Technical Lead (ISSO) Technical Lead (ISSO) Technical Lead (ISSO) Fredericksburg, VA Work Experience Technical Lead (ISSO) eGlobal Tech 2017 to December 2017 End Present As an ISSO, I support the FISMA compliance Security Authorization services in support of the USCIS Office of Information Technology (OIT) mission of providing independent Security Authorization (formerly Certification and Accreditation (C&A)) and FISMA compliance services to USCIS. Ensure all Security Authorization documentation for assigned systems remain accurate and up to date on a continuous basis, including but not limited to accurate and valid lists of assets (hardware/software), accurate boundary diagrams, accurate ports and protocols, etc. Coordinate and facilitate Security Control Assessor (SCA) activities as required and directed by the Federal Government. For example: ? Coordinate and support all Security Assessment interviews as required. ? Ensure appropriate accounts and access is provided to the SCA team within a timely manner. Load and maintain all supporting artifacts and information from these documents such as appropriate for assigned systems into the DHS and USCIS repositories as designed by ISD (for example, Information Assuarnce Compliance Systems (IACS) and ECN. Compile, write, update, finalize, produce and support activities for IT Security Common Control Catalogs and related documentation including, but not limited to, Security Plans or other documents required. Complete and maintain an up to date inverntory of all system components to assigned systems. Conduct Annual Assessment and Contingency Plan testing as required by DHS, USCIS and ISD. Provide additional FISMA support for Chief Financial Officer (CFO) designated systems as required. Ensure system is properly patched and hardened according to DHS requirement. Facilitate and assist with reviews and updates to POA&M content such as breakdown of milestones as required. Manage, maintain and track all assigned tasks and duties related to POA&Ms. Complete WEAR documentation as required and to meet USCIS, ISD and DHS standards and requirements and ensure they are approved at least 60 days prior to POA&M expiration. Facilitate and provide continuous support for the USCIS WEAR program to include but not limited to analysis, creation, approval, status tracking, and overall management of WEARs in relation to System-Level and Program-Level POA&Ms in a format provided by the Government on a daily, weekly, monthly basis

or as defined and directed by the Government. Review Audit logs and alerts from SPLUNK on a daily/ weekly and monthly basis as required by DHS, USCIS and ISD. Review ISVM compliance in SPLUNK using the ISVM Vulnerability Report Dashboard. Review Security Center (SC5) or Nessus and send critical, high, medium and low vulnerabilies to support team for remediation plan. Perform thorough review of SC5 and SPLUNK to determine authentication failures and review informational vulnerabilities that provide system information such as enabled ports etc. Request renewal, creation, or revocation of SSL Certificates by working with system administrators or application teams to complete a DHS Form 142-42. Review and approve Change Requests (CR) via the ServiceNow (SNOW) tool. Review and approve myAccess Requests by ensuring a detailed business justification has been provided to incluse the users role and purpose of the account request. Review ports and protocols to ensure that unnecessary ports are disabled. IT Security Engineer Soliel LLC December 2016 to December 2017 As an IT Security Engineer, I supported the FISMA compliance Security Assessment & Authorization services in support of the Department of Labor (DOL) Office of the Chief Information Officer (OCIO) Enterprise Security and Authorization Management (ESAM) mission of providing independent Security assessment &Authorization and FISMA compliance services to DOL. Analyze and update System Security Plan (SSP), Risk Assessment (RA), Privacy Impact Assessment (PIA), System Security test and Evaluation (ST&E) and the Plan Of Actions and Milestones (POA&M) Assist System Owners and ISSO in preparing Security Assessment and Authorization package for companies IT systems, making sure that management, operational and technical security controls adhere to a formal and well-established security requirement authorized by NIST SP 800-53 R4 Designate systems and categorize its C.I.A using FIPS 199 and NIST SP 800-60 Conduct Annual Self- Assessment (ASA) (NIST SP 800-53A) Perform Vulnerability Assessment. Make sure that risks are assessed, evaluated and a proper actions have been taken to limit their impact on the Information and Information Systems Created standard templates for required security assessment and authorization documents, including risk assessments, security plans, security assessment plans and reports, contingency plans, and security authorization packages Ensured Systems' Plan of Action & Milestone

