A&A Engineer A&A Engineer A&A Engineer - Obsidian LLC Reston, VA Authorized to work in the US for any employer Work Experience A&A Engineer Obsidian LLC August 2016 to Present Working knowledge of ACAS and HBSS and EMASS (Intermediate) Work the all 6 steps of the Risk Management Framework which consists of Categorization (Fips 199), Select - choosing Security Controls based on level of Risk determined by Step 1 and Implementation - composing the SSP- but familiar and possess working knowledge of all six. Assist System Owners in compiling implementation plans for the SSP to facilitate subsequent compliance audit. Assist system owners in formulating COOP and disaster recovery plans Provide A&A support to achieve ATO for the GSS at the State Department. Familiar with GOTS application to perform A&A duties - Security Categorization, E-Authentication Risk Assessment Write/Edit/enhance: Privacy Impact Statement, Risk assessment Review, SSP, Contingency Plan Security Engineer MacCauly Brown LLC December 2014 to August 2016 Provide technical support to tier 2 SOC analysts Responsible for administration of Symantec Endpoint Protection Responsible for administration of McAfee Network Systems Manager (IDS application) ? Rebuilt the NSM and five (5) Sensors Provide Arcsight support when necessary. Spearheading newly introduced C&A activities: ? Authoring SSP ? Assembling appropriate 800-53 securiity controls to be introduced to the US Senate ? Creating plans on how to check compliance to newly prescribed security controls. ? Discovering all Security related systems (Arcsight Bit9, Tenable, Carbon Black,, SEP to name a few Perform compliance testing and planning Performed GAP analysis Responsible for exclusion list for vulnerable scanning. Learning how to use Tenable (vulnerability scanning) ArcSight and C&A Engineer TSA December 2013 to December 2014 Provide ArcSight senior level support for the EMOC team at TSA. Audit security compliance to specific portions of the SSP Gather artifacts to prove security compliance Participate in application security and risk assessments Generate monthly reports for senior management as required per contract. Daily hands on support, maintenance as well as Installation of ArcSight infrastructure, to include but not limited to, SmartConnectors, and ESM. Maintained and supported Loggers and Connector Appliance Responsible for level 2 ArcSight support Authored SOPs for ArcSight infrastructure Attend CCB (configuration change board) for

any configuration changes for ArcSight. Investigate security breaches and collecting logs for forensic purposes Provide artifacts to prove security compliance as per FIPS 199, NIST 800-53 and existing SSP Provide solutions for ArcSight technical issues. Train newly hired personnel on navigating the DHS/TSA secured environment. Track, maintain and close POAMs Performed Continuous Monitoring duties, including but not limited to: coordinating scans, generating schedules, generating post-scan reports, posting such reports on SharePoint, act as liaison between Engineers and C&A personnel. Reviewed and maintained System Security Plan (SSP). Used Foundstone and Nessus and TripWire for vulnerability scanning and penetration testing. Worked closely with Incident Response team, to provide proper guidance as to remediation or escalation of current security issues/breaches. Working knowledge of Symantec Endpoint Protection (SEP 12), as well as McAfee Web Gateway, Familiar Microsoft ISA (Internet and Security Acceleration) servers. Working knowledge of Continuous Monitoring Familiar with Risk Management Framework (RMF) Performed C&A duties to include but not limit: ? Gap analysis ? SSP maintenance ? Compliance testing ? Obtain ATO IT Auditor/C&A Datum Software LLC January 2012 to November 2013 Part of a 16 man team designing a cloud solution for the Joint Chiefs of Staff at the Pentagon. Perform security assessments, determine mitigating controls, and identify/track its mitigation Responsible (authored and managed -risk assessment) Performed Evaluation, selection, implementation, integration of COTS products for security purposes. Authored Risk Acceptance letters in preparation for the Designated Approving Authority's (DAA) authorization/approval (e.g. ATO). Working knowledge of NIST 800-53, Fedramp, RMF, and FIPS guidelines. Authored and maintained the Security Engineering Plan (SSP) Performed Security Audits to prove compliance to SSP Working knowledge of Traceability MAtrix Responsible for gathering artifacts for proving compliance to DIACAP as well as NIST security controls. Familiar with VMware, SEP (Symantec Endpoint protection, ESXI and how they are fortified for C&A purposes. Possess working knowledge of SEP (Symantec Endpoint Protection), Tripwire, Nessus scanning tools. Provide planning and consulting services for ArcSight ESM. Worked closely with the Instant response Team. Used TripWire for vulnerability scanning and penetration testing. Responsible for alerting

