Sr. Cyber Security Policy & Compliance Analyst Sr. Cyber Security Policy & Compliance Analyst Sr. Cyber Security Policy & Compliance Analyst - Booz Allen Hamilton Dumfries, VA Seeking an IT Security Auditor or Cyber Security Analyst position in a growing organization with focus on FISMA, Sarbanes-Oxley 404, HIPAA, PCI DSS, HITRUST, System Security Assessments & Monitoring, Risk Assessments, or other information system security programs. Authorized to work in the US for any employer Work Experience Sr. Cyber Security Policy & Compliance Analyst Booz Allen Hamilton December 2017 to Present Department of Commerce Provide cyber security assistance throughout the security assessment and compliance lifecycle process. Responsible in conducting security assessments, continuous monitoring of cyber security and privacy policies, programs, compliance artifacts and/or, standards. Support the management of government and industry security compliance, as well as systems accreditation Supports the administration of the documentation, validation and accreditation processes necessary to assure systems meet security and privacy requirements. Conduct a crosswalk review of the NIST SP 800-122 Privacy Controls by reviewing privacy overlays of security and privacy controls on a system Conduct Compliance and Policy Checks for the various Bureaus on the following artifacts: Contingency Plans & Tests, Configuration Management, System Interconnections and System Security Plans. Create dashboards for SharePoint from Overall Scorecard of Compliance and Policy Checks on the various Bureaus. Participate in Compliance Review Board (CRB) weekly meetings to discuss concurrence statuses of PIA documents created for various DOC's specific information systems. Review open POA&Ms, current SSPs, SARs & PTA documents for the PIA document being reviewed for compliance and concurrence. Provide concurrence or non-concurrence status for reviewed PIA documents with explanations and recommendations. Support CSAM reviews to identify expired and missing artifacts for the various Bureaus. Perform CSAM Administrative work by attending and responding to CSAM users with questions and help in maneuvering through CSAM 4.1. Sr. IT Security Analyst Ohio Department of Medicaid August 2013 to August 2017 Responsible for conducting structured assessment & authorization (A&A) activities utilizing the Risk Management Framework and in compliance with the Federal Information Security Modernization Act (FISMA)

requirements Conduct Business Impact Analysis (BIA) to analyze mission-critical business functions, and identify and quantify the impact those functions if these are interrupted Conduct IT system testing based on the appropriate analysis and review techniques provided by NIST Develop and update the information systems security documentation (e.g., System Security Plan, Contingency Plan, Contingency Plan Test, Business Impact Analysis, FIPS-199, eAuthentication, Privacy Threshold Analysis, Privacy Impact Assessment, System of Records Notice) Knowledgeable in NIST SP 800 series including SP 800-60, SP 800-53, SP 800-53A, SP 800-18, SP 800-34, SP 800-62, SP 800-37, SP 800-137 Assess adequacy and efficiency of security controls by updating Security Control Assessment Plan (SCAP), Security Test & Evaluation (ST&E) Report and Security Assessment Report (SAR) Plan, execute and report on IT system vulnerability root causes and mitigation recommendations Provide a security review of system documentation, audit logs, rule set and configuration to validate policy compliance. Report IT security incidents in accordance with established procedures Plan, develop, implement, and maintain an Incident Response and Audit Program for events of interest and address Plan of Action and Milestones (POA&Ms) in continuous monitoring with various point of contact Plan, schedule, coordinate, prepare, execute, document the results of test plans and test scripts, and provide lessons learned for incident response, contingency, and continuity of operations drills, exercises, and activities. Effectively communicate technical information to non-technical personnel via email, face-to-face meetings and periodic bulletins Coordinate with system owners and ISSOs across the organization to ensure timely compliance Participate in meetings to discuss system boundaries for new or updated systems to help determine information types for categorization purposes. Determine the classification of information systems to aid in selecting appropriate controls for protecting the system. Upload supporting docs in the System's Artifact Libraries, Google Docs, and CSAM Review Rules of Behavior (RoB), Interconnection Security Agreement (ISA) and Memorandum of Understanding (MoU) for clients using NIST SP 800-47 Review and revise System Security Plan (SSP), System Security test and Evaluation (ST&E) Risk Assessment (RA), Privacy Impact Assessment (PIA), and the Plan of Actions and Milestones (POA&M) Information Security Analyst

