Cyber Security Analyst Cyber Security Analyst DOD Top Secret Clearance Baltimore, MD Experience performing audits and risk assessments of internal controls over Information Technology (IT) under multiple frameworks including: National Institute of Standards and Technology (NIST), Cyber Security Risk Assessments, Federal Information Security Management (FISMA), Vulnerability Assessment, Sarbanes-Oxley 404 compliance, Security Assessment and Authorization, Federal Information Systems Controls Audit Manual (FISCAM) Framework, Committee of Sponsoring Organizations (COSO), and Control Objectives for Information and Related Technologies (COBIT). Authorized to work in the US for any employer Work Experience Cyber Security Analyst Booz Allen Hamilton October 2017 to Present Assess, design, implement, automate, and document security processes and solutions leveraging Amazon Web Service (AWS) and other third-parties Develop Security Policies and/or ensuring Security Compliance for Cloud implementations Analyzed and update System Security Plan (SSP), Risk Assessment (RA), Privacy Impact Assessment (PIA), System Security test and Evaluation (ST&E) and the Plan of Actions and Milestones (POA&M) Prepare security-related controls, documentation, policies, standards, baselines, guidelines, that comply w/FISMA/FedRAMP criteria, based on information gained in interviews Review software systems to assess & document compliance w/FISMA/FedRAMP criteria IT Security Assessor Deloitte & Touche LLP October 2016 to October 2017 Responsible for conducting Security Control Assessment (SCA) over security and access management on Federal client systems based National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4 and NIST SP 800-53A Revision 4. Create Security Assessments Plans (SAP), Reports (SAR), and Plan of Action and Milestones (POA&Ms) to identify system findings or weaknesses and track mitigation. Performs A&A documentation reviews and communicate threats, vulnerabilities, and risk information to stakeholders. Conducted compliance and vulnerability assessments using Nessus and Splunk. Prioritize findings based on risk and document detailed corrective and remediation plan or actions. Develop recommendations to mitigate cyber risk threats and support implementation. Conduct review of general computer control (GCCs), cybersecurity reviews, and audits as identified on the internal audit plan. Analyzes vulnerability scans, interpreting risks and employing manual checks

to validate vulnerability data. Security Analyst IX Solutions May 2013 to October 2016 Supported Sarbanes-Oxley (SOX) compliance review by testing general application controls, change management to evaluate the design and operating effectiveness of client's internal controls. Led planning and performance of walkthroughs and internal controls testing for SOX, IT general controls (ITGC), and A-123 audits. Supported audit plan development for IT internal controls testing across multiple platforms and applications. Conducted technology internal controls risk assessments for SOX, A-123, FISCAM, SSAE16 (SOC) and HIPPA audits Assisted in coordinating, defining, and planning project related activities throughout the system development life cycle (SDLC) to support overall project success. Performed operational audits of employee's compliance with the company's safety policy, cash handling policy, and other operational policies. Conducts security Assessment and Authorization, cyber security risk assessments Internal Auditor Modest Technology Solution April 2010 to May 2013 Designed and executed tests of IT controls (ITGC and application controls). Led various internal audit and client status meetings. Planned and executed risk-based IT audits or IT advisory projects Providing Training and awareness for IT staff in terms of IT Governance and the IT Audit process. Supported IT SOX testing and assisted Internal Audit with audit approach. Performed compliance and IT controls reviews on client environments. Analyzed IT and Business processes and controls. Performed operational audits of employee's compliance with the company's safety and cash handling policy. Identified weaknesses and performed root cause analysis. Performed IT Risk Assessments and analysis in various client environments. Education M.S. in Public Administration University of Baltimore B.S. in Criminal Justice University of Baltimore Skills SECURITY (5 years), CYBER SECURITY (4 years), NIST (5 years), FEDERAL INFORMATION SECURITY MANAGEMENT ACT (4 years), FISMA (4 years), Management, Word, Typing, Organizational Skills, Excel Additional Information ? Over eight years of experience in system security monitoring, auditing and evaluation, C&A, Risk Assessment of GSS (General Support Systems) and Security Control Assessment (SCA) ? Experienced and detailed knowledge of security testing tools such as Splunk and Nessus Security Center ? Develop, review and evaluate System Security Plans (SSP), Security Assessment Report (SAR), Risk Assessment

Report (RAR), Plan of Action and Milestone (POA&M) etc. according to NIST Special Publications and FedRAMP. ? Perform comprehensive assessments and write reviews of management, operational and technical security controls for information systems ? Ability to multi-task, work independently and or as part of a team ? Leads and conducts vulnerability assessments and risk analysis of target system ? Effective interpersonal and verbal/written communication skills Areas of Expertise ? Risk Management Framework ? Cyber Security Risk Assessment ? NIST 800 53A Publications ? FISMA Compliance ? Risk Assessment Management ? Vulnerability Assessment ? Security Assessment and Authorization ? FedRAMP ? Communication and Analytics ? Monitoring & Reporting

Name: Kevin Kelley

Email: brookehenry@example.com

Phone: +1-251-310-7271x433