessus. Junior Cybersecurity assurance engineer Sektec Security Inc March 2013 to April 2015 Experience in cloud system assessments, primarily with AWS (Amazon Web Services) by utiliz- ing FedRAMP and NIST guidelines Experience in executing Step 4 (Security Assessment) of the NIST Risk

Management Frame- work (RMF). Experience in developing and disseminating Security Assessment Plans. Experience in interpreting and evaluating implementations of NIST 800-53 rev 4 security con- trols. Documenting findings within Requirements Traceability Matrixes (RTMs) and Security Assess- ment Reports (SARs). Experience reviewing and interpreting Nessus Vulnerability and Compliance scans Ability to execute Security Assessments and develop and deliver supporting documentation with- in aggressive timelines. Assessing systems of varying scope and complexity and comprised of various technologies. Work on multiple assessments simultaneously. Security Specialist / Junior SOC analyst GAP - Hanover, MD April 2010 to March 2013 Perform incident response activities such as host triage and retrieval, malware analysis, remote system analysis, end-user interviews, and remediation efforts Creates new ways to solve existing production security issues Research and test new security tools/products and make recommendations of tools to be imple- mented in the SOC environment Provide trend analysis and data reports associated with tracking case workload and cycle time associated with all work performed. Conduct recurring security vulnerability assessments, physical security inspections of contractor plants and facilities performing work for the government involving the storage and/or production of sensitive arms, ammunition and explosives. Conduct security vulnerability assessments of cleared industrial facilities performing on classified contracts for the U.S. Education Battersea County High school - London BA in Business and Finance Vauxall University - London Skills Sharepoint, Nessus, Nist, Splunk, Authentication, Ms office, Risk assessment, Scanning, Sar Additional Information Summary of skills: FIPS 199, FIPS 200, NIST 800-53 Rev4, NIST 800-30, NIST 800-37, NIST 800-39, E-Authentication, Privacy Impact Assessment (PIA), Risk Assessment (RA), SSP, ISCP, SAR, Plans of Action and Mile- stones (POA&M), Authorization to Operate (ATO) Letter, MS Office, SharePoint, Access, Nessus Vul- nerability Scanning Tool, Splunk, C-Cure, Passage Point.

Name: Jonathan Ramsey

Email: jean61@example.net

Phone: (485)495-3780x618