Senior Cyber Security Analyst Senior Cyber Security Analyst Senior Cyber Security Analyst - Weatherford International Houston, TX ? 6+ years' worth of experience in Cyber Security/Project Management/Cyber Counterintelligence /Network Security Architecture/Malware Reverse Engineering ? Information Security Analyst with a solid track record of success leading teams and driving operational improvement in governmental and privately-run organizations. ? Successful at utilizing multiple Cyber Security tools and applications for analysis and threat hunting to identify anomalies in the environment, increase security, and decrease risk over company and client systems to facilitate smooth operations. ? Demonstrates a high level of understanding for operational and project management functionality which enhances quick decision making and resolving tactical issues using procedural (SLA) timeframes outlined by the organization. ? Proven record of evaluating system vulnerability in-order to recommend security improvements as well as improve efficiency while aligning business processes with network design and infrastructure. ? Superior capacity to solve complex problems involving a wide variety of information systems, work independently on large-scale projects, and thrive under pressure in fast-pace environments while directing multiple projects from concept to implementation. ? Supported client security policies and activities for networks, systems, and applications including vulnerability management, incident reporting, mitigation, and continuous monitoring. ? Worked on all assessment and authorization (a& a) phases and processes. Proven ability to support the full lifecycle of the assessment and authorization (a& a) process. ? In accordance with NIST, FISMA, OMB app reviewed and updated the Information system security policies. Used Iii a130 and industry best security practices. Solved unique and complex problems with broad impact on the business. Subject Matter Expertise In: ? Project management for large cyber security projects utilizing advance methodology (e.g. Six Sigma). ? Developing strategies to enhance overall cyber security program. Maintaining and improving security posture for IT governance. ? Advanced Persistent Threat (APT)/ Cyber CI (Counterintelligence) ? Cyber Security Forensic (malware analysis/ identifying intelligence related activity) ? Cyber security for critical infrastructure Nuclear, Oil, & Gas (SCADA/NERC CIP) ? Cyber security (FISMA) for US Government DoD (DIACAP), Civilian (NIST) ? Advanced cyber intrusion analysis/detection/forensic (rootkit, malware, etc.) ? Penetration Testing for large enterprise networks. Authorized to work in the US for any employer Work Experience Senior Cyber Security Analyst Weatherford International - Houston, TX June 2017 to Present Responsibilities: ? Applied PMI processes for all Cyber Security projects, redesigned cyber security processes through BRP, and used Six Sigma for quality enhancement on multiple cyber projects. Performed static & dynamic analysis of malware (APT) and its delivery mechanism (malicious documents e.g. pdf, doc, etc.). ? Extracted TTP, exploit, author attribution, C2, and more. Utilized custom sandbox to isolate malware, unpack malware, monitoring registry changes, and identifying malware communication channels. ? Analyzed high-level language constructs (branching statements, looping functions, network socket code, and more) of malware/APT. ? Performed digital fingerprinting to determine foreign adversary/actor behind malware/spear phish and correlated the data back with the Intelligence community. ? Used malware (APT) analysis to develop IDS signatures (Snort), FW rules, AV signatures, Net Witness Meta, and create ArcSight channels/reports for APT specific threats ? Produced reports & briefings to provide an accurate depiction of the threat landscape that impacted the US Congressional resource. Liaison for Cyber Threat Analysis entities such as Joint Cyber Threat Working Groups, Law Enforcement, DOD and the Intelligence Community. Developed Tactics, Techniques and Procedure (TTPs) reports. ? Conducted Cyber CI (Counterintelligence) assessments, operations, and investigations for congressional programs. Assessed the effectiveness of Cyber CI related activities across the organization. Identified problems that directly affect the accomplishment of Cyber CI program goals and objectives and created alternatives and corrective actions. ? Developed and coordinated proactive Cyber CI projects and activities to detect attempts by foreign intelligence services to target Congressional resources (technology and personnel). ? Provided assessments on cyber capabilities and activities of foreign intelligence, security services, and potential threats to and impact on Congressional information systems and operations. ? Conducted open and classified source research in support of Cyber CI initiatives. Created and updated threat profiles for congressional programs and its asset to be used for threat modeling for potential cyber-attack/spear attack. ? Served as a Cyber CI investigator for reports of

