**Bright Kojo Boateng**

**8030 Juliet Lane Apt # 301**

**Manassas, VA 20109**

Brightkboateng@gmail.com

**Clearance - Secret**

**CAREER FOCUS:** Looking to apply my experience and skills to help attain organizational goals and objectives. To enhance knowledge for professional growth in the field of Information security and elevate to higher achievements in my career.

**SUMMARY OF QUALIFICATIONS**

• Working knowledge of NIST SP’s (800-37, 800-60, 800-53 Rev 4, 800-18, 800-53A) for documentation review and updates. Experience with the following tools: GRC, Risk Vision, CSAM and eMASS

• Perform security categorization using FIPS-199 and the selection of technical, operational and managerial controls using NIST SP 800-60 guidelines.

•Work effectively in a team environment and participate in collaborative initiatives that foster the mutual exchange of knowledge and expertise.

• In-depth understanding and professional knowledge in providing support and guidance to System Owner’s through the NIST RMF System A&A processes, including annual self-assessment (NIST SP 800-53A) completion, CP Testing and POA&M remediation.

•Perform Security Control Assessments (SCA) according to NIST SP 800-53A.

•Review and update Contingency Plans (CP) using NIST SP800-34 guidelines.

•Ability to multi-task, work independently and as part of a team, share workloads, and deal with sudden shifts in project priorities. Vast knowledge on MS Office (Word, Excel, Access, Outlook)

**EDUCATION&CERTIFICATIONS**

BS, Computer Science -University of Cape Coast, Ghana May 2008

Security+, CEH, ITIL, CISA, CCSK Certifications.

**WORK EXPERIENCES**

**Mind Point Group 01/2021-Current**

**Information systems security officer**

* Develop, update, and/or review RMF documentation to include Security Plans, Implementation Plans, Plans of Action and Milestones (POA&Ms), and Risk Assessment Reports.
* Assess system compliance against NIST security requirements to include the NIST 800-53 controls.
* Produce evidence as necessary to support compliance status of NIST security requirements
* Work with system administrators, engineers, and developers to create or update system/site policies, procedures, and process guides
* Coordinate with other system SMEs to identify and develop authorization boundary diagrams, architecture diagrams, and hardware and software inventories
* Analyze vulnerability scans of information systems and assist in remediation tasks
* Attend meetings with stakeholders to discuss statuses of efforts
* Able to work independently and collaboratively with application developers, engineers, and others.
* Submit weekly reports to leadership regarding system/program status using (Word, Excel, Access, Outlook)

**CACI Federal Inc., Chantilly, VA (DHS CDM Contract) 06/2018 – 11/2020**

**Security Accreditation & Authorization Specialist:**

•Review and validate security documentation to ensure necessary security controls are in place and operating as intended.

• Provide cyber security analysis, with a focus on Assessment and Authorization (A&A), under the implementation of the Risk Management Framework (RMF).

• Prepareand review documentation, including risk assessment reports, certification and accreditation (C&A) packages, and plan of actions and milestones (POA&M).

•Review systems to identify potential security weaknesses and recommend improvements to amend vulnerabilities, implement changes, and document upgrades.

•Support DHS’ system accreditation and Ongoing Assessment and Ongoing Authorization processes and activities to ensure the implementation of NIST SP 800-53 security controls.

•Participate in ongoing meetings for systems undergoing the ATO (Authorization to Operate) process and the continuous monitoring of systems with full ATO.

•Provide management and Ongoing Authorization (OA) Compliance Support to include Risk Management Framework (RMF) and FISMA compliance, Security Release management, Security Authorization and OA, and DHS policy Directives and Cyber Orders.

•Support the Risk Management and Compliance Lead by providing support to maintain ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

• Recommend improvements on the security risk posture through new SOPs, tools, or methods.

• Compliance POA&M analysis, management, compliance, and remediation

• Monitor security advisories and security bulletins to ensure compliance with applicable security requirements.

• Support Security Test and Evaluation/Security Assessment activities.

**ASM Research, Chantilly, VA (Veterans Affairs CRISP CONTRACT) Jan 2017 – June 2018**

**Senior Cyber Security Analyst:**

• Executing reviews of RMF Security Controls to ensure FISMA and NIST compliance.

• Support leadership to identify capability gaps in vulnerability management services by analyzing Plans of Action and Milestones (POA&Ms) associated with the facility or system.

• Conduct analysis and aggregation of Security Control and POA&M evidence from various sources.

• Maintain knowledge of current RMF security trends and be able to clearly communicate them to the client.

• Analyze vulnerability assessment data to identify technical risks to the organization.

• Assist client in identification and reduction of findings at a site and enterprise level.

• Assess the Cybersecurity risk of IT systems documenting them in formal risk assessments and supporting artifacts associated with the Assessment & Authorization (A&A) process.

• Organize, develop, and present briefings, written summaries, and written reports incorporating narrative, tabular and/or graphic elements. Submit weekly reports using (Word, Excel, Access, Outlook)

• Applies knowledge of security principles, policy and regulations to daily tasking.

• Has experience with Cyber Security document management and is familiar with security and privacy rules.

• Researches policies, procedures, standards, and guidance, and recommends needed changes under specific conditions for the protection of information and information systems.

•Perform Information Assurance tasks and Cybersecurity support for the Continuous Readiness Information Security Program (CRISP).

• Assist in the remediation, coordination and validation of POA&Ms.

• Responsible for vulnerability remediation through patching using VA approved methods.

• Implements IT security solutions and assures successful implementation.

• Support & review security documentations & scans before submission for ATO.

**Pure Medical LLC, New York, NY June 2015 - Jan 2017**

**Information Security & FISMA Compliance Analyst**:

• Develop POA&M (Plan of Action & Milestones) document to take corrective actions resulting from ST&E (System Test & Evaluation)

• Assess program and security controls using Organization IT Security Policy Handbook and NIST Special Publications to provide information necessary to determine their overall effectiveness.

• Performed Contingency Plan Test and Training to ensure systems recoverability as defined in IT systems security requirements.

• Participated in security team meetings and rendered other support to IT Security office, which included ensuring appropriate steps are taken to implement information security requirements for all IT systems

• Responsible for monitoring compliance with information security policies by coaching others within the organization on acceptable uses of information technology and how to protect organization systems.

**S.I.P.S. Consult, New York, NY June 2013 – May 2015**

**Security Accreditation & Authorization Specialist:**

• Conducted the IT Risk Assessment and documented key controls.

• Develop, review and evaluate Security Plan based on NIST Special Publications 800-18.

• Investigates possible security breaches identified through review of audit reports and follows up accordingly with departments / management.

• Prepared and reviewed C&A package for Information Systems.

• Document all operational processes and procedures to optimize support

• Evaluate, test, coordinate, monitor and maintain information assurance controls.

• Assess information assurance controls for compliance and assist with development of security standards and procedures.

**New York Presbyterian Hospital, New York June 2010 – May 2013**

**Information Security Analyst:**

**•** Ensure that Information Systems security architecture, designs, plans, controls, processes, policies and procedures are aligned with client policies.

• Analyzed and defined security requirements for networks, applications/systems, end user computing, mobility, and data center technologies and solutions

• Determined security requirements by evaluating business strategies and requirements; researching information security standards; conducting system security and vulnerability analysis and risk assessments.

• Reviewed and updated Contingency Plan (CP) using local guidelines.