Lead IT Security Analyst / Validator Lead IT Security Analyst / Validator Lead IT Security Analyst / Validator - KBRwyle Jacksonville, FL * 11+ years of experience in IT management and supervisory positions achieving outstanding results in all assigned responsibilities. * Security Operations - Implementation of policy and maintenance including backup, recovery, monitoring, incident management, patch and vulnerability management, and physical security. * Incident Response - Strong understanding of incident response and resolution to include detection and analysis, containment, eradication, and recovery. * DOD IA A&A - Extensive experience building A&A packages and aligning Army, Navy, Marine Corps, Air Force, and DHA systems with A&A processes, requirements, and controls through the Risk Management Framework (RMF). Work Experience Lead IT Security Analyst / Validator KBRwyle - North Charleston, SC 2019 to Present Address: 5935 Rivers Ave # 100, North Charleston, SC 29406 Supervisor: Augustine Brown (843-300-4792) Lead IT Security Analyst / Validator Charleston, South Carolina (REMOTE) Responsibilities: Lead IT Security Analyst / Validator * Provide guidance as needed throughout the RMF ATO process. * Review the results of each step, confirm that the step is complete and on time, and report the status to DHA Leadership by conducting biweekly meetings with the PMOs and posting minutes in eMASS and making weekly entries in CSTAR. Responsible for the assessment of the 800-53 security controls, ensuring they are addressed as required in eMASS. * Provide technical support throughout the RMF process. * Host biweekly meetings and work with SCARS and Program Offices to answer technical questions and ensure the result of each step is technically complete and accurate. Cybersecurity Analyst - Consultant PART TIME - Georgia Technical Research Institute - Atlanta, GA 2016 to Present Address: Baker Bldg (Gtri), 925 Dalney St NW, Atlanta, GA 30318 Supervisor: Sheila Isbell(678-296-7951) Cybersecurity Analyst - Consultant Atlanta, Georgia Responsibilities: Security Analyst / Consultant * Assist and advise on the creation and transition of DIACAP Authority To Operate (ATO) packages to the Risk Management Framework (RMF) for the United States Army and United States Marine Corps. * Assist in the development and creation of management applications and the implementation of IA security controls to existing and pre-production systems. * Provide feedback and advice to system owners,

project managers, and IA teams for IA issues and RMF implementation. * Assist with needed RMF documentation for system ATO. Cybersecurity, Senior Information Assurance Specialist & Site Lead DirectViz Solutions LLC. and Enterprise Solutions & Management Inc. / USN - Springfield, VA 2016 to 2019 Address: 6987 Meadowforest Court, Springfield VA, 22151 Supervisor: Brett Sherard (703-597-1454) Cybersecurity, Senior Information Assurance Specialist & Site Lead Commander Navy Region Southeast (CNRSE) Jacksonville, Florida Responsibilities: Cybersecurity, Senior Risk Management Specialist & Site Lead * Implementation of DoD Risk Management Framework (RMF) formerly known as the Information Assurance Certification and Accreditation Process (DIACAP) in order to obtain ATO for 40 systems throughout the region IAW DODI 8500s, 8500.2s, and 8510s. * Categorize IS systems in accordance with NIST SP 800-60. * Develop System Level Continuous Monitoring (SLCM) Strategy previously Information Security Continuous Monitoring (ISCM) Strategy in accordance to NIST SP 800-137. * Tailor baseline security controls assigned during Step 2 Categorization to meet specific system needs determined by hardware and software specifications. * Identify common controls and control inheritance provided by DOD and apply to package via eMASS. * Select applicable security control overlays based on system categorization. * Conduct and submit Privacy Impact Assessment (PIA) to ensure proper identification and protection of PII/PHI. * Identify active ports, draft, and submit PPSM Registration for GIG connectivity. * Apply technical and administrative approved controls determined by Step 2 Checkpoint. * Develop RMF A&A documentation and artifacts, to include the System Level Continuous Monitoring (SLCM) Strategy, HW/SW/Information Flow Diagrams, System Categorization Forms, System Topologies, Configuration Management Plan, Configuration Control Board (CCB) Charter, System and Services Acquisition Plan, System and Information Integrity Plan, System and Communication Protection Plan, Security Assessment and Authorization Plan, Risk Assessment Plan, Program Management Plan, Security Planning, Physical and Environmental Protection Plan, Personnel Security Plan, Media Protection Plan, Identification and Authentication Plan, Contingency Plan, Audit and Accountability Plan, Security Awareness and Training Plan, Incident Response Plan, Access Control Plan, Risk Assessment Review (RAR) and Plan of Action

