VICTOR LARNOR NYARKO,
Tel # 571-338-1568,
E-mail: nyarkoteh@gmail.com
Alexandria, Virginia

EXPERIENCE SUMMARY:

Mr. Nyarko is a cyber security and risk management professional, with over 10 years of professional work experience in the Information Technology Security industry. An accomplished and focused professional with diverse skill set, which encompasses systems security and risk management, security controls assessment and testing and security metrics and documentation development. He is also a strong advocate and adherent to scope, time and quality management and treats milestones as sacred.

Skills:

- ○ *Ability to execute security controls assessment, including 800-53 compliance in accordance with NIST RMF.*
- ○ *Experience in the practice of Agile Methodology.*
- ○ *Knowledge of network protocols, TCP/IP, and common security vulnerabilities.*
- ○ *Strong knowledge of FedRAMP and FISMA Assessments.*

- ○ *Thorough knowledge of federal laws and directives pertaining to information security*
- ○ *Experience using security scanners (e.g., Nessus, Netsparker, etc) and remediating vulnerabilities.*
- ○ *Able to update, define, and evaluate cybersecurity risk indicators, including cyber threats, and vulnerabilities.*
- ○ *Threat Modeling: Define, Visualize, Identify, Mitigate & Validate*
- ○ *Ability to provide as needed in the following areas:*
- ✓ *Governance, Risk and Compliance (GRC)*
- ✓ *Policy Development*
- ✓ *Security Architecture and Design*
- ✓ *Security Engineering Support*
- ○ *Strong ability to make recommendations and technical presentations to senior management.*
- ○ *Enormous collation, preparation and tracking ability and management of all documentations through the RMF process.*
- ○ *knowledge of RMF tools, system, and reporting mechanisms/requirements for A&A.*
- ○ *Knowledge of Security Information and Event Management (SIEM)to correlate and identify indicators of threat activity.*
- ○ *Experience with project management methodology.*

PROFESSIONAL EXPERIENCE:

Leidos

Snr. Information Security/Assurance Specialist 10/ 2023-

- *Lead the Cyber ALF Team in the implementation of cybersecurity through the Acquisition Lifecycle Framework (ALF) within components of the Federal Agency.*
- *Review the phases of ALF vis-à-vis the Risk Management Framework (RMF).*
- *Perform security analysis using NIST SP 800-37, NISP SP 800-39 and 800-53.*
- *Perform cybersecurity reviews for all information systems acquisitions as part of ITAR.*
- *Review cybersecurity and security clauses in RFPs, SOWs, etc, as part of ITAR.*
- *Ensure that the Cyber ALF implementation aligns with all policy instructions & directives.*

Accenture Federal Services

Senior Assessment & Authorization Specialist 09/2019- 10/2023

Led the Assessment and Authorization team and coordinated artifacts collections efforts.

- *Performed Assessment of security controls: Testing, Examine & Interview.*
- *Ensured that security controls are implemented correctly, operating as intended and producing the desired outcome for FedRAMP and FISMA assessments.*
- *Select, review, and assess security controls, including privacy controls.*
- *Put the ATO package together for the Authorization Official, which includes the SAR, POA&M, and the SSP.*

Senior Security Specialist

- *Developed and gathered requirements from the Presidential Executive Order 14028 and other OMB memoranda, for the Zero Trust program.*
- *Created Zero Trust Assessment framework for Gap Assessment.*
- *Created Requirements Traceability Matrix (RTM) for each of the 5 CISA Zero Trust pillars: Identity, Device, Application, Network and Data.*
- *Mapped the Zero Trust Maturity Models to the requirements.*

Performed gap analysis of the organization's current state and the future state as reference to the Zero Trust principles.

Information System Security Officer (ISSO)

- *Drafted, reviewed, and updated Risk Management Framework (RMF) artifacts required for risk compliance.*
- *Coordinated with Operations and Maintenance (O&M) teams to drive compliance with Security Controls and requirements.*
- *Worked with System Owners and controls assessors to draft achievable Plans of Actions & Milestones (POA&Ms) to remediate findings Monitor and reporting on POA&M remediation activities.*

- Served as a Point of Contact (POC) for cyber security questions.
- Advised System Owners on cyber security best practices.
- Provided clarification on cyber security policies and regulations.
- Coordinated with Information System Security Managers (ISSMs) and Operations and Maintenance (O&M) teams in support of account approvals.
- Coordinated with O&M and Identity Credentials & Access Management (ICAM) teams to manage user authentication and management.

