

Transportation Security Officer Transportation Security Officer Transportation Security Officer - Fort Lauderdale International Airport Weston, FL Over 5 years of experience in Information Technology services supporting security initiatives for government and commercial customers. Work experience encompasses threat analysis, incident response, network surveillance, Data mining, Risk Management Framework (RMF), National Institute of Technology (NIST), System Development Life Cycle (SDLC), Information security documents, developing and promulgating Security Assessment Plans (SAP) and Security Assessment Reports (SARs). Authorized to work in the US for any employer Work Experience Transportation Security Officer Fort Lauderdale International Airport - Fort Lauderdale, FL November 2015 to Present Fort Lauderdale, FL Tampa International Airport, Tampa, FL Palm Beach International Airport, Palm Beach, FL Transportation Security Administration (TSA) Transportation Security Officer Administrative Assistant-Inspections/Compliance. November 2015- Present

- * Performed regulatory inspections/investigations related to suspected security violations which include hand-wand and pat-down searches
- * Participated in activities designed to identify security threats through techniques as directed by Headquarters. Communicated appropriately and effectively in difficult situations, such as those involving higher than normal pressure, adversarial circumstances.
- * Acquired advanced skills in security equipment: Explosive Trace Detection, Computed Tomography X-ray, Heimenn X-ray, and Advanced Imaging Technology
- * Responsible for simultaneously operating computer-aided dispatch systems, a multi-channel radio console and a multi-line telephone. Work requires the ability to complete assignments quickly and accurately and to handle several requests simultaneously
- * Responsible for daily maintenance and troubleshooting, of SharePoint and Airport Information Management system (AIM) and integrating both into daily airport operations, regularly collaborating with content managers and other site owners in the continual development of TPA Web Site Collection to include new site creation
- * Maintained and developed multi-user database on MS Access
- * Trained and supervised new employees as required
- * Assist AFSD-Inspections with managing and filing civil enforcement investigative reports.
- * Performed audits of SIDA badges, credentials and PIV cards in support of the Compliance office.
- * Provided

advanced computer assistance to include proficiency in MS Access, MS Excel and MS Word. *

Created and maintained MS Access and Database used to track regulatory violations to include the design and construct of flexible ad hoc queries to report and quantify civil penalties. * Maintained records in accordance with TSA Records Management Plan to include Disposition of Records. *

Reviewed and analyzed information to ensure compliance with established regulations, policies, and procedures, including those governing the preparation and submission of cases. Refers non-compliant cases back to initiating staff for resolution. * Provided written and oral explanations of administrative policies. * Prepared incident reports in TSA's Performance and Results Information System (PARIS).

IT Security Analyst Global Solution Network - Rockville, MD May 2012 to October 2015

Conduct IT risk assessment to identify system threats, vulnerabilities and risk, and generate reports. Maintain, review and update information security system documentations, including System Security Plan (SSP), Plan of Action & Milestone (POA&M), Risk Assessment (RA), policies and procedures, security control baselines in accordance with NIST guideline and security practices. ?

Apply appropriate information security control for Federal Information System based on NIST 800-37 rev1, SP 800-53, FIPS 199, FIPS 200, and NIST SP 800-53A R4

Assess security controls and develop security assessment report (SAR)

Support A&A activities (Categorize, Selection, Implement, Assessment, Authorize, Monitor) according to the A&A project plan. ?

Review authorization documentation for completeness and accuracy for compliance. ?

Facilitate Security Control Assessment (SCA) and monitor activities. ?

Executed examine, interview, and test procedures in accordance with NIST SP 800-53A Revision 4. ?

Ensure cyber security policies are adhered to and that required controls are implemented. ?

Validated information system security plans to ensure NIST control requirements are met. ?

Assist team members with proper artifact collection and detail to client's examples of artifacts that will satisfy assessment requirements. ?

Review security logs to ensure compliance with policies and procedures and identifies potential anomalies. ?

Update and review A&A Packages to include Core Docs, Policy & Procedures, Operations and .Maintenance Artifacts, SSP, SAR, FIPS 200, FIPS 199, and POA&M. ?

Collect Operation and Maintenance artifacts on an ongoing basis so that Security Control Assessment

(SCA) is seamless. ? Upload supporting documentations into the System's Artifact Libraries, Google Docs, and CSAM. ? Manage vulnerabilities with the aid of Nessus vulnerability Scanners to detect potential risks on a single or multiple assets across the enterprise network. Information Security Analyst Global Solutions Network - Rockville, MD February 2010 to May 2012 Ensure proper system categorization using NIST 800-60 and FIPS 199; implement appropriate security controls for information system based on NIST 800-53 rev 4 and FIPS 200. Conduct security assessment interviews to determine the Security posture of the System and to Develop a Security Assessment Report (SAR) in the completion of the Security Test and Evaluation (ST&E) questionnaire using NIST SP 800-53A required to maintain Company Authorization To Operate (ATO), the Risk Assessment, System Security Plans, and System Categorization. Reviewing, maintaining, and ensuring all assessment and authorization (A&A) documentation is included in the system security package. Perform information security risk assessments and assist with the internal auditing of information security processes. Assessed threats, risks, and vulnerabilities from emerging security issues and also identified mitigation requirements. Work with system owners to develop, test, and train on contingency plans and incident response plans. Tests, assess, and document security control effectiveness. Collect evidence, interview personnel, and examine records to evaluate effectiveness of controls. Review and update remediation on plan of action and milestones (POA&Ms), in organization's cyber security assessment and management (CSAM) system. Work with system administrators to resolve POA&Ms, gathering artifacts and creating mitigation memos, residual risk memos and corrective action plans to assist in the closure of the POA&M.

Computer & Software Proficiencies ? Microsoft Office Suite ? Adobe ? Qualified Typist (70wpm) ? Nessus Vulnerability Scanner ? MS Project ? Accellion/WatchDox secure file solution ? Caliber Requirements Tool ? Doors Requirement Management Tool ? HP Quality Center ? CSAM Education Bachelor in Computer Information Systems Saint Leo University - Saint Leo, FL 2015 to 2016 Skills Cash Handling, Customer Service, Excel, Management, Organizational Skills, Security, Stocking, Word Certifications/Licenses Security Guard Additional Information COMPUTER: Proficient in Microsoft Word, Microsoft Excel, Microsoft Outlook, and Microsoft Power

Point. LANGUAGE SKILLS: Knowledge of Tigrina and Amharic (oral).

Name: Kelly Huang

Email: stanley87@example.org

Phone: +1-595-622-8100x42629