CI anomalies or allegations of espionage. Documented investigative activity by preparing detailed written reports. Maintains liaison contacts throughout the intelligence community. ? Reviewed the security architecture of the organization to find gaps that impact the enterprise. Provided comprehensive solutions to enhance the security architecture. Cyber Security Consultant Able Vets LLC - Kearneysville, WV April 2016 to May 2017 Responsibilities: ? Managed various IT security projects to ensure project were in scope, budget, and time. Managed staff members on various cyber security projects. ? Conducted data exfiltration/leakage assessment (Advanced Persistent Threat /APT). ? Performed malware analysis using various tools (e.g. Encase, HBGary FireEye, Net Witness, IDA Pro). Conducted analysis on captured user, computer, and network security events, in a near-real time environment, to determine security vulnerabilities, policy violations, and malicious behavior. ? Identified user behavior that may be indicative of potential malicious or counter intelligence related activity. ? Performed IT auditing services (C & A) for various government agencies using NIST, NERC CIP, SCADA & DoD (DIACAP) guidelines. ? Implemented risk management framework for organizations and developed affective strategy for continuous monitoring. Developed secure guideline for cloud computing, worked on projects integrating IT governance controls in cloud computing. ? Performed penetration testing & vulnerability assessment for compliancy assessment. ? Developed documentation for security authorization package/certification packages (e.g. ST & E, POA & M, security plans, business continuity plans/disaster recovery plans, risk assessments and more, ? Developed IT security policies, guidelines, baselines, and procedure for various organizations (government, banking, commercial, and more) to reflect their respected IT governance adherence (e.g. FISMA (NIST/DIACA), SOX, PCI, SCADA, NERC CIP and more). ? Assist in the writing and review of organizational security policies to support internal control (access management, contingency planning & testing, Security Awareness, intrusion detection, Patch Management, Anti-Virus, etc.) ? Developing IT security internal control for SOX environment (section 302 & 404). Auditing for Internal control for IT governance project (FISMA/SOX). Auditing domains such as Change Management, Access Management, and Operations for SOX [section 404], Cyber Security Manager Jelani Consulting, MD

August 2015 to April 2016 Responsibilities: ? Utilized various project management methodology & PMI process to enhance various cyber security programs within the Department. Managed the 24x7 DoT SOC/CIRT. ? Developed reports for CIO, CISO, and other executives (Dept. Secretary) about IT security posture across the department. Developed daily cyber security situation awareness reports from various sources (advisories, SIEM, Intel briefing, etc.). Advised in IT risk management for the department. ? Lead liaison for cyber security for the Department. Incident response liaison between the department and other government organizations (DHS US-CERT, DC3, NSA). Represented the department in government wide initiatives Cyber Storm, GFIRST, NCRCG, Federal Law Enforcement, JointCyber Threat Working Groups, DOD and the Intelligence Community. ? Analyze Cyber Intelligence threats (advanced persistent threats) by investigating of cyber security incidents, assisting the DOT Inspector General, FBI, NSA, ARL (Army Research Lab), AFRL (Air Force Research Lab), and other law enforcement agencies with forensic analysis (Malware/shellcode analysis via. tools Encase, IDApro) ? Designed & implemented the department SIEM (Arcsight) to monitor the DOT enterprise (over 20,000 assets). Administration of the DOT security infrastructure consisting of IDS/IPS systems (Snort, ISS, IDSM2, IPS, NFR, Checkpoint IPS1), Vulnerability Assessment tools (Found scan and Nessus). ? Creating IDS signatures to detect undesired or malicious network activity (i.e. APT, worm scanning and payload propagation). ? Assist in the writing and review of Departmental security policies (Security Awareness, IDS, Patch Management, Anti-Virus, etc.) ? Ensuring that systems were compliant with departmental rules, OMB mandates & FISMA (NIST guidance). ? Developed C & A (certification and accreditation) documents (System Security Plans, Security Test & Evaluation Plans, Risk Assessments, Contingency Plans) on major systems using NIST guidelines (NIST 800-18, NIST 800-30, 800-53, and more). Managed the continuous Monitoring phase, which included monitoring and mitigating POAM, conducting self-assessments. ? Assist in authoring OMB Exhibit 300 Capital Asset Plan and Business Cases and related content to include performing and documenting analyses of alternatives (AOA), cost benefit analyses, risk analyses, developing performance goals and measures, and authoring related CPIC life cycle documentation to the OMB Exhibit 300 for the IT security portfolio.

