**[Information Systems Engineering](https://www.postjobfree.com/resume/ad323p/information-systems-odenton-md)**

**Location:**Odenton, MD

**Posted:**March 03, 2024

**Contact Info:**

[agrant30@yahoo.com](mailto:agrant30%40yahoo.com?subject=Information%20Systems%20Engineering)

[410-841-8146](tel:+1-410-841-8146)

[pdf](https://www.postjobfree.com/resume-download/ad323p?output=pdf) [docx](https://www.postjobfree.com/resume-download/ad323p?output=docx) [txt](https://www.postjobfree.com/resume-download/ad323p?output=txt)[**Email to me**](https://www.postjobfree.com/contact-candidate/ad323p/information-systems-odenton-md?etr=%20id=)

Top of Form

Your Email: cs@advanceqt.com [change email](https://www.postjobfree.com/change-email)

**Subject:**Response to your resume Information Systems Engineering

Message 

Job Description (optional) 



Bottom of Form

**Resume:**

Anthony L Grant

2569Vireo Court

Odenton, MD 21113

410-841-8146

Agrant30@yahoo.com

PROFFESSIONAL SUMMARY

Twenty-five (25) years of experience supporting program initiatives across multiple networks in the Intelligence Community. Driven, enthusiastic, innovative professional with varied experience in systems engineering, software engineering/development; focused on sustainable design and operations. Highly effective working with teams of developers to produce results on projects.

SECURITY CLEARANCE

•TOP SECRET SCI/FSP – CURRENT

SKILLS

Systems Engineering/Requirements Management

Network Security

Data Flow analysis

Atlassian suite “Confluence and Jira/” Bit Bucket”

CERTIFICATIONS

•CompTIA Security+-CE

•Certified in Risk and Information Systems Control (CRISC)

•Certified Data Privacy Solutions Engineer (CDPSE)

•Certified Information Systems Security Professional (CISSP) (Exam date: March 2024)

EDUCATION/TRAINING

University of Phoenix – MS - Computer Information Technology

Columbia Union College – BS - Information Systems

SAIC Penetration training course

Computer Forensic Specialist Training

National Security Agency Information Assessment Methodology (IAM) and Information Evaluation Methodology (IEM)

Cisco Certified Network Administrator (CCNA) Course

PERSONAL ATTRIBUTES

Strong Communicator

Team Leader

Intelligent and Creative

CORE PROFFESSINAL COMPETANCIES/AREAS OF EXPERISE

OPERATING SYSTEMS

Linux

Windows

CYBERSECURIY TOOLS

•Nessus (Security Center/ACAS)

•Exacta

•Tripe-wire

FRAMEWORK AND METHEDOLGIES

•Scaled Agile Framework (SAFE)

•National Institute of Standards and Technology (NIST)

•System Development Lifecycle (SDLC)

•Federal Information Processing Standard (FIPS)

•Risk Management Framework (RMF)

WORK EXPERIENCE

Accolade Systems – Nov 2023 – Present. Sr Systems Engineer/Information Systems Security Engineer – Enterprise Infrastructure Team

Partner with team of software and system engineers to provide over-site and services to data Services Team (Scrum Master).

Design, implement and manage Identity and Access Management (IAM), Role-Based Access Control (RBAC) and Privileged Access Management (PAM) solutions to ensure secure and efficient user and client access to applications, systems, and environments.

Collaborate with Security Operations on security and risk-related issues such as Role Based Access Control (RBAC), guiding product teams to develop a plan to change or resolve security/risk issues.

Familiar with Release Planning, Sprint reviews and Scrum of Scrum artifacts

Coordinates with Product design security design of new and existing features and provides engineering direction and oversight during planning, development, testing and implementation.

Analyzes user’s requirements, concept of operations documents, and high-level system architectures to develop system requirements specifications. Analyzes system requirements and leads design and development activities.

Guides users in formulating requirements, advises alternative approaches, and conducts feasibility studies. Provides technical leadership for the integration of requirements, design, and technology.

Incorporates new plans, designs, and systems into ongoing operations.

Develops technical documentation to include system Architecture and system design documentation.

Interacts with the Government regarding Systems Engineering technical considerations for associated problems, issues, or conflicts.

Communicates with other program personnel, Government overseers, and senior executives.

