IT Auditor IT Auditor Cybersecurity, IT Security Manager, IT Auditor Woodbridge, VA Maintain a unique set of skills in both Information Technology (IT) and Security. Retired military (US Army Special Ops G2/3 Staff +21 years), and worked as project manager in Information Assurance with (HQDA CIO/G-6) Pentagon staff on the Army Data Center Consolidation Program and on Internet Protocol version 6 (IPv6) conversion Army-wide. Worked with various Government agencies - like Department of Justice (DEA, FBI, BOP, etc.) and the State Department to ensure compliance on various IT systems. Most recently, worked as a sub-contractor for Ernst & Young (EY) as an IT Auditor on Department of Health & Human Services (DHHS) / Center of Medicine & Medicaid Services (CMS) Audit Team for FY 2017. Authorized to work in the US for any employer Work Experience IT Auditor i-VisioNET, Inc - List, CA May 2017 to September 2017 for each of the following WT: NGS Access Control (AC) that comprise of 22 separate support documents to prepare/edit for review; NGS Configuration Management (CM) that comprise of 12 separate support documents to prepare/edit for review; NGS CLAIM that comprise of 37 separate support documents to prepare/edit for review; NGS Common Working File (CWF) System - Verify the entitlement and eligibility for submitted claims prior to processing in FISS, MCS, VMS applications. CWF document that comprise of 19 separate support documents to prepare/edit for review; NGS Fiscal Intermediary Shared System (FISS) that comprise of 28 separate support documents to prepare/edit/review: processes and generates payments for Part A claims. Supported by DXC Technologies (the merger of Hewlett Packard Enterprise and CSC or Computer Science Corp); NGS Multi-Carrier System (MCS) that comprise of 30 separate support documents to prepare/edit for review; NGS Security Management (SM) that comprise of 18 separate support documents to prepare/edit for review; The WT's identify the processes and procedures that provides customized healthcare solutions for federal government agencies. Conducted an extensive research and review of prior year / fiscal year (PY/FY) audits to develop current FY audit requirements. Conduct EY random selection of data populations for testing on a variety of IT financial systems for compliance with FISMA, FISCAM and NIST standards; IT Audit input calculations used to populate the Statement of Social Insurance and Statement of Changes in Social Insurance. Security Manager DynCorp International, LLC March

2013 to April 2017 for DynCorp International (DI) during contract competition, award and transition period of Department of State (DoS) Global Information Technology Modernization (GITM) contract. Responsible for security and information assurance compliance of DoS Foreign Affairs Manual (FAM), National Industrial Security Program Operating Manual (NISPOM), National Institute of Standards and Technology (NIST) requirements. Develops, plans, directs policies and procedures to identify controls and mitigate risks, prevent data losses, and protect the personnel and assets of the program. Assists and Executes required Personnel Security procedures and functions as defined by the NISPOM in support of the DI Corporate Personnel Security and the cognizant Information and Facility Security Officers (FSO), supports systems and services for individuals both within and outside the accredited systems and provides technical and professional leadership to other IT support personnel at multiple operating facilities. Security manager interfaces with federal and government officials as required; will work with various vendors for support and maintenance contracts; will work with internal IT and business groups for support and procurement requirements; and will work with internal asset management and facilities groups. Engagement Manager Project Manager (PM) - Engagement Information Technology Program Manager (PM) D&S Consulting, Inc April 2012 to March 2013 April 2012 - March 2013 Engagement Manager Project Manager (PM) - Engagement Information Technology Program Manager (PM) for ViaTech, Inc. (a DSCI Company) at the Software Engineering Center (SEC) in Aberdeen Proving Grounds (APG), Maryland. Engagement PM to coordinate directly with every Army Fort, Post, Camp, Station or Installation in the Continental United States (CONUS) and Overseas Continental United States (OCONUS) working on the Army Data Center Consolidation Plan (ADCCP); which supports the acquisition activities related to reducing the Army's data center 'footprint' in managing and maintaining overhead cost for the Army; this includes monitoring costs, validating requirements, tracking the schedules and also generating reports back to Congress. Conduct research and analysis to support migration of Army applications into an enterprise environment. The ADCCP strategy will provide the foundation for reducing over 700 CONUS Data Centers to a more manageable and affordable amount to significantly reduce the estimated 14,000 Army applications and infrastructure to support

1.4 million user accounts, including the Army, Army National Guard, Defense Information Systems Agency (DISA), a number of combatant commands and control Commands working with other Agencies. Engagement PM on ensuring 100% of all Army Internet Facing applications (I.F. Apps) is migrated to the DISA Demilitarized Zone (DMZ) or Defense Enterprise Computing Centers (DECCs) during a five-year timeframe. Collaborate with Army Cyber Command on identifying and inventorying all I.F. Apps and sync coordination efforts with the ADCCP migration. Coordinate with the DISA, Program Executive Office Enterprise Information Systems (PEO-EIS) on technical specifications of I.F. Apps migrating to DISA DMZ / DECC. Developed a prioritization plan to retain, retire, maintain locally or migrate I.F. Apps with ADCCP efforts. Ensure Cyber Directorate adheres to the Cyber tasks as depicted in the HQDA ADCCP execution order. Information Assurance Analyst D&S Consulting, Inc June 2010 to March 2012 Department of Defense (DoD) Contractor on Headquarter Department of the Army (HQDA) staff for Chief Information Office (CIO/G-6) Cybersecurity Directorate. Information Assurance Action Officer of the Army Tactical Information Systems (IS) Security Classification Guide (SCG) for System of System (SoS)/Family of Systems (FoS) level Classification guidance. This includes conducting breakout sessions with the PEO Community to identify key security classification issues, developing recommendations to resolve these issues, incorporating proposed changes in the SCG, and gaining concurrence among the key stakeholders. Brief leadership on security updates to gain signatures of the Army leadership. Staff the SCG for CIO/G6 approval. Monitor new equipment fielding to support Internet Protocol version 6 (IPv6) and Public-Key Infrastructure (PKI) integration for NIPRNET / SIPRNET. Determine the level of current state of compliance in satisfying IA requirements as cited by DoD, Joint, and Army regulations. Recommend solutions to resolve IPv6, PKI and other IA implementation issues. Advised on the current IPv6 and PKI issues, identify vulnerabilities, and review supporting mitigation action plan for applicability. Principle Information Security - IT technical lead Directive 63, Inc October 2007 to October 2009 for US Department of Justice - Federal Bureau of Investigation (FBI) in support of the Tactical Operations Support Center (TOSC - a covert facility offsite). Primary work location was at the Engineering Research Facility (ERF) in Quantico, VA. Supported a diverse set of IT systems and