(POA&Ms) are closed or update in a timely manner using a tracking tool CSAM Manages Systems' Accounts to ensure Privilege Users Accounts are Re-certified twice a year. Ensured Separation of Duties is enforced by reviewing all Accounts in the Windows Server Admins and Domain Admins. IT Compliance Analyst Smarththink LLC June 2013 to December 2016 Conducted kick off meetings to collect systems information (information type, boundary, inventory, etc.) and categorize systems based on NIST SP 800-60. Conducted security control assessments to assess the adequacy of management, operational privacy, and technical security controls implemented. Security Assessment Reports (SAR) were developed detailing the results of the assessment along with Plan of Action and Milestones (POA&M). Developed system security plans to provide an overview of federal information system security requirements and described the controls in place or to meet those requirements. Created and updated the following Security Assessment and Authorization (SA&A) artifacts; FIPS 199, Security Test and Evaluations (ST&Es), Risk Assessments (RAs), Privacy Threshold Analysis (PTA), Privacy Impact Analysis (PIA), E-Authentication, Contingency Plan, Plan of Action and Milestones (POAMs). Prepared Security Assessment and Authorization (SA&A) packages to ascertain that management, operational and technical security controls adhere to NIST SP 800-53 standards. Performed vulnerability assessment, making sure risks are assessed and proper, actions taken to mitigate them. Conduct IT controls risk assessments including reviewing organizational policies, standards and procedures and providing advice on their adequacy, accuracy and compliance with industry standards. Developed risk assessment reports. These reports identified threats and vulnerabilities. In addition, it also evaluates the likelihood that vulnerabilities can be exploited, assess the impact associated with these threats and vulnerabilities, and identified the overall risk level. IT Security Analyst Federal Integrated Systems Corporation June 2012 to June 2013 Held kick-off and weekly meetings with system owners prior to assessment engagements and weekly activities relating to CSAM Collected, reviewed and analyzed audit logs for anomalies Managed vulnerabilities using Nessus vulnerability scanners to detect potential risks on a single and multiple assets across the Enterprise Network. Created reports detailing identified vulnerabilities and the steps to remediate them.

Tested and document comprehensive security assessment results that include a full description of the weakness and deficiencies discovered during assessment information System Security controls per the NIST 800-53A Revision 4 guidelines. Assisted in identifying and communicating application control deficiencies and the associated risks. Assisted with the development and maintenance of plan of action and milestones (POA&Ms) to document security vulnerabilities and mitigation strategies. Monitored controls post-authorization to ensure continuous compliance with security requirements. IT Helpdesk Support Analyst US Security Associates February 2010 to June 2012 Configured and installed new devices and software; maintained the computer system Installed OS and common applications, diagnosed and repaired Laptop and PC Desktop, Built and installed new devices Detected and resolved users issues on Laptop and PC desktop Assigned users and computers to proper groups in Active Directory. Modified configurations, utilities, software default settings Installation of telephone and networking equipment Worked directly with contracted customers to assure their satisfaction with equipment Provide support for software, hardware and networking related issues. Setup and support a network consisting of wireless computers, network printers, routers and access points Education BA in Marketing University of Ghana August 2008 Certifications/Licenses Certified Information Security Manager (CISM) Certified Information Systems Auditor (CISA) Certified in Risk and Information Systems Control (CRISC) Certificate of Cloud Security Knowledge (CCSK) CompTIA Security+ Certification Certified Scrum Master (CSM)

Name: Robin Foley

Email: qmartinez@example.com

Phone: +1-356-672-8742x91088