Operational experience with value delivery using Agile methodologies of Project Management

Possess persuasive communication and presentation skills, excellent people skills and skills to remove team impediments.

Strong understanding of Identity and Access Management solutions.

Experience integrating applications with CASPORT.

Experienced with web service experience using REST, SOAP, XML, and JSON

NiFi, LDAP experience

Possess the ability to communicate ideas and status updates clearly and professionally to peers, management, and external stakeholders including the customers.

Experienced with functional testing, integration testing, system testing, and user acceptance testing.

Experienced in supporting incremental software development projects using Agile Scrum approach to evaluate and assess software.

Ability to create test plans, test procedures, user stories, change requests and problem reports.

Experience interacting with Product Owners, Business Analysts, Scrum Masters, and Developers

Ability to apply test estimation techniques to software development efforts.

Experience using JIRA and Confluence.

Ability to review software development and provide sound requirements and feedback.

Support the Government in the enforcement of the design and implementation of trusted

relationships among external systems and architectures.

Perform system or network designs that encompass multiple enclaves, to include those with

differing data protection/classification requirements.

Applied Insight July 2021 – Nov2023 - Systems Engineer - Cross Domain Solutions (CDS) Engineering Team - Present

Reviews and tests data types for adherence to the design requirements and documents test results.

Provides technical and management support to improve the inherent security of agencies boundary through actionable engineering practices and in concert with host agency best practices.

Enables cross-domain information sharing, including executing transfer of data transfer over secure protocols through use of dataflows.

Works directly with technical POCs to identify gaps in CDS capabilities, designs solutions for the gaps, and supports engineering teams in implementation of solutions Ensure effective, periodic review and control of the evolving configuration of a system, both hardware and software components and associated documentation, during the life of the system

Data format analysis on data (JSON, XML) to determine security policy requirement.

Subject matter expert in meetings regarding CDS processing of data management request.

Support engineering, design, and implementation of new and/or improved CDS capabilities.

Utilize Splunk (end user) to facilitate analysis of Data management Request.

Contributes to the development of sections of systems engineering documentation such as System Engineering Plans, Initial Capabilities Documents, Requirements specifications, and Interface Control Documents

Manages system requirements and derived requirements to ensure the delivery of production systems that are compatible with the defined system architecture(s)

Assists with the allocation of the same to individual hardware, software, facility, and personnel components.

Coordinates the resolution of action items from Configuration Control Board (CCB) meetings, design reviews, program reviews, and test reviews that require cross-discipline coordination.

Perform analysis of technical alternatives for a project and make preliminary recommendations.

Entegra Systems – Systems Engineer/Systems Security, AWS Security – Mar 2021 – July 2021

Analyze user requirements to derive software design and performance requirements.

Write or review software and system documentation.

Design or implement complex database or data repository interfaces/queries.

Develop or implement algorithms to meet or exceed system performance and functional standards.

Assist with developing and executing test procedures for software components.

Experience working with Agile, JIRA, and Confluence

Designed networking technologies like TCP/IP and UDP multi-cast into security design solutions to support development initiatives.

Managing services that detect and automate the mitigation of cybersecurity threats across Amazon’s infrastructure.

Worked with data scientists, software development engineers, and other security engineers across multiple teams to develop innovative security solutions through implementation of NIST security controls.

Developed and established baselines for security controls implemented in cloud infrastructures; that included cyber security controls; to include controls designed to prevent attacks on data; security measures in cooperation with cloud service providers.

Assisted in building and managing services that detect and automate the mitigation of cybersecurity threats across Amazon’s infrastructure.

Worked with data scientists, software development engineers, and other security engineers across multiple teams to develop innovative security solutions at massive scale.

General Dynamic Oct 2020 – Mar 2021 – Subject Matter Expert (SME) Systems Security Engineer (ISSE). Resigned due to Covid-19.

Translate business outcomes, business requirements and technical requirements into technical designs for new technology solutions or enhancements to existing technology solutions, while following architectural standards and organizational policies

Analyze user requirements to derive software design and performance requirements

Provide recommendations for improving documentation and software development process standards.

Write or review software and system documentation.

Develop software solutions by analyzing system performance standards, confer with users or system engineers; analyze systems flow, data usage and work processes; and investigate problem areas.

Implement recommendations for improving documentation and software development process standards.

Confer with system engineers and hardware engineers to derive software requirements and to obtain information on project limitations and capabilities, performance requirements and interfaces.

