Sr. Information Risk Manager- Information Security Sr. Information Risk Manager- Information Security Sr. Information Risk Manager- Information Security Fort Worth, TX Cleared Information Assurance Manager with experience in RMF, ATOs. Risk Analyst with an extreme work ethic. Currently working in the finance sector addressing Information Security and Risk. My cleared role outside of the Finance sector focuses on DOD Information Assurance with the U.S. Army National Guard. I focus on enterprise risk and cyber warfare within the DOD. RMF consulting, corporate strategy and business plan implementation are available via a consulting rate. Authorized to work in the US for any employer Work Experience Sr. Information Risk Manager- Information Security Depository Trust & Clearing Corporation-DTCC - Coppell, TX March 2019 to Present Reassess existing processes and create new ones that most effectively anticipate, manage and reduce risk to DTCC and its participants. Support the security strategy, program assessment and control life cycle processes. Support the attestation request, response, and sampling workflows. Support design of the solution with relevant management reporting metrics and risk thresholds. Align cybersecurity program assessment reporting with stakeholders in support of managing risk and identifying opportunities to enhance DTCC s security profile Coordinate key cyber security program initiatives and their alignment with NIST CSF, including rationale(s) for risk reduction or avoidance End to End Process Analysis and risk reduction initiatives Research best practices and industry trends for the information security program with external organization, 3rd parties industry specialists, symposiums, and industry organizations and assess suitability for DTCC implementation Aligns risk and control processes into day to day responsibilities to monitor and mitigate risk Participate in and influence information risk assessment process improvement Schedule and perform information risk assessments using DTCC methodology; identify, document and communicate control deficiencies in business processes and technology systems Partner with the business and technology to agree cybersecurity risk findings identified through the risk assessment (e.g., vendor, application, infrastructure), new initiatives, and ad hoc processes Provide risk remediation recommendations that the business and technology may implement to mitigate identified control gaps Partner with business and IT to ensure that risks are clearly articulated in a manner that is

understood by business and technology audiences Evaluate management responses to ensure that remediation plans and tasks adequately address identified control gaps Information System Security Engineer 5 L3 Technology - Greenville, TX January 2018 to March 2019 The Information System Security Engineer performs system architecture design, risk assessment, security control selection, implementation, and test planning with respect to information assurance. The ISSE supports the steps one through six of the Risk Management Framework (RMF) Security Life Cycle ensuring information assurance is included in the design architecture. The ISSE is responsible for documenting security controls/requirements for inclusion in the system requirements specifications. The ISSE drives and supports the ATO (A&A) process in support of gaining a full ATO. The ISSE is responsible for developing Risk Assessment Reports (RAR), Security Plans (SP), Security Control Traceability Matrix (SCTM), and other applicable documentation pertaining to documenting an accreditable information system design. ISSE supports software engineers in hardening various operating systems. Individual responsibility includes identifying the information protection needs for systems and networks. Design, develop, and implement system security measures that provide confidentiality, integrity, availability, authentication, and non-repudiation. Review and assist design engineers in overarching system design with a focus on Information Assurance. Interact with customers and accreditation officials to define and achieve required Information Assurance objectives. RMF Support though all six steps 1. Catagorize (FIPS-199) 2. Select Security Controls (NISTP SP 800-53) 3. Implement Security Controls (which could not be tailored out using overlays. 4. Access Security Controls (NISP SP 800-53) 5. Authorize and 6. Monitor (A.K.A. Continuous Monitoring). Project Position: Information System Security Manager (ISSM) meets DoD 8570.01-M, Information Assurance Workforce IAT III. Project Scope: Identify Security Controls Risk Management framework steps/ Selection of Security Controls NIST SP 800-53 r4 (RMF Rev4),FIPS 199/NIST 800-60 SYSTEM CATEGORIZATION. SYSTEM INFORMATION Cyber Threat Boundaries, recommend threat mitigation strategies with appreciate adjustments to project burn rate. Transport and WCF NOC Analyst ManTech International Corporation - Honolulu, HI November 2016 to January 2018 Transport and WCF NOC Analyst Monitored and adjusted IAP Status and