technologies to evaluate and report on the security posture of IT systems being fielded or in development. Evaluate system hardware, system software applications, operating systems, communications interfaces, protocols, and data exchanges to determine the level of compliance with security controls established by Federal and Agency requirements - to include but not limited with FIPS, NIST, DOT and DOD requirements. Report security posture and assess vulnerability and risk assessment of IT systems. Evaluate and test IT systems for classified/unclassified environments. Develop policies and procedures, architectural designs, and Network security analyses on IT systems. Provide mission security support and System Administrative functions on IT systems with best business practices for IT systems, and network infrastructures. Develop contract deliverables on Physical Security, Risk Assessment Reports, Security Test Plans/Test Reports, Enterprise Security scan of IT system(s) for both Windows and MAC base platform, server and Operating System (OS). Review and staff System security plans (SSPs), Standard Operating Procedures (SOPs), Concept of Operations (CONOPS), Contingency of Operations (COOPs), Risk Management and other associated materials for Interim Approval To Operate (IATO / ATO). Document the security posture of IT system(s) and make recommendations to mitigate risks. Oversee and review the work of other security team members work activities products prior to delivery of Government review and approval. IT Auditor - Contractor SNS-One, Inc March 2007 to June 2007 on sub-contract with KPMG independent auditor that performs an evaluation of the Department of Justice (DOJ) Drug Enforcement Administration (DEA), and Bureau of Prison (BOP) general controls environment, using the six control areas of GAO's FISCAM and corresponding critical elements as a guide. To augment the audit steps called for in the FISCAM access controls section, information security specialists will be employed, as needed; to perform additional tests using automated security assessment tools. Utilizing the FISCAM to guide compliance for IT audits tailored unique IT systems within a closed environments. During the planning process, held discussions with the task monitor to determine the extent of necessary logical access controls testing. Assist in performing a review of the general and application controls of the reporting entities IS controls environment that are significant to the financial statements using the following security

guidelines, including future amendments, as required. Independent Consultant The Bode Technology Group January 2007 to March 2007 Responsible for company security requirements, policy, and adherence to DSS established guidelines. Wrote company automated information system security plan (SSP) and standard operating procedure (SOP) for Sensitive Compartmented Information and Special Access Program environment. Contract Program Security Officer (CPSO) - Security Manager DOJ / DOD August 2003 to November 2006 August 2003 - November 2006 Contract Program Security Officer (CPSO) - Security Manager over multiple Special Access Program (SAP) facilities in support of DOD and other Government Agencies. Provided Security and IT oversight and support to ensure compliance with NISPOM / NISPOMSUP and applicable DCID regulations. Platoon Sergeant / Senior Admin Noncommissioned Officer United States Army - Fort Bragg, NC January 1982 to October 2003 US Army Special Operations Command (USASOC) Deputy Chief of Staff Intelligence (G2) Special Security Office (SSO). Perform a variety of sensitive administrative functions for the safeguarding of classified Sensitive Compartmented Information (SCI) for USASOC SSO, USA Special Forces Command, 75th Ranger Regiment and 160th Special Operations Aviations Regiment (SOAR); serves as the Major Command (MACOM) Sensitive Compartmented Information (SCI) Billet manager that provides critical oversight of 1200 Reserve and National Guard SCI billets; maintains multiple sensitive databases containing records and access levels to over 3500 collateral security clearances that requiring access to Sensitive Compartmented Information (SCI) on personnel assigned to USASOC both Active/Reserve military, civilians and contract personnel at Fort Bragg, NC. Education MS in Computer Science University of Maryland University College BS in Information System Management University of Maryland University College Skills Fisma, It Audit Links https://www.linkedin.com/in/dennis-yarbrough-b7979a16/ Military Service Branch: U.S. Army Service Country: United States Rank: Sergeant First Class (SFC / E7) January 1982 to October 2003 Awards U.S. Army Military Awards and Decorations 2003-10 The following awards and decorations were earned during the period of January 1982 and October 2003: Meritorious Service Medal x 2 Army Commendation Medal x 8 Army Achievement Medal x 6 Meritorious Unit Award Army Good

Conduct Medal x 7 Army Occupation Medal (Berlin) Korea Defense Service Medal x 2 National Defense Service Medal (with Bronze Star) Iraqi Campaign Medal Global War On Terrorism Expeditionary Medal x 2 Global War On Terrorism Service Medal Non-Commissioned Officer Professional Development Ribbon x 3 Army Service Ribbon Overseas Service Ribbon x 4 Combat Action Ribbon Parachutist Badge Foreign Parachutist Badge (Canadian) Recruiter Badge Drivers Badge (Wheel) Marksmanship Qualification Badge Expert Rifle & Mortar

Name: Heather Evans

Email: wgarcia@example.com

Phone: 730.934.8604