Information System Security Officer-ISSO

- Provided support for Cybersecurity Maturity Model Certification (CMMC).
- Reviewed existing client's Policies, Standards and Best Practices to map the security controls to the CMMC module in ServiceNow.
- Aligned security controls to key regulations such as 800-171, CMMC, FedRAMP, 800-53
- Performed security controls analysis for the CMMC controls mappings to NIST 800-171.
- Worked with Internal Audit to track security owned issues and work with the security issue owners to define Management action plans (MAP)
- Coordinated security programs activities, including audits, deliverables, security documentation (SSP-MARS-E/NIST 800-53r5)
- Identified and tracked security issues throughout the organization that are not in compliance with client's policies and standards and work with the business to mitigate them.
- Created operational and executive metrics for reporting and tracking security issues and prepared business reports for different audiences throughout the organization including senior executives.
- Monitored the implementation of mitigating projects for timely remediation.
- Worked with the Security Governance team to provide inputs to security policies and standards based on analysis from security issues.
- Worked with stakeholders to report and update on Customer Audit Findings

Security Delivery Specialist

Managed the end-user based of the Enterprise Cyber Governance System (RSA Archer), a Federal Agency's POA&Ms and systems inventory records management system.

- Successfully trained over 30% of the current ECGS end-users on POA&Ms tracking, remediation, and systems reporting.
- Developed a process of analyzing and reporting on quarterly systems inventory and POA&Ms management records.
- Identified a methodology to track and document all "Delayed POA&Ms" in ECGS for remediation and mitigation.

- *Used excel spreadsheet and other capabilities to analyze and document FISMA reportable systems counts.*
- *Performed monthly independent Verification & validation analysis on POAMs, Systems Inventory data, including FISMA Reportable Systems count.*
- *Quarterly analyzed and reported on the Systems Inventory and POA&Ms data calls.*
- *Provide ECGS end-user support and monitor the mailbox for issues resolutions.*
- *Developed and updated the ECGS User manual and uploaded it to SharePoint.*
- *Updated the Powerpedia page of the ECGS with newer contents.*
- *Engaged in regular communication with all information security Subject Matter Experts (SMEs) and stakeholders.*

Defense Point Security/System1, Inc
Senior Security Controls Assessor *07/2018-09/2019*

- *Assessed and tested security controls for both cloud-based and on-premises systems to ensure the controls are implemented correctly, operating as intended, and producing the desired outcome for ATT, annual ATO and Ongoing ATO at a Federal Agency. This is to ensure FedRAMP and FISMA compliance and reporting.*
- *Performed Cloud Platform assessment for AWS East/West and EPIC, for FedRAMP Compliance.*
- *Developed and compiled security controls artifacts request list for the internal assessment team for easy identification of security controls mapping.*
- *Developed and designed security controls test plans, security test and evaluation report (ST&E) and security test scripts for security assessment report documentations.*
- *Worked with ISSOs to ensure that the enclave (system of systems) is established, maintained, and operated in a manner that reflects the organization defined standards as well as FISMA standards.*

BAE Systems, Inc.
Information System Security Officer (ISSO) *0 6/2016-07/2018*

- *Provided direct support to Federal Customers' Continuous Monitoring program.*

  Conducted interviews, documentation reviews, and other data gathering activities.
- *Analyzed Security controls, security planning, policy and procedures development, security controls assessment, risk analysis, and the development of recommended risk mitigation solutions.*
- *Tracked and coordinated mitigation activities with system owners and IT support staff, to reduce risk to the systems by managing and facilitating risk mitigation activities.*
- *Managed and edited the documented status of mitigation plans of action and milestones in tools, such as the Cyber Security Assessment and Management (CSAM).*

- *Developed and updated security authorization documentation, to include the following: System Security Plans, Risk Assessments, Contingency Plans, Procedures and Test Results,*

Security Assessment Plans and Reports, Configuration Management Plans, Interconnection Security Agreements and Memorandum of Understandings, Privacy Threshold Analysis, Privacy Impact Assessments

The Midtown Group *02/2014-06/2016*
Security Analyst

- *Assisted in the development of technical SOPs.*
- *Scheduled and lead integrated project team meetings.*
- *Awareness of DoD and NIST Specific regulations to support authorization of customer systems.*
- *Responsible for managing projects throughout the ATO process.*
- *Played key role as Subject Matter Expert in ensuring security baseline met NIST Standards.*
- *Guided leadership and customer security techniques and compliance procedures.*
- *Supported security tests and evaluations (ST&Es).*
- *Created and tracked POA&Ms.*
- *Provided security support and evaluation to development teams to integrate Information assurance /security throughout the System Life Cycle Development of major and minor application releases.*
- *Investigated, documented, and gathered information on data security recommendations.*
- *Reviewed ATO packages for security issues and provided guidance and expertise in resolving issues to support accreditation activity.*

<u>EDUCATION:</u>

- *M.S., Information Systems Management, Strayer University. Washington, DC*
- *B.S., Mathematics, University of Cape Coast, Ghana.*

<u>Certifications:</u>

- *AWS Certified Developer-Associate*
- *Security+*
- CAP
- CISM