KeyW Corporation Feb 2018 – Oct 2020 – Information Systems Security Manager (ISSM)

As Information Systems Security Manager, I was responsible for management of all cybersecurity operations and related processes to include overall leadership information assurance task order/contract governance, risk, and compliance, encompassing role will assure compliance with applicable information assurance processes, encompassing system accreditations, and security of IT systems using Government and industry IA standard, policies, guidelines and best practices. In support of IT transformational activities for a large US Government customer. Performance locations included multiple CONUS sites. The primary contract objective was to provide world-class Information Management and Information Technology (IM/IT services that provide secure, available, dependable, and deliver responsive, dependable customer support, technical support activities included IT infrastructure and shared services, general IT, cybersecurity services, engineering design, telecommunications services, emergency response and special projects.

Primary advisor to the Company Director of Security, Facility Security Officer (FSO) on all classified information systems security matters and liaison to the local Defense Security Service

Performed as primary customer contact for program activities, leading program review sessions with customer to discuss cost, schedule, and technical performance.

Establishes design concepts, criteria and engineering efforts for product research, development, integration, and test.

Establishes milestones and monitors adherence to master plans and schedules, identifies program problems, and obtains solutions, such as allocation of resources or changing contractual specifications.

Directs the work of employees assigned to the program from technical, manufacturing, and administrative areas.

Maintain secure operational environment!

Effective application of service cost and service management practices to achieve full cost transparency.

Lead ISSO team; enabling the accreditation of deployed systems.

Provided, guidance, support, and validation of system security documentation for division Information Systems Security Officers (ISSOs)

•Prepared security metric for executive management

•Lead and managed, implemented security vulnerability management operations; ensuring implementation of systems scan validations.

•Initiate and manage Assessment and Authorization (A&A) processes.

•Conducted and managed risk and vulnerability assessments of planned and installed information systems to identify vulnerabilities, risks, and protection needs.

•Provide solutions to complex problems that require the regular use of expertise and creativity.

Engility Corporation - Aug 2017 – Feb 2018 (Lead - Senior Information Systems Security Officer)

•Risk Management Framework Implementation with emphasis on continuous monitoring and strategic risk mitigation.

•Vulnerability Assessment and security testing implementation using Nessus and proprietary network scanning tools.

•Implementing security enterprise initiatives across networks with emphasis on security system configuration, port security, patching and administrative policy

Northrop Grumman Jan 2017 – Aug 2017 (Information Systems Security Engineer)

•Participated on engineering team for the design, development, implementation and/or integration of secure networking, computing.

•Participates as a security engineer on engineering team for the integration of Information Assurance architectures; systems; or system components.

•Applied knowledge of Information Assurance policy; procedures; and workforce structure to design; develop; and implement secure networking; computing; and enclave environments.

•Supported security planning, assessment; risk analysis; and risk management.

•Identifies overall security requirements for the proper handling of Government data.

•Interacts with the customer and other project team members.

•Performs system or network vulnerability analysis (Nessus) and technical testing that encompasses multiple enclaves; to include those with differing data protection/classification requirements.

•Recommends system-level solutions to resolve security requirements.

•Create documentation to support information system authorization/accreditation packages.

ManTech International - Nov 2015 – Dec 2016 (Principal Information Systems Security Engineer)

•Conduct assessments of existing IT architecture for compliance with security requirements from applicable security frameworks

•Supports various programs and projects throughout the Department of Defense. Intelligence Community in support of and Federal sponsors as the Cybersecurity Lead, or in direct support of the Cybersecurity Lead as the project Information Systems Security Officer

•Create documentation to support information system authorization/accreditation packages.

•Provide continuous monitoring support for information systems.

•Develop IT architecture deliverables, specific to information security countermeasure implementations, for operational systems and systems under development.

Computer Sciences Corporation - Nov 2012 – Nov 2015 (Information Systems Security Engineer

•Manage information technology projects to facilitate protection of information system assets.

•Manage and oversee the development, revisions, and maintenance of System Security Plans (SSP), accreditation documentation.

•Providing security coordination and review on all system test plans

•Conduct system audits and surveys, and gathers pertinent security documentation for inclusion into system accreditation packages (XACTA)

•Coordinate with echelons of management to provide security management policy guidance.