took action for any noticeable anomalies (noticeable change in the normal rise and fall of the IAP s, increased latency or packet loss). Experience with the following tools Splunk - used for trend analysis regarding deviation form network baseline. eHealth - looking at utilization, latency, errors on circuit level. IAP Status Page - Provides real time monitoring of the IAP s. FLMTR - Used for ACL whitelist verification Panorama - Managed firewall and used to look at the Global firewall rules. Pala Alto Firewalls - Used to look at allowed and blocked traffic. Arbor - Used to look at top talkers driving peak flows to try to identify the cause. Brightcloud - Used to lookup antivirus definitions F5 Load Balancer- Looked at stats, memory and dropped services. Preformed fault isolation and diagnostic/assessment functions to include: determination and execution of corrective action(s) on a real-time basis. Remedy, HP OpenView, Silvx, Cisco Prime Optical, Netcool, INMS . Experience with Promina / ATM, MSPP, ODXC networks. Cyber Security Analyst III Genesis Business Systems - Honolulu, HI August 2016 to January 2018 Cybersecurity research, analysis and reporting for all Cybersecurity compliance issues. Tracking, validating, and reporting all levels of Cyber systems from attachments to organic systems. IAVA compliance work, responsible for POAM creation and briefing ,hands on experience with ACAS and CMRS, Nessus and Scans eMASS usage on SIPR. Conducted technical and procedural audits of systems using evaluation tools and configuration standards searched Security Requirement Guides (SRG), Security Technical Implementation Guides (STIG). Security Content Automation Protocol (SCAP) automated tools, STIG Viewer, SCAP Compliance Checker (SCC), HBSS Policy Auditor, DISA STIG Viewer, Vulnerability Management System (VMS). Provided overall information systems compliancy status, vulnerability trends, and briefs to USPACOM leaders and ISSM. Key Accomplishments: Led preparation for Computer Network Defense Service Provider inspection (CNDSP). Resulting in a successful validation of a robust cybersecurity program . Led preparation for Command Cyber Readiness Inspection (CCRI) Cybersecurity Scorecard and Cyber Scope Analyst responsible for CIO monthly product for U.S. PACOM CIO and Secretary of Defense. Developed U.S. PACOM standard operating procedure (SOP) for secure hard drive disposal. IT System Manager U.S. Army National Guard - Kalaeloa January 2014 to December 2017 Set up CPN and STT communications

equipment during monthly drill. Trained soldiers on use of CPN and STT though the use of SOPs and hands on training. Provided IT Mentorship and Training to achieve 100% up time for all drills. Key Accomplishments: Awarded an Army Achievement Medal during Annual Training for developing Standard Operational Procedures for the deployment of a Command Post Network (CPN) and Satellite Transportable Trailer (STT). Top 7% take Security+ and pass after completion of two week training Developed a rigorous Company Physical Training schedule during Annual Training to instill esprit de corps. Maintained perfect Army Fitness Test score Transferred to higher echelon to act as Subject Matter Expert for CPOF, CPN and Field Network Communications Held position two ranks higher and acted as section NCOIC during Annual training. Acted as senior Communications consultant prior to company movement for Annual training 2016. Business Expansion Manager/ IT Director Kiku International Corp - Honolulu, HI February 2013 to May 2016 Managed and Directed IT operations for two restaurant locations. Developed and executed plan for new restaurant including staffing and movement of bakery and retail store to new location. Set up and maintain wired and wireless networks at multiple locations. Set up and onsite and offsite backup systems. Trained Staff in Cybersecurity best practices and proper Business plan execution Key Accomplishments: Launched new business location two weeks before the start of University MBA program. Assisted in choosing new general manager and approved team leads. Provided guidance during full phase program management from property selection and lease lock-in. Completed full scale SWOT and competitive analysis for Caf launch. Streamlined product launch life cycle though the use of analytics. I.T. System Leader, Specialist U.S. Army - Honolulu, HI 2011 to 2013 While forward deployed to Afghanistan led a team of IT technicians to maintain communications connectivity across three separate military installations. Created two classified communication networks and acted as Project Manager for the installation of a fiber optic network backbone. Upon return to Hawaii, facilitated a unit wide migration from Windows Vista to Windows 7. Key Accomplishments: Selected as lead remote IT professional in Southern Nangarhar and provided immediate communications support via Fast Action Support system, enabling critical communication uplinks across a battle space with over 3,000 soldiers. Responsible for Brigade

