Information System Security Officer (ISSO) Contract Information System Security Officer (ISSO) Contract Information System Security Officer (ISSO) Contract - Diversified Technical Services, Inc San Antonio, TX Over four years of experience as an Information Technology professional. Insightful, results driven security professional with demonstrated knowledge in Cyber-Defense/Cyber- Security methodologies, principles and best practices. Possesses comprehensive knowledge of information security policies and procedures, assessment and authorization procedures, administrative, technical and operational measures, vulnerability of computer and data communication systems, and basic tools and practices for protecting information systems to ensure the confidentiality, integrity and availability of resources and data. Background includes policy development, vulnerability assessment, physical and operational security practices, problem solving, risk management and helpdesk management. Superior capacity to solve complex problems involving a wide variety of information systems, and thrive under pressure in fast-pace environments in order to achieve and exceed company organizational goals. Security Clearance: Secret Authorized to work in the US for any employer Work Experience Information System Security Officer (ISSO) Contract Diversified Technical Services, Inc May 2018 to Present for Air Force Recruiting Information Support System - Total Force (AFRISS-TF) May 2018 - Present Information System Security Officer (ISSO) Contract Serves as the organization's Information Assurance Officer & Cyber Security subject matter expert providing technical and managerial expertise to internal company and external contract delivery initiatives. Responsible for executing Risk Management Framework (RMF)'s Assessment and Authorization (A&A) Process to support the following systems; DISA Milcloud's Air Force Recruiting Information Support System - Total Force -Test and Development (AFRISS-TF-TD) and DISA DECC's Air Force Recruiting Information Support System - Total Force (AFRISS-TF) to maintain authorization of the systems throughout their lifecycle. Managed detail oriented activities for Assessment and Authorization (A&A) to Achieve Authorization to Operate (ATO) for two mission critical Air Force Recruiting IT systems. Perform a vast array of substantive and comprehensive technical and administrative cyber security management tasks to deliver an outstanding array of IA services to include; RMF Program