JP Morgan Chase - Columbus, OH December 2011 to August 2013 Determined the scope for system audit. Usually started with a kick off meeting with key officials and the audit committee Implemented Sarbanes-Oxley Act (SOX 404) requirements including COSO, COBIT and ISO 27001 and 27002 where applicable Created a test plan to determine controls to be tested as well as methods of testing. Effectively participated in testing of the SOX IT General Controls Conducted audit within specific timeframe utilizing subject matter expects and other system owners Supported requirements gathering and design efforts of critical projects as needed Collected evidence from various point of contacts to update COSO, COBIT or PCI-DSS finding report to test for effectiveness and adequacy of controls by analyzing test plan against evidence collected via examination, interview and testing Submitted report of risk/audit analysis. Plan, execute and report on IT system vulnerability root causes and mitigation recommendations Conducted continuous IA controls for any deficiencies. Deficient controls were then reported to the ISSO for appropriate mitigation actions Conducted IT controls risk assessments that included reviewing organizational policies, standards and procedures and provided advice on their adequacy, accuracy and compliance with the Payment Card Industry Data Security Standard [PCI DSS] Updated Business Impact Assessment [BIA] template to monitor efficiency and adequacy of Contingency plan. Plan, schedule, coordinate, prepare, execute, document the results of test plans and test scripts, and provide lessons learned for incident response, contingency, and on-going monitoring activity. Prepared written reports after the completion of the assessment Maintained client's information security governance, risk and compliance activities to align with the NIST Risk Management Framework (RMF) Performed Contingency Plan Test and Training to ensure systems' recoverability as defined in IT systems security requirements Developed POA&M (Plan of Action & Milestones) document to take corrective actions resulting from ST&E (System Test & Evaluation) Prepared and review Authorization to Operate (ATO) packages (i.e. SSP, RA, CMP, ISCP, DRP, IRP and PIA) for various systems Assisted in the conduct of risk and vulnerability assessments of planned and installed information systems to identify vulnerabilities, risks, and protection needs Performed security control assessment using NIST 800-53A guidance and as per continuous monitoring requirements

Reviewed core documents such as System Security Plan, Contingency Plan, Incident Response Plan, Standard Operating Procedures, Plan of Actions and Milestones, Remediation Plans, Configuration Management Plan PROFESSIONAL AFFILITAION Booz Allen Hamilton Women in Cyber Member of Executive Women's Forum (EWF) Education BA in Economics & Chemistry Ohio Wesleyan University - Delaware, OH Skills SECURITY (6 years), COBIT (1 year), NIST (6 years), FISMA (4 years), RISK MANAGEMENT (5 years), Information Security, Cyber Security Additional Information AREAS OF EXPERTISE Experience with performing Security Control Assessments, Risk Management Framework, Cybersecurity Framework, Information Assurance, NIST 800 Series Special Publications. Experience with common control programs and in advising on how to remediate risks. Experience in working with senior executives and senior government officials, COSO, COBIT, Sarbanes-Oxley Act, HIPAA, HITRUST, PCI DSS, ISO 27001, 27002, Security Authorization & Accreditation (A&A), FIPS, FY18 CIO FISMA Metrics, Strong verbal and written communication. SOFTWARE AND PLATFORM Windows, Microsoft Works: Word, Excel, Access, Outlook, Power Point, SharePoint, VBA/Macros, VMWare, Tableau, Crystal Reports, Qualtrics, CSAM, Nessus Tenable Vulnerability Scanning Tool, WebInspect. SUMMARY OF QUALIFICATIONS I have over 5 years' experience analyzing and mitigating risks for federal and commercial entities. My expertise includes NIST Risk Management Framework (RMF), Cloud Security, Information Assurance, System Monitoring, regulatory compliance and loss mitigation. Knowledge areas include FISMA compliance- [categorization through to continuous monitoring] and other commercial frameworks including COSO, COBIT, ISO and HIPAA. My knowledge of industry standards and ability to meet milestone deadlines make me a valuable addition to any organization focused on staying on top of information security matters.

Name: Amanda King

Email: ingramchristina@example.net

Phone: +1-257-612-3852