appropriate personnel, for remediation Responsible for upkeep of ArcSight dashboards, so that analysts and Incident Response personnel are monitoring efficiently. Ensure compliance to TSA best practices on Single Sign On Administer user accounts on ArcSight, as well as Tivoli Access Management Familiar with RBAC polices and its adherence to TSA best practices Installed and troubleshoot ArcSight SmartConnectors and Flex Connectors. Administered User and user privileges (add, delete, unlock). Authored quarterly Risk Assessment reports, disclosing overall Risk stature of the Joint Staff Niprnet and Siprnet networks. Working knowledge of IAVMs and POAMs, and their management as well mitigation. Familiar with accreditation boundaries for auditing purposes. Authored, maintained and reviewed SSPs, as well as prove compliance. Sr. C&A Engineer Terremark Worldwide Inc September 2010 to December 2011 Responsible for authoring the company SSP. Responsible for proving compliance to NIST 800-53, FIPS-100 and other governing guidelines, including DIACAP, and FIPS as well as FedRamp security controls. Responsible for having POAMS mitigated by appropriate network/ security personnel. Worked directly with Government agency's Information Security Departments. Familiar with low, moderate and high levels of security controls. Assist independent auditors for risk assessments and security compliance. Familiar with SAS 70 reports and audits. Generated, coordinate, and manage POAMs (Plan of Actions & Milestones) and ensure its remediation and closure. Working knowledge of Tivoli Identity Manager - provision accounts over various directories Establish Roles Based Access Controls and configurations. Working (administrative) knowledge of Single sign on capabilities for cloud and non-cloud applications. Familiar with IAAS and SAAS (Infrastructure and Software as a Service) Familiar with accreditation boundaries for auditing purposes. Provide Risk assessment evaluations on systems that are to be installed on the production network (Unclassified and Classified). Performed due diligence on any proposed installations of hardware and software application on the network. Authored standard operating procedures for the creation of Risk Assessments. Worked with engineers and project managers to gather ample security information on system(s) to be accredited. Proficient in all aspects of performing certification and accreditation processes, including performing audits on information system's security control

Coordinate penetration testing, negotiate mitigation, create POAMS, and provide continuous monitoring and re-certification. Familiar with full life cycle of C&A process - to include SSP (Security System Plan), SRTM (Security Requirements Traceability Matrix), ATO (Authorization to Operate), POAM (Plan of Action and Milestones) EC's (Electronic Communication). Assisted and coordinate third party organizations in ST&E functions, providing evidence of security control compliance. Working knowledge of VMware, ESXi and Hypervisor (Cloud computing components. ArcSight SME / C&A Engineer Lockheed Martin September 2008 to September 2010 Part of the COTS product development team specializing in Security measures. Responsible for the product development of ArcSight Manager - a security tool for collecting, analyzing and managing enterprise event information. Possess working knowledge of developing and implementing agent/connector for various software solutions, including but not limited to Datapower, Websphere, Tivoli Identity Manager, Tivoli Access Manager, Tivoli Directory Integrator. Developed both SmartConnectors as well as Flex Connectors for ArcSight Manager. Knowledgeable in the analysis of security events being gathered from servers that are in the various FBI network environments, from development to production. Responsible for troubleshooting ArcSight Manager's functionality. Responsible for installation, development, and migration of the ArcSight Manager solution throughout the FBI network. Direct liaison between the FBI environment and the ArcSight support personnel. Responsible for any upgrade/patches to the ArcSight solution, including any recommendations for any enhancements. Part of a two-man team that is considered the subject matter expert on ArcSight. Responsible in assisting testers in performing and passing of the ArcSight solution functionality. Working knowledge of Rational Suite - including ClearQuest, ClearCase, and Requisite pro as well as Software Development Lifecycle. Implemented PKI certificate(s) for secured data transmission between, agents, the manager as well as an Oracle database. Working knowledge of Tivoli Identity Management and Tivoli Access Management Provided due diligence research on Oracle Identity Management (vs. Tivoli Identity Manager) Ensured adherence to FBI best practices on RBAC (Roles Based Access Controls) Familiar with forensic investigation and log retrieval. As a C&A engineer, responsible for researching and documenting known