Management, Security Policy/SOP Development, Security Assessment and Compliance, Computer Network Vulnerability Remediation, Plan of Actions and Milestone (POA&M) Management, and Risk Management to name a few. Trained System Administrators on how to create and complete DISA STIG Checklists specific to AETC's Guidance and created Presentation PowerPoint Slides for each individual System Admin to brief in weekly A&A Meetings to PMO. Created STIG & ACAS Tracker Documents for IT Systems to track vulnerabilities and remediations. Analyze existing and future systems, reviewing security architectures against existing and future architectures, and developing engineering solutions that integrate information security requirements to proactively manage information protection throughout the system's lifecycle. Senior Information Assurance Engineer Business Technology and Solutions June 2017 to May 2018 Contract) Assisted in the transition from the current DoD Information Assurance Certification and Accreditation Program (DIACAP) to the Risk Management Framework (RMF) Assessment & Authorization process based on National Institute of Standards and Technology (NIST) to support the Air Force Personnel Operations Agency (AFPOA). Managed detail oriented activities for DoD Assessment and Authorization to Achieve Authorization to Operate (ATO) for two highly specialized Army Materiel Command IM/ IT systems. Documented and report the security posture of systems through the Enterprise Mission Assurance Support Service (eMASS); successfully obtained and retained Authority to Operate (ATO) for multiple test environments, platforms, systems, networks, and enclaves under the purview of AFPOA. Established and annually test policies and procedures for configuration management, information system security, incident response, disaster recovery and contingency planning. Received the "Thumbs Up" Award for creating instructional "How To" guides for task procedures. Conducted security analysis of applications, appliances, and information systems (e.g. Windows 7, Windows Server 2008/2012, Solaris, Linux, and Unix) to ensure compliance with DoD requirements, NIST, RMF and Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs). Updated the System Security Plan (SSP) and Plan of Actions and Milestones (POAM) and other cybersecurity-related documentation to address vulnerabilities in the information system discovered during the security impact analysis or security control monitoring. Provided a project plan template for conducting information system security Certification & Assessment / Assessment & Authorization tasks (to include annual security assessment/reviews) and software certification to accurately track progress, including specific tasks, milestones, and delivery schedule utilizing Microsoft Project with applicable Gantt Chart view. Attended enterprise Information Assurance (IA) related working groups, conferences, and meetings to identify and execute emerging Information Assurance (IA) policies and/or creation and staffing of new IA policies. Provided a monthly status report to address major issues affecting system accreditation and/or authorization, any changes to requirements, any conflict of interests and mitigation efforts or plans that impact ability to perform responsibilities as outlined. Developed and deliver relevant Information Support Plan (ISP) and/or Tailored ISP Support (TISP) pertaining to cybersecurity as directed by the AFPOA System/Application Project Manager. Provided training to employees on cybersecurity/ IT in the event new technology in hardware or software is implemented. Cyber Security Engineer 22nd Century Technologies Inc December 2016 to June 2017 Contract) Supported the mission of the United States Air Force 24th Air Force Cyber Wing 33rd Network Warfare Squadron to conduct network security monitoring and intrusion detection analysis for NIPRNet (Unclassified) and SIPRNet (Classified) and JRSS (Joint Regional Security Stacks) Network using the AF's selected IDS/IPS tools: ArcSight 6.5, Wireshark, Fidelis XPS, Solera BlueCoat, Splunk, and Tipping Point in addition to open source research, forensic analysis and log reviews. Appointed by Crew Commander to perform Lead Operator duties such as monitoring Connectors, Sensors, Email Gateway, Firewalls and reporting observations of suspicious activity at end of shift De-brief. Researched NIPR and SIPR defensive cyber operations events to determine the necessity for deeper analysis and conduct an initial assessment of type and extent of intruder activities. Entered event data into mission support systems according to operational procedures and reports through the 33rd operational chain. Recorded suspicious events, meeting established thresholds, into the operational database for suspicious traffic ensuring records contain sufficient information to stimulate future research of suspicious traffic. Compiled suspicious events records and other artifacts as part of its Monthly Operational Report. Provided pass-on information to bring incoming crews up to speed on latest suspicious traffic seen from a given port, IP, etc. Developed comprehensive security write-ups which describes security issues, analysis, and remediation techniques to client leadership. Managed incident life cycle ensuring that all investigations kept current and are completed. Received "Outstanding Performer" recognition from 33NWS Flight Chief for offering solutions to accomplish new priorities assigned to misson. Information Assurance Security Operations Analyst Accenture Federal Services January 2016 to November 2016 Assured Compliance Assessment Solution (ACAS) system administrator. Conducted vulnerability assessments and reported Information Assurance Vulnerability Management (IAVM) findings to the client. Lead weekly meetings directly with client on IAVM vulnerability findings. Generated a Plan of Actions & Milestones (POA&M) for client to meet DoD and client Information Assurance requirements. Conduct bi-weekly meetings with client to report findings for Command Cyber Readiness Inspection (CCRI) and overall awareness of security posture. Managed Security Technical Implementation Guide (STIG) compliance by conducting checks/reporting, audits, track and monitor vulnerability progress. Updated daily security monitoring log with ArcSight, and followed up with application and system owners for resolution. Interpret, validate and apply Army, DoD, and NIST security regulations; DoD 8510.01, Risk Management Framework (RMF), DoD 8570.01, Information Assurance (IA) Training, Certification, and Workforce Management and methodologies to ensure supported agencies are in compliance with the latest DIACAP/RMF requirements, IA processes and security requirements. Assisted in developing Security Monitoring Rule Baseline document for SAP Hana Technology. Performed monthly validation for 10% of rules and reports generated through ArcSight, in addition to reporting results to client in Bi-Weekly Cyber Security Meetings. Participated in risk analysis to test audit and syslog rules to ensure rules are properly configured and reporting was adequate and timely. Received recognition from client for resolving multiple alerts that deemed suspicious but were essentially false-positive. IT Consultant/ Analyst HCL America for - San Antonio, TX June 2014 to December 2015 Contract) Awarded HCL's STAR Certificate of excellence for exemplary contribution to the USAA IT mission. Provided 1st and 2nd line support troubleshooting of IT related problems from in-house software to hardware, such as IOS applications, Thin clients, Virtual Machines, VPN, Active Directory, Microsoft Exchange Server, Laptops, PCs and Printers. Logged all calls in VM Service Manager Incident Logging system. Took ownership of user problems and followed up on the status of problems on behalf of the user and communicated progress in a timely manner. Utilized Virtualization Software (VMware, Citrix, Vsphere) in a professional workplace environment. Maintained a high degree of customer service for all support queries and adhered to all service management principles. Routinely exceeded call-handling goals, closing an average of 60 calls daily (25% above quota) with a 75% first-call resolution ratio. Excelled in asking probing questions and researching, analyzing and rectifying problems. Tracked prolonged outages in Remedy database and activated escalation process involving tiered maintenance teams as appropriate. Education Information Security Continuous Monitoring NIST September 2017 St. Phillips College January 2014 to May 2014 Bachelor of Business Administration in Business Administration Wayland Baptist University - San Antonio, TX June 2009 Skills SECURITY (2 years), INFORMATION ASSURANCE (2 years), BUSINESS CONTINUITY, RISK MANAGEMENT (2 years), TRAINING (1 year) Certifications/Licenses (CompTIA) CompTIA Advanced Security Practitioner Certification March 2018 to March 2021 (E-Council) Certified Ethical Hacker (C|EH v9) November 2016 to November 2019 (CompTIA) Security+ certified July 2018 to July 2021 Additional Information CORE COMPETENCIES Project Management Vulnerability Assessments Security Controls Information Assurance Risk Management User Training Business Continuity Vendor Collaboration

Name: Fred Bailey

Email: joshua81@example.org

Phone: (678)661-8112x30059