and Milestone (POA&M). * Link individual controls in eMASS to applicable artifacts for verification of test results. * Formal testing of assigned security controls and documentation of results in eMASS. * Interpreting, decomposing, and allocating IA/IS requirements as well as designing IA/IS system and subsystem solutions. * Assessing and mitigating security threats and risks and evaluating IA/IS operational concepts. * Ensure proper processes and procedures for the United States Department of Defense are followed and ensure risk management is applied on all information systems (IS). * Develop policies and procedures to ensure information system reliability and accessibility. * Prevent and defend against unauthorized access to systems, networks, and data. * Conducts risk and vulnerability assessments of planned and installed information systems in order to identify vulnerabilities, risks, and determine protection needed to secure system. * Develop and implement programs to ensure data users are aware of, understand, and adhere to systems security policies and procedures. * Assess security events to determine impact, and implement corrective actions. * Implement Information Security/Cyber Security policies, principles, and practices in the delivery of all IT services. * Ensure the structured process for the certification and accreditation (A&A) of a DoD Information System and ensure (IA) posture throughout the system life cycle is maintained. * Provide guidance to sites for ACAS SCAN results and implement mitigation process ensuring IAVA compliance for all systems. * Conduct systematic examination of IS to determine adequacy of security measures, identify security deficiencies, predict effectiveness of proposed security measures, and to confirm adequacy of such measures after implementation. * Provide baseline training awareness materials, content, and products pertaining to DOD IA policies, concepts, procedures, tools, techniques, and systems to DOD components to integrate into their IA training and awareness programs. * Conduct pre-validation reviews of A&A packages for compliance with DoN and DoD Information Assurance (IA) policies, coordinating with sites to obtain missing items or correct known discrepancies. * Assist customers with the DADMS registration forms for software applications, DIT-PR registration forms for IT systems and software licensing purchase through Softchoice. * Provide technical and project management support throughout CNRSE on Special Purpose Systems and Local Area Network environment to optimize network performance. *

Recommend corrective action on information technology networking issues. * Conduct risk assessments in the efforts of preventing problems that can be caused by the introduction of new or modified technology and IT applications. * Routinely work with contract representatives, vendors, customers, and end users to coordinate work, resolve problems, and or provide information on IT/IA related issues. * Provide solutions for problems that are elevated beyond the Help Desk or problems in which the end user is not completely satisfied. * Monitor budget and ensure annual spending requirements are met. * Mentor junior analyst and ensure performance and training requirements are met daily. * Draft and disseminate monthly status reports of contract requirements and progress of tasks outlined in contract. * Provide advice and updates pertaining to designated system requirements outlined in contract both written and verbally to COR and DVS/ESM management. * Coordinate quarterly travel needed for 13 sites to meet quarterly IA requirements of designated systems. Cybersecurity, Security Operations Center (SOC) Analyst Deutsche Bank - Jacksonville, FL 2016 to 2016 Address: 5022 Gate Pkwy N, Jacksonville, FL 32256 Supervisor: Mike Southerland (352-256-5957) Cybersecurity, Security Operations Center (SOC) Analyst Jacksonville, Florida Responsibilities: Cybersecurity, Security Operations Center (SOC) Analyst * Monitor, evaluate, respond to, mitigate, and escalate alerts triggered by NIDS, ArcSight, Symantec Endpoint Protection, and CISCO FireSIGHT systems. * Evaluate proxy logs through Splunk tool to detect patterns in traffic that result in vulnerabilities and threats within the Deutsche Bank network. * Utilize regular expression (REGEX) to examine malicious patterns in network traffic not detected by passive systems. * Analyze packets from NIDS alerts and compare to Splunk rules to determine false positive and true positive alerting. * Utilize McAfee Trusted Source to verify blocked traffic and submit found malicious URL's for future blocking. * Coordinate with CTI, CTA, Network Operations, SMTP, and Firewall teams to identify unknown and mitigate known malicious activity. * Analysis of ArcSight alerts to detect brute force attacks, malware infections, unauthorized system configuration, and all other malicious activities within the Deutsche Bank network. * Understand and research current cyber-attack methods used to exploit network vulnerabilities. * Document, contain, and mitigate known security incidents detected on the network. * Execute incident response process