Inspected and approved information assurance aspect of OMB Exhibit 300. IT Security Specialist INOVA - Sterling, VA September 2014 to July 2015 Responsibilities: ? Manage system information security architecture, design, installation, operational planning, and risk remediation activities on more than 15 servers/systems worldwide for various government clients, ensuring all systems installed according to schedule. ? Conduct risk assessments and collaborate with clients to provide recommendations regarding critical infrastructure and network security operations enhancements. ? Develop Continuity of Operations (COOP) and Disaster Recovery (DR) operations and conduct evaluation of COOP and DR during annual incident response training. ? Provide up to ten on-site server maintenance visits on monthly basis, troubleshooting various technical problems and performing operating system administration with Linux-based computer systems. ? Ensure information assurance by transmitting secure data between classified systems; perform ethical hacking, malware reverse engineering, penetration testing, and Certification and Accreditation (C&A) within Security Operations Center (SOC) environment. ? Draft technical manuals, installation manuals, installation progress updates, and incident response plans in-order to enhance system security documentation; create required system compliance reports and information requests. ? Enforce IT processes to ensure consistent, well-integrated application structures in full compliance with Sarbanes Oxley (SOX) and Payment Card Industry - Data Security Standards (PCI DSS) regulations; participate in system Certification and Accreditation as well as Federal Information Security Management Act processes. IT Security Analyst Tuva LLC - Odenton, MD November 2013 to August 2014 Investigated use and configuration organizationally of multiple business process tools and create gap analysis on current solution vs. Ideal solution. ? Communicated functional and technical analysis, design and specifications to all supporting organizations. ? Collaborated and directed efforts within quality assurance to ensure desired results. ? Developed innovative solutions to meet the needs of the business that can be reused across the enterprise creating the environment for consolidation of tools to robust, customizable solutions. ? Redesigned the agency internal control plan in compliance with the new regulatory guidelines. ? Ensure it controls of the environment are secure and meet the required policies related to institution, federal, state, and local regulations. ? Performed periodic audits/reviews on application and department access rights to Identified, triaged, and documented the instances of vulnerability areas and devices. Education Bachelor's Degree in Computer Science University of the Western Cape Additional Information Core Competencies: ? Staff Management ? Disseminating Data ? Investigations & Incident Response ? Con Ops & Gap Analysis ? Operations Management ? Empowering Leadership ? Project Management ? Documentation Systems ? Cyber Security Analytics ? Monitoring Events ? Reports & Analysis ? Policies & Procedures   TECHNICAL SKILLS: Software Tools: Windows Office Suite, Smart Dashboard (Firewall Application), Wire Shark, Cisco WAAS Device, SolarWinds, Check Point, Source Fire, Bit9, Carbon Black, Proof Point Ticketing Applications: Remedy, Seibel, Maximo, Jira Security Systems: McAfee, IDS/IPS, VPN, Firewall, NAC, Secure Analytics, Risk Vision, Stealth Watch Operating Systems: Windows Client, Windows Server, Windows 7, 8, 10, Mac, Kali Linux Monitoring/Threat Hunting Applications: Nessus, Qualys Guard, ArcSight, Splunk, McAfee ePO, RSA Archer, Fire Eye Tools, Kibana, HP OpenView Security Standards/Guidelines: FISMA, NERC CIP, BASEL II, SOX, PCI DSS, GLBA, HIPAA, and more Networking: SAN, LAN, WAN, WINS, DNS

Name: Andrea Jarvis MD

Email: jsloan@example.net

Phone: 784-723-7950