|  |
| --- |
| Los Angeles, CA **|**(213)-332-4168 **|**asozed11@gmail.com |

.

**ASORO AIZEYOSABO**

|  |  |
| --- | --- |
|  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Professional Summary | Skilled Information Security Analyst, knowledgeable in risk management framework (RMF), systems development life cycle (SDLC), security life cycle, and vulnerabilities management using FISMA, FedRAMP, HIPAA, and applicable NIST standards. Organized, Solutions-focused, deadline-focused, team oriented, work well independently, or in team providing all facets of computer supports with in-depth knowledge and understanding of numerous software packages and operating systems. A proven project and team lead with aptitude for good customer service, leadership, excellent communication (both oral and written), and presentation skills. Specialized in providing IT security expertise and guidance in support of security assessments and continues monitoring for government and commercial clients.  **Functional areas of expertise include:**   |  |  | | --- | --- | | * Assessment and Authorization (A&A) * IT Security Compliance * Vulnerability Assessment * Vulnerability Scanning * Security Test and Evaluation (ST&E) | * Certification and Accreditation (C&A) * Risk Assessment * Systems Development Life Cycle * Technical Writing * Project Management and Support | |

|  |  |
| --- | --- |
|  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Skills | |  |  |  | | --- | --- | --- | | * Tenable Nessus Vulnerability Scan * MS office suite (Visio, Excel, Word, PowerPoint) * GRC Tool: CSAM, eMASS, CSET, and more * Splunk SIEM/Tripwire/ ServiceNow/Remedy * AD, SQL, Linux, Python, Arduino, Debugging * AWS services such as EC2, S3, RDS, VPC, Lambda, IAM, and CloudFormation. | * Plan of Actions & Milestones (POA&M) * Risk Mitigation * HIPAA compliance * Project Management * Incident Reponses & Tracking |  | |

|  |  |
| --- | --- |
|  |  |

|  |  |
| --- | --- |
| Work History | IT SECURITY ANAYLST 05/2021 to Present  **Panthergon IT & Cyber Security Solutions (PITCSS), LLC, Laurel, MD**   * Facilitated and supported client’s security policies and compliance activities for vulnerability management, incident reporting, mitigation, and continuous monitoring for all clinical technologies, systems, components, networks, and applications; supported full life cycle of HIPAA compliance, and assessment & authorization (A&A) processes * Developed, reviewed, and updated Information Security System Policies, System Security Plans, and Security baselines in accordance with NIST, FedRAMP, FISMA, OMB App. III A-130 and industry best security practices * Direct experience with formatting, customizing, and providing feedback for documentation relating to Information Assurance & IT Security Vulnerability * Reviewed authorization documentation for completeness and accuracy for compliance * Facilitated Security Control Assessment (SCA) and Continuous Monitoring Activities * Executed examine, interview, and test procedures in accordance with NIST SP 800-53A * Ensured cyber security policies are adhered to and that required controls are implemented * Assisted team members with proper artifact collection and provided guidance and examples of artifacts that will satisfy security control requirements during assessments * Updated and reviewed A&A Packages to include Core Docs, Policy & Procedures, Operations and Maintenance Artifacts, SSP, SAR, FIPS 200, FIPS 199, POA&M, CPTPR, BIA, PTA, PIA, and more * Collected Operation and Maintenance artifacts on an ongoing basis so that Security Control Assessment (SCA) is seamless * Uploaded supporting docs in the System’s Artifact Libraries, Google Docs, and CSAM * Updated, reviewed, and aligned SSP to the requirements in NIST 800-53; so that assessments can be done against the actual requirements and not ambiguous statements * Managed vulnerabilities with the aid of Nessus vulnerability Scanners to detect potential risks on a single, and multiple assets across the enterprise network * Reviewed SAR post assessment; created and completed POA&M’s milestones to remediate findings and vulnerabilities * Monitored security controls post authorization to ensure continuous compliance with the security requirements   **it security engineer** 07/2020 to 05/2021  **Xzentia, LLC.**   * Facilitated implementation of security controls to protect hospital systems and data against unauthorized access, modification, or destruction * Conducted regular security controls assessments and audits to identify vulnerabilities within the hospital’s IT infrastructure * Coordinated with IT and administrative staff to ensure that security policies are understood and adhered to * Provided training and guidance to hospital staff on cybersecurity best practices * Prepared and maintained documentation related to security certifications and accreditations, ensuring all systems and software comply with established standards |

|  |  |
| --- | --- |
|  |  |

|  |  |
| --- | --- |
| eDUCATION | * Associate of Science (AS) in Computer Science| Santa Monica College, Los Angeles, CA |

|  |  |
| --- | --- |
|  |  |

|  |  |
| --- | --- |
| Other Skills & Competencies | * Ability to establish and maintain effective working relationships with clients and co-workers. * Skills in interviewing users to help analyze and resolve issues. * Strong organizational, analytical and planning skills * Ability to read and interpret system security policies, rules and regulations. * Ability to communicate security and risk-related concepts to both non-technical and technical audiences. * Strong communication (verbal & written) and presentation skills. * In-depth knowledge of AWS security services, including AWS Identity and Access Management (IAM), AWS Key Management Service (KMS), and AWS Security Hub. * Excellent communication, leadership, and problem-solving skills. |