when a security incident has been declared. * Document and present findings to management suitable for upper level evaluation. Information Assurance Technician IAT 2012 to 2015 * Manager of 10 personnel and allocated resources to accomplish assigned tasking. * Help Desk Manager - Responsible for the resolution of trouble calls for over 200 users. * US Navy Qualified System Administrator responsible for effective provisioning, installation/configuration, operation, security, and maintenance of systems hardware and software. * Ensure Information Awareness Workforce (IAWF) is compliant with DoD 8570.01-M Information Awareness Workforce Improvement Program. * Interpret, decompose, and allocate IA/IS requirements as well as designing IA/IS system and subsystem solutions. * Assessing and mitigating security threats and risks and evaluating IA/IS operational concepts. * Assisting in the creation packages for the DoD Information Assurance Certification and Accreditation Process (DIACAP) in order to obtain an ATO throughout the Fourth Fleet AOR IAW DODI 8500s, 8500.2 8510s. * Ensure processes for the United States Department of Defense are followed and ensure that risk management is applied on all information systems (IS). * Assist in developing policies and procedures to ensure information systems reliability and accessibility, and prevent and defend against unauthorized access to systems, networks, and data. * Conduct risk and vulnerability assessments of installed information systems in order to identify vulnerabilities, risks, and protection needed. * Assist in developing and implementing programs to ensure that systems, networks, and data users are aware of, understand, and adhere to systems security policies and procedures. * Assess security events to determine impact, and implement corrective actions through the application of information security/Cyber Security policies, principles, and practices. * Ensure structured process for the certification and accreditation (A&A) of a DoD Information Systems and establish (IA) posture throughout the system life cycle is maintained. * Provides guidance for RETINA, ACAS SCANS and mitigation process also ensuring all IAVA compliance are met for all systems. * Provide baseline training and awareness materials, content, and products pertaining to DOD IA policies, concepts, procedures, tools, techniques and systems for users. * Assist with DIACAP, A&A documentation and artifacts, to include the System Identification Profile (SIP), DIACAP Implementation Plan (DIP), Validation Plan, and Validation Reports, Plan of

Action and Milestone (POA&M) and Scorecard using eMASS. * Generate and provide Contingency Plan and assist in completing Configuration Management plans and Incident Response Plans and procedures. * Conduct risk assessments on systems being submitted for A&A by analyzing automated scans to include, Retina and other tools as deemed necessary, along with architectures, POA&M's. Commander, Navy Region Southeast United States Navy - Jacksonville, FL 2008 to 2015 32212-0102 Supervisor: Cornelius Mitchem (904-270-6740) Petty Officer First Class (E6) Commander U.S Naval Forces Southern Command Jacksonville, Florida Education Master's in Information Assurance Embry Riddle Aeronautical University-Worldwide - Daytona Beach, FL January 2019 to Present Master's in Management Information Systems Embry Riddle Aeronautical University 2018 System Administrator School Navy "C" School - San Diego, CA 2015 Communications Circuits IT "A" School - Pensacola, FL November 2008 BA in English Stetson University 2007 Skills Security, testing, training Military Service Branch: USN Service Country: United States Rank: E6 February 2008 to November 2015 Commendations: 2014 United States Southern Command Enlisted Person of the Year Ranked number 1 of all enlisted personnel in all 5 branches operating in the SOUTHCOM AOR - 2015 2014 Sailor of The Year Ranked 1 of 25 First Class Petty Officers in 2014. 2011 Sailor of The Year Ranked 1 of 32 Second Class Petty Officers in 2011. Joint Commendation Medal - 2015 Naval Commendation Medal x2 2014, 2015 Naval Achievement Medal Awarded May 15, 2014 for creating a detailed plan of action and milestones to ensure all requirements were accomplished prior to inspection while achieving zero degradation in communications support." 2014 CCRI Inspection Awarded April 20, 2012 for dedicated efforts and superior managerial skill which ensured outstanding results during all deployment certification events . Awarded December 16, 2011 for superior managerial skill and leadership ability which lead to an average divisional score of 98% for the Communications and LAN work centers. Awarded April 27, 2011 for consistent dedication and outstanding work ethic , which led to the only work center with zero discrepancies on March s Force Revision for the Communications and LAN work centers. Awarded June 10, 2010 for superior performance resulting in USS Taylor s 2010 final certification which directly enabled USS Taylor to deploy for the

2010 Mediterranean Theater Security Cooperation Deployment. Certifications/Licenses Certified Information Systems Security Professional (CISSP) Certified Ethical Hacker (CEH) Certified Authorization Professional (CAP) CompTIA Security+ CompTIA Network+ CompTIA A+

Name: Lisa Potts

Email: slewis@example.net

Phone: 808-932-4307x295