•Conducts vulnerability management, security configuration management (Tripe-wire vulnerability management tool)

•Managed Information Assurance Vulnerability Alert (IAVA’s)

•Reviewing and developing AIS accreditation/ certification support documentation.

•notifying the customer when changes occur that might affect system accreditation/certification.

•Performing system and network inspections

•Identified vulnerabilities and implemented countermeasures.

Apex Systems – Jan 2012 to Nov 2012 (Sr. Information Systems Security Officer)

•Managed, direct, and conduct reviews of the system(s) security posture through audit reviews/analysis, security compliance.

•Developed a relationship and partner with Sponsors C&A teams in support of infrastructure certification and accreditation procedures.

•Collaborated with customers (internal and external) during the design and development process to employ best practices when implementing security requirements and controls.

•Coordinated with security managers (both corporate and local) and Information Systems Security Engineers (ISSE) to define, implement, and maintain information security policies, strategies, and procedures.

•Conducts security analysis to support Defense Information Systems Agency (DISA) ports, protocols, and services initiatives.

•Performs evaluations of ports and services to ensure compliance with certification and accreditation methodologies.

•Implement and direct change management policies and procedures for hardware and/or software deployed, refreshed, or decommissioned.

•Administrated logical access on various platforms and applications.

•Analyzed security processes and procedures for process improvement Perform vulnerability assessments to ensure compliance with DOD directives.

G2, Inc. Jan 2010 – Nov 2012 (Senior Information Systems Security Engineer)

•Manage the new hire process for ISSO/ISSM support to ensure direct charge work is sufficient and has sustainable coverage.

•Implemented Certification & Accreditation (C&A) services through Security Incident Management, Configuration Management (CM) and Change Control Board (CCB), Remediation of POA&Ms and Identity and Access Management for Enterprise level network and applications.

•Developed policies, providing support for operational and security tasks.

•Provided security engineering designs and implementation in all aspects of Information Assurance and Information Security (InfoSec) Engineering.

•Assessed and mitigated system security threats/risks throughout program life cycles in support of application development projects

•Validated system security requirements definition and analysis.

•Established system security designs, implementing security design in hardware, software, data, and procedures.

•Verified security requirements.

•Performed system certification and accreditation planning and testing and liaison activities and supported secure systems operations and maintenance.

•Conducts certification and accreditation in support of the commercial and National Security Agency (NSA) and Department of Defense (DOD) software development efforts.

•Wrote Privileged Users Guide (PUG), Security Concept of Operation (SECONOPS) in support of network centric systems that support NSA and DOD mission objectives.

•Conducted Security Testing utilizing Technical Implementation Guides (STIGS) to support the development and security compliance of the Fight-Club application.

•Review of all C&A documentation (DIACAP) conducting analysis of SRTM security artifacts, DIACAP implementation Plan, O&M Plans.

Science Application International Corporation (SAIC) Apr 2006 – Jan 2010

Lead, Security Teat Team – Lead PKI Instructor - Senior Information Systems Security Engineer

•Created and reviewed System Security Plans (SSPs) for in accordance with DCID 6/3, NIST SP 800, ICD 503 and the NISCAP

•Conducted and reviewed scans using Nesses, Nmap and Nikko to facilitate testing technical controls to support certification and accreditation activities.

•Reviewed and analyzed audit logs to determine security breaches.

•Conducted war-driving to identify rouge wireless access points for inclusion into overall vulnerability assessment.

•Conducted vulnerability and compliance security scans to include monthly, quarterly, and annual: Nesses and DISA STIGs

•Exceptional Knowledge of Windows Server Update Services

•Supported Defense Information Systems Agency (DISA) (Project Lead) in the implementation of Public Key Infrastructure training program, Instructing DOD and private industry attendees in policy, implementation, operations, and coordination of PKI emerging technologies.

•Performed evaluation, risk identification, and definition of mitigation strategies for the DOD Federal Information Security Management Act (FISMA) requirements.

•Conducted computer security engineering for classified and unclassified networks and supported the government in preparation C&A; planning and implementation by reviewing and developing program documentation, ran DISA Gold Disk for certifications; recommending computer security requirements, supporting development of local area network and wide area networks.

Improsive Technologies Oct 2003 – Apr 2006 Senior Information Systems Security Engineer

•Manage/schedule mandatory IS patching, updating, and scanning based on vulnerabilities and threats or regulatory compliance; maintain the day-to-day security posture and continuous monitoring for all systems.