wide KG 175D taclane (encryption/decryption device) upgrade and only non-civilian subject matter expert for Satiate Communications Terminals (SATCOM). Enabled upper management access to key communication infrastructure points at over (3) forward operating bases, allowing commanders to have real-time communication during Deployment, resulting in the security of over 2% of Afghanistan. Identified key cryptology equipment nearing end of life cycle and secured funding for full replacement. Upon leaving active duty I was offered a Position with General Dynamics as Remote site Field Service Rep. Helpdesk Leader and Satellite Operator, Specialist U.S. Army - Honolulu, HI 2007 to 2013 IT and communications efforts successfully allowed for full command of Area of Responsibility (AOR). Drafted technical documentation for program reference and maintenance, Created unit level Standard Operating Procedures for Communications Section. Key accomplishments: Devised innovative IT infrastructure for stadium seating and real-time decision making in the Battalion Command & Control Center. Improved Command & Control reduced small unit response time to threats by an average of 20 minutes. Personally Responsible for communications' equipment valued in excess of $1,000,000 USD. IT Helpdesk Leader and Satellite Operator, Specialist U.S. Army - Honolulu, HI 2008 to 2011 Responsible for communications equipment valued in excess of $1 million. Drafted technical documentation for program reference and maintenance, and also created unit level Standard Operating Procedures for Communications. Brigade subject matter expert for satellite communication. Key accomplishments: Improved Command & Control unit response time to threats by an average of 20 minutes. Devised innovative IT infrastructure for stadium-style seating and real-time decision making in the Battalion Command & Control Center. Offered Position within Whitehouse communication agency. Information management Technician, Specialist U.S. Army - Honolulu, HI 2007 to 2008 Led IT security compliance day-to-day efforts for over 400 users. Facilitated a unit wide migration from Windows XP to Windows Vista. Led the management of all secret and encrypted IT communication infrastructures. Selected as Information Assurance Officer after only two months of employment. Managed Mobile end user device program -Blackberry. Selected as unit trainer for Information Assurance and Practical Cyber Security. Key accomplishments: Identified two cases

of infrastructure out of physical data security compliance and promptly created a plan for replacement and upgrade to meet compliance standards. Upgrades were made completed ahead of schedule furthering the unit's battle readiness and deployment capabilities. Offered Position within Whitehouse Communications Agency (WICA) Education Candidate: Master of Science - MS in Information Security Engineering SANS Institute October 2018 to January 2021 Master of Business Administration in International Business University of Hawaii, Shidler College of Business - Honolulu, HI 2014 to May 2016 Bachelor's in Management Information Systems Lamar University - Beaumont, TX 2003 to December 2007 Military Service Branch: U.S. Army Service Country: United States Rank: SGT January 2007 to Present Active Duty U.S. Army 2007-2013 National Guard 2014- Current Certifications/Licenses CompTIA Advanced Security Practitioner Certification (CASP) September 2016 to September 2022 ITIL v3 Foundation February 2016 to Present Certified Information System Security Professional (CISSP) December 2016 to December 2020 Certified Scrum Master (CSM) October 2016 to October 2020 Certified Ethical Hacker v9.0 (CEH) January 2016 to January 2020 Scrum Fundamentals October 2016 SCRUMstudy - Accreditation Body for Scrum and Agile Additional Information Active Secret Clearance with TS/SCI Processing

Name: Debbie Wilson

Email: annerussell@example.com

Phone: (865)618-8641x641