Principal IT Security Analyst Principal IT Security Analyst Principal IT Security Analyst Acworth, GA

Work Experience Principal IT Security Analyst KBRWYLE - Charleston, SC October 2016 to June 2019 KBRwyle provides specialized engineering, professional, scientific, and technical services for customers in the U.S. Department of Defense, NASA, and a variety of other federal agencies. Its areas of expertise include  systems and sustainment engineering, program and acquisition management, life science research, space  medical operations, information technology and test, and evaluation of aircraft, weapon systems, and networks.    Support training for validation process and write precise as well as thorough Validation Documents included  not restricted to Validation Reports, Validation Plans, Master Document Lists. Analyze results from allotted test  scripts to assure accurate, complete documents and import results to PCAT. Perform security validation, testing, and auditing with the NIST guidance: Application Security and Development; Windows and RedHat Operating  Systems; SQL Server and Oracle Database; Active Directory; McAfee Antivirus; VMWare VSphere and clients;  Layer 2 and 3 Cisco Switches; and Common Criteria Identifier. Government IA Lead CribMaster - Marietta, GA September 2014 to May 2016 Stanley Black & Decker is a diversified global provider of hand tools, power tools and related accessories, and mechanical access solutions. CribMaster is $70M global leader in inventory and asset management solutions for  industrial environments.  Advice the executive management on information security requirements, Payment Card Industry (PCI)  compliance, and risk mitigation. Audit and review of software configuration settings on application security and development via the Security Technical Implementation Guide (STIG). Responsible for all documentation and IT  Governance compliances procedure to maintain DoD certifications for CribMaster software. Provide information  security briefing, threat management, and online instruction to meet annual security training requirements. Information Assurance Analyst/ Cyber Security Analyst, Conscious Security and Smartronix Marine Corps Logistic Base - Albany, GA March 2011 to September 2014 Albany, GA  March 2011 - September 2014  Conscious Security provides IT services to commercial and government organizations. Smartronix, Inc. is a U.S. based, highly reputable information technology and engineering solutions provider specializing in Cloud  Computing, Cyber Security, Health IT, Network

Operations, and Mission-Focused Engineering. Provided the Information Assurance (IA) analysis and certification and accreditation (C&A) expertise required to support the security risk, compliance, impact and execution of all steps necessary for obtaining DIARMF accreditation and maintain complete C&A packages for assigned legacy logistics information systems. Audit security requirements, products, STIG applicable configurations, and network architectures to ensure accreditation documentation met United States Marine Corps (USMC) and DoD IA controls and standards. Provided advice and recommendations on IA and C&A matters, and programmatic support in dynamic and challenging environments, participated in collaboration team meetings to coach program managers and IA practitioners through certification and compliance processes, and tracked critical IA processes and elements through the use of automated and semi-automated tools. Drafted for approval all required provisioning process, configuration control, contingency execution, and artifacts in support of accreditation actions. Maintained the accurate, steady, and consistent flow of information in response to client direction through established processes, threat management and incident reporting. Sr. Computer Network Technologist, Ft Sam Houston, Computer Sciences Corporation, San May 2010 to May 2011 Computer Sciences Corporation is an American multinational corporation that provides information technology services and professional services. Provided advice and recommendations on Information Assurance Security and policies to obtain unit organization DIARMF accreditation. Wrote technical guides and instructions for system administration guides and server / network administration to improve business and technical process. Served as an operator for multiple application platforms such as Army Battle Command Systems (ABCS), virtual drones, and Joint Land Component Constructive Training Capability (JLCCTC). Serve as an instructor of Virtual Battle Space (VBS2) and Force XXI Battle Command Brigade and Below (FBCB2) in facilitating simulated training environment of the WarFighter focus. Sr. Systems Analyst, Ft. Hood Advanced C4 Solutions - Killeen, TX March 2008 to January 2010 Advanced C4 Solutions, Inc. provides converged IP, cyber, and mission support services, as well as professional services. Served as an Information Assurance Security Officer (IASO) for the III Corps Group and with its several tenant units, duties include maintaining National Security Agency (NSA)

certified network safe's access codes, provisioning support, personnel security, and secret level architectural design plans. Additional duties were performed as system administrator and network account processing. Primarily handled the SIPRNET expansion program of the Ft. Hood Base to provide installation, vendor mediation, accreditation, and information dissemination throughout multiple military organizational levels (Company, Battalion, Brigade, and Headquarters) as well with the coordination of vendor contract support. Staff Sergeant Ft Lewis, US Army - Tacoma, WA February 2000 to February 2008 The United States Army is the land warfare service branch of the United States Armed Forces. It is one of the seven uniformed services of the United States, and is designated as the Army of the United States in the United States Constitution. Primary MOS is 25B as qualified for variety of IT and computer-related positions, potentially in systems administration or engineering. Provided service as a systems administrator in a helpdesk and management environment which encompassed Active Directory, Software development, Hardware support, networking support (cabling and design), server management, and information assurance support and provided networking solutions and support under brigade command level units and organizations working with Cisco equipment, Composite HealthCare System (CHCS) and Standard Army Management Information System (STAMIS). Supported vendor products such HP, DELL, and more. Served in multiple and additional roles such as linguist, a combat life saver, hazardous materials handling Non-Commissioned Officer (NCO), supervisor, project officer, database manager, website manager, and instructor. Ensure compliance on Personally Identifiable Information, HIPAA, ISO 27001, and Army Regulation 25-1. Education MS in Information Systems in Systems and Technology South University 2011 Bachelor of Arts in Psychology in Psychology Pasig Catholic College 1999 Skills Security, Information assurance, Network architecture, Oracle, Sql, Nist, Provisioning, Technical support, Authentication, Unix, Dod, Auditing, Risk management, Account management, Security plan, Helpdesk, Architecture Military Service Branch: United States Army Rank: E6 Additional Information 19 years of Information Systems and Technology experience focused on Security in an ever-evolving and changing field under the Department of Defense Information Assurance Risk Management Framework (DIARMF) or previously known as DIACAP.

Served the military for 8 years as an Information Systems Analyst providing technical desktop support, project management, assessment and audit through the Security Technical Implementation Guide (STIG) of the National Institute of Standards and Technology (NIST). Provided Information Assurance and Cyber Security, Certification and Accreditation, and 5 years of compliance internal auditing with several organizations as a contractor and as a permanent employee for 8 years under the multiple facets of environment on medical data protection (HIPAA), planning and delivery (ITIL), risks assessments (DIARMF), documentation requirements (ISO), and security reviews (STIG). Active Government Clearance: Secret.    CORE COMPETENCIES Contingency Plan Backup and Restoral Plan Site Security Plan Validation Tests    Vulnerability Management Validation Plan and Account Management Plan Configuration Change  Procedures Control    Network Architecture Incident Reporting Identification and IT Risk Process and  design and process Management Authentication Assessment    DoD Information Assurance Helpdesk and Security System Application and Provisioning and De-  Risk Management Technical Support NIST Controls Auditing Provisioning Process  Framework (Windows, Unix, Oracle,  SQL, Desktop)

Name: Reginald Nguyen

Email: grant92@example.org

Phone: (652)276-3657