•Contracted to SAIC to provide the auditing, assessment and INFOSEC direction.

•Support the Federal Government in security requirements of FIPS 199 and NIST security standards to include NIST Risk Management

•Development of System Security Plans (SSPs), Risk Assessments, and Asset Valuations. Proficient in information security concepts and application security “best practices.”

•Preparing highly confidential documentation and ensuring compliance with security standards and procedures.

•Development and execution of C&A, ST&E and SSP documentation along with vulnerability testing.

•Exercised excellent judgment in structuring and organizing work, setting priorities, balancing the interests of clients, and readily adjusting priorities to respond to customer demands.

•Perform FIPS 199 and NIST security standards-compliant statistical security analysis on a multi-tiered system according to vulnerability, risk, security features, and technical areas.

•Identified anomalous behavior in data collected during a network intrusion or suspected intrusion.

•Applied network intrusion knowledge to the development of countermeasures that will detect, remove, and mitigate intrusion activity.

BAE Systems, Alexandria, VA (Senior Security Engineer) Jan 2001 - Oct 2003 Senior Information Systems Security Engineer

•Conducted C&A on systems using the Department of Defense (DOD) Information Technology Security C&A process (DITSCAP) and National Information Assurance C&A Process (NIACAP).

•Develop C&A documentation, to include System Security Plans, Requirements Traceability Matrices, Security Test & Evaluation Plans, Risk Assessments, Contingency Plans, Security Awareness Plans, Incident Response Plans, MOAs, and other Security Plans.

•Wrote Systems Security Authorization Agreements (SSAA) and Systems Security Plans (SSP) to facilitate C&A of major applications on mainframe platforms.

•Performed Certification and Accreditation Testing.

•Performed risk assessments to include discovery, analysis and mitigation of software and network system vulnerabilities utilizing a variety of testing methodologies.

•Assessed and evaluated administrative controls (policies) supporting major applications.

•Analyzed software analysis results from network and database analysis tools to identify vulnerabilities and formulate risk mitigation strategies.

Northrop Grumman Technical Services, Laurel, MD (Senior Security Engineer) Jan 2000 - Jan 2001 Information Systems Security Engineer

•Collected and analyzed security and IA network infrastructure data and created network design schematics on U.S Navy and Marine Core facilities critical to the design implementation and deployment of the Navy Marine Core Internet (NMCI) project.

•Conducted IV&V Risk mitigation on vulnerabilities identified in Department of Justice (DOJ) risk assessments for C&A of major applications.

•Conducted web and network analysis using software analysis tools.

•Performed requirements analysis, risk assessments (Risk Watch), test, and support for C&A of multiple computing platforms.

•Performed network security consulting analysis that included monitoring of network infrastructures for vulnerabilities using network and host-based intrusion detection systems.

Technology Automation and Management Inc. Nov 1999 – Jan 2000 Information Systems Security Engineer

•Applied software security engineering and assurance principals in the design, code, test, and integration of security-based components and solutions into the U.S. Army Joint Total Asset Visibility (JTAV) Windows NT web-based system.

•Evaluated, test and installed software security products onto secure architectures.

Integrated security methodologies into all phases of SDLC with emphasis on analysis, design, integration, testing.

•Implemented Configuration/Change Management Control through identifying, controlling, and auditing all changes made to systems.

Troy Systems Fairfax, VA (Security Analyst) Oct 1995 – Nov 1999 Security Analyst

•Provided full life cycle analysis, design and programming support for the development and maintenance of corporate Management Information Systems web-enabled applications, involving programmatic planning, monitoring of software and hardware development activities and object-oriented design software coding.

•Developed security risk assessment process for remote connections to SUN Partners/Vendors.

•Conducted risk assessments and remediation plans.

•Developed team website, infrastructure process and procedures of Information Security team.

•Administrated logical access on various platforms and applications.

•Analyzed security processes and procedures for process improvement.

•Evaluated and implemented security software tools.

United States Air Force - Local Area Network Senior ranking officer Security Manager. Oct 1985 – Oct 1995

• Performed trouble shooting on hardware problems.

• Configured routing protocols and implemented system designs.

• Configured and implemented LANs, ACLs.

• Configured static routes.

• Monitored and provided Maintenance to the LAN which consists of more than 150 user