vulnerabilities for application applying for an ATO. Established test parameters for test engineers, using a Security Requirement Traceability Matrix tool. Established and mitigated any vulnerability. Any unmitigated vulnerability was placed in a POAM list. Provide Risk assessment evaluations on any proposed systems that are to be installed on the production network (Unclassified and Classified). Responsible for managing and mitigating POAMs. Acted as a liaison between ISSO and System owners for compliance of NIST 800-53, Developed and authored SSP, Information Security Manuals. Worked with S T& E testers and in organizing POAM;s for presentation to System Owners. Familiar with Nessus, Nmap and Foundstone for vulnerability scanning. Developed and documented testing procedures (SOP).Implemented and managed STIG and Gold Disk activities. Experienced in setting test parameters to verify validity of test results. Performed audits on IT security controls. Security Analyst Unisys June 2006 to September 2008 Subject-Matter-Expert for the NETIQ products - Security manager and Vulnerability Manager. Planned, implemented, and support the SM and VM application. Provide technical support for enterprise/internet security for the TSA Security Operations Center. Provide reports using NetIQ - Vulnerability Manager by scanning servers in the TSA environment. Monitor and analyze security and application logs from servers in the TSA network - using NetIq's Security Manager as well as Vulnerability Manager. Analyze security events triggered by Security Manager and or ArcSight). Decipher which events warrant opening a trouble ticket, and which are considered network noise. Work with operators and analysts in the TSA SOC to determine and analyze any tickets opened as a result of NetIQ's scanning and reporting activities. Familiar with FISMA rules and recommendations regarding access controls, configuration management, audit, accountability as well as authentication. Provided a roadmap that identified TSA's security-hardening rules into NetIQ's own rules. Assisted in creating rules in ArcSight to analyze any breaches of security guidelines. Identify business process, design and implementation of NetIQ and its transition of data into ArcSight. Supervise 3 junior analysts and 3 operators. Generated Daily threat reports using RSS feeds such as Secunia, as well as NetIQ. Responsible for scanning TSA servers (using Foundstone and Nessus) prior to placement in the TSA network. Provided scan reports. to proper

management levels, via portal as well as PDF-formatted reports. Troubleshoot servers - e.g. Scan Engine, NetIq SM, and VM servers. Hands on experience with Plan of Action and Milestone (POAM) process. Provide C&A testing on new incoming servers, using NMAP (Foundstone Scanning). Familiar with configuration management in regards to remediation of servers in the secured network environment. Assist Project Manager in various administrative duties to include: interviewing possible candidates, audit and sign timesheets, ensure team is meeting SLA requirements, and investigating failure thereof. Experienced in developing a security stature - e.g. developing policies, assessing risk, and countermeasures. Participated in the security architectural panel, where design and implementation of security measures are both discussed, and planned. Provided assistance in formulating, budgetary compliance, as well as financial input in any RFP's. Technologies and Tools used: NetIQ Vulnerability Manager, Security Manager, ArcSight, Foundstone, Secunia, NetCert, NMAP,NESSUS. Contractor self-employed May 2004 to June 2006 Security and Financial Consultant Provide technical support for sales personnel. Technical support provided for Vulnerability management solution- including assessment and remediations. Responsible for setting up technical demonstration of the company's Vulnerability management solution. This solution is a hardware/software enterprise security solution. Familiar with Vulnerability scanning and reporting using Nessus as well as Foundstone, and Altiris.. Familiar with RSS feeds including Secunia, USCert. Responsible for testing software versions as they evolved. Responsible for upgrading existing clients' software. Provide webinar and webex demonstration, as well as live demos. Authored installation and training manuals. Provide internal training as well as for business partners. Responsible for version management of all training and installation manuals. Familiar with VMWare. Provide technical response to RFP and RFQ's. Provided financial analysis for firms bidding on RFQ. Formulated budgets and burn rates for clients based on awarded as well as prospective contracts. Generated variance reports for budget versus actual costs. Experienced in responding to government RFP's and RFQ. Dept. of Treasury - NOC Engineer EIS Enterprises Inc September 2000 to May 2004 Member of the Internet Security team supporting the Treasury Department's private network of over 350,000 users,

the largest private network in North America. Responsible for all Internet operations and maintenance of firewalls, load-balancing servers, Sun Servers providing Send Mail services. Configure, maintain and monitor X.500 and LDAP servers. Research virus threats and escalate as warranted. Update and maintain virus pattern files and scan engines on mail servers. Configured and tested Cisco routers, prior to installation. Configure and maintain internal and external DNS servers. Monitor and analyze network activities and logs for scanning, probing, or intrusion Develop and deploy component failure, impact analysis documentation to include; repair time, affected systems, services, costing, and emergency methodologies. Update security scheme as required. Perform routine Unix, NT, DNS, and firewall system administration as required or recommended. Experience in troubleshooting, TCP/IP networks, gateways, routers, switches and firewalls. Familiar with configuring and securing Axent /Raptor firewalls. Troubleshoot routing and data circuits issues on Treasury WAN. Responsible for constant Wide Area Network connectivity throughout US Treasury sites. Hands on experience with HP Open View, Peregrine, Tivoli NetView, NetCool, and Nagios monitoring systems as well as Remedy ticketing system. Perform configuration management duties for firewalls, routers, and switches - e.g. OS and SW versions. Perform queries on Oracle based relational databases - including over 2000 nodes within the Dept. of Treasury network. Used on a daily basis the following protocols SMTP, LDAP, EIGRP, OSPF, SNMP, SSH, SSL. Education Bachelor's Degree in Accounting and technical background George Washington University Skills ms office (8 years), IT seurity (10+ years), Accounting (10+ years), IT engineering (10+ years) Certifications/Licenses Symantec Endpoint September 2020

Name: Marie Barrera

Email: dustin39@example.org

Phone: +1-469-279-4073