Contractor, Information Security Analyst Contractor, Information Security Analyst Contractor, Cyber Security Analyst - Mine Safety and Health Administration Lakewood, CO Authorized to work in the US for any employer Work Experience Contractor, Information Security Analyst Mine Safety and Health Administration - Lakewood, CO April 2017 to Present Successfully coordinated as Lead Point of Contact (POC) with external security consultants for the MSHA's High Value Asset (HVA) Security Assessment and Authorization project between November, 2017 and April, 2018. Provided SME in research on evolving security issues and IT risks to the ISO team, building relationships with in the team and communicating our team goals to our internal and external customers effectively. Coordinating OIG FY18 FISMA audit to review audit guidance references, gather applicable supporting evidence from internal customers and plan engagement with auditors and agency personnel who will provide critical information for the success of the audit. Conducted reviews of System Security Plan (SSP) implementation statements in CSAM for MSHA's HVA to capture infrastructure and application system changes in the control environment. Participated in the implementation of the OCIO Fiscal Year 2016-2019 Security Self-Assessment and ISCM Plan that included the: a. Annual Security Assessment(ASA) for MSHA HVA for FY2017, FY18 Authority to Operate(ATO), FY19 ASA b. Information Systems Continuous Monitoring(ISCM) c. Security Assessment and Authorization of agency HVA under the FISMA inventory and; d. Security testing of the information system as part of ongoing system development life cycle (SDLC). Successfully established a process for conducting weekly, monthly and ad hoc Splunk Log Reviews to investigate suspicious events through incident response procedures Lead security POC for the implementation of HPE Fortify Static Code Analyzer to ensure (a) a formal development security testing plan is established by the development team (b) configuration changes are tested for security impact analysis prior to release (c) remediation action by developers is trackable and associated with change requests (d) change requests tickets are explicitly approved based on security impact assessment (e) the entire process is auditable Reviewed IBM Big Fix weekly vulnerability scan reports for missing vendor patches for potential impact communicated with System Owner for approval decision to facilitate timely deployment to OCIO Security. Reviewed

HPE Web Inspect application vulnerability scans quarterly, communicated to System Owner to review and provide cost and timeline of remediation action, drafted Plans of Action and Milestones (POAMs) in CSAM to track and report effectiveness of remediation process. Conducted monthly and quarterly account reviews for privileged and non-privileged users to ensure user entitlements are appropriate and no authorized users retained access to the system. Annually participated in contingency planning activities as a subject matter expert including review and update of agency contingency plan, role-based contingency training, functional testing and communication exercises. Conducted agency security policy review, gap analyses of more than 20 outdated security policy documents against more than 15 current policy and procedures documents to ensure alignment with changes in the DOL Computer Security Handbook Reviewed current system architectural designs against the proposed data modernization initiatives (DMI) and business case rationale and the level of security planning integration throughout the System Development Life Cycle (SDLC). Led the security assessment of the MSHA Unified Communications Systems against NIST SP 800-53 rev.4 controls to establish control weaknesses and to inform management of any existing risks in the system. Developed, documented and tracked Plans of Action and Milestones (POA&M) in the Cyber Security Assessment & Management (CSAM) with client management teams to ensure remediation action plans are on track for timely resolution of weaknesses and closure. Established a POA&M and security documentation tracking tools for the System Assessment and Authorization program for all system under our portfolio to support System Owners with regular friendly reminders for monthly reviews and updates. Senior Information Technology Auditor GEICO - Washington, DC September 2016 to Present Senior Information Technology Auditor, GEICO (Chevy Chase, Washington, DC), September, 26th 2016-To-April, 22nd 2017 SOX control audit for a vast terrain of technology platforms. IBM Open Pages platform SME for Audit Program Management. Review and approval of test plans for General IT Auditors. Work paper review, process improvement, client management communication. Audit reporting to IAD Management. Security policy and compliance review Physical security audits Microsoft Azure Cloud access control audit Use of PowerShell to obtain Active Directory SOX testing data Use of Excel for SOX

control testing data analytics IBM Qradar SIEM functionality audit. DevOps environment audit Change and configuration management audit in various environments C*Cure 9000 Subject Matter Expert on Physical Security Senior IT Auditor United States Agency for International Development June 2010 to April 2016 Roles & Accomplishments Information Security Management: Developed draft audit charter, convened stakeholders for review, developed business case for management approval. Reviewed existing risk management protocols, security policy, system security plans (SSP), evidence of annual review, approval and version control. Convened business process owners, executive risk function to map an appropriate RMF to enterprise business strategy. Developed internal audit function through talent management, knowledge sharing and collaborations across business functions. Conducted active directory audits and database security audits. Conducted Infrastructure assessments and security controls assessments across the group. Conducted FISMA readiness audits and consulting services across the group. Assisted in the execution of Internal Audit IT Risk Assessment and development of the annual IT audit plan. Planned and executed technology audits (e.g., data center audits, general control reviews, information security reviews, system development assessments, etc.). Provided leadership and support to the Internal Audit team to integrate technology coverage into operational and financial audits. Specifically provide assistance in the identification and testing of key application controls as well as the use of computer assisted audit techniques to improve the risk focus and efficiency of operational and financial audits. Planned and led audits within assigned areas of responsibility. Responsible for all aspects of audit execution: assessing risk and performing detailed audit planning; providing leadership throughout the audit; regularly communicating with management; developing and communicating audit concerns to appropriate levels of management; drafting audit reports; and working with management to develop reasonable and sufficient corrective actions. Project team SME for the development of the USAID/MCIO System Managers' Handbook, an IT process workflow, policy and engineering reference draft manual Project team SME linking USAID/MCIO ISSO Handbook to System Manager Handbook for effective implementation of Agency information security policy. IT Assurance & Compliance Lead US Centers for Disease

Control & Prevention January 2001 to May 2010 Developed draft IT charter, convened stakeholders for review and developed value proposition for management approval of the audit charter. Developed internal IT audit function from ground up, through talent management, knowledge sharing and stakeholder collaboration to ensure FISMA, HIPAA, FOIA agency wide security policy and Mission order compliance Provided technical leadership during the preparation, planning, design, and implementation phases of IT project activities, including proposal development, determining specific network requirements, solution design & architecture, configuration and implementation of reference design, documentation, and knowledge transfer. Focus area was to develop a security culture across the organization with emphasis on continuous improvement of the control environment. Assisted internal CDC groups to properly complete and submit Certification and Accreditation (C&A) documents (also known as Security Assessment and Authorization) in compliance with NIST guidelines. Assist in the completion of C&A, and CRA documentation Provided verbiage within SSP documentation to satisfy NIST 800-53 controls and ITIL Process owner for Service delivery, security management and access management. Member of the data center internal Audit Team responsible for auditing ITIL process owners for non-conformance, deficiencies, and opportunities for improvements prior to and after ISO20000 certification of the data center. Development and implementation of a security roadmap for the data center to detail a timeline and order to address policy, personnel, and technical issues to improve the security posture of the organization. Ensure the change management process addresses risk, changes are tested in the test environment before implementation in the production environment and that there are appropriate segregation of duties across all business processes. Successfully implemented data center initiatives to create pre-approval process for change management system, identity and access management, policy compliance, firewall implementation, IPS implementation, card key access, Event Log Management (ELM) implementation and more Education MBA in Business Edinburgh Business School, Heriot-Watt University, Scotland 2012 Skills Sharepoint, Active Directory, Microsoft Office, security, testing, training, Excel, Word, Organizational Skills

Name: Steven Oliver

Email: shawnkelley@example.net

Phone: 285-312-4358x208