Cybersecurity/ Incident Response Analyst Cybersecurity/ Incident Response Analyst Information Technology Engineer - Smart Computing Solutions Bowie, MD ? A Security Assessment and Authorization (SA&A) professional knowledgeable in Compliance and Risk Management Framework (RMF), System Development Life Cycle (SDLC), Risk Assessment and Vulnerability Management, FISMA, FedRAMP and OMB. ? Experience in using the following NIST SPs: 800-18, 800-37, 800-39, 800-53/53Arev4, 800-60, FIPS 199 & 200, Sans 20 and IS0 27001. ? Experience in the development and review of artifacts such as System Security Plans (SSP), Contingency Plans (CP), Disaster Recovery Plans (DRP), Incident Response Plans (IRP), Configuration Management Plans (CMP), Privacy Threshold & Privacy Impact Assessments. ? Understanding of Cloud protections as expressed in FedRAMP for Federal Government agencies. ? Knowledge and experience with IT security theories, concepts, best practices, and emerging issues; the infrastructure protection environment and project management theory and techniques. ? Experience documenting technical issues identified during security assessments and recommending improvements in the existing service support tools and standard findings ? Knowledge of Assessment & Authorization (A&A) process to support Authority to Operate (ATO) activities including but not limited to security control assessments (SCA) and POA&M management ? A proven team lead with aptitude for good customer service, and excellent communication skills. ? Thrive in a highly collaborative, fast-paced work environment and multidisciplinary team setting where leveraging technology for continuous business improvement is the norm Work Experience Cybersecurity/ Incident Response Analyst Encompass IT Security Solutions - Bowie, MD April 2019 to Present Perform incident monitoring, response, triage, and initial investigations Monitoring and analysis of security events to determine intrusion and malicious events. Monitor Security events and logs such as Proxy logs, IPS/IDS events, Firewall, Active Directory (user verification), Vulnerability Scans, Anti-Malware events, Endpoint Security, Web Application Firewall, NetFlow, Packet Capture, computer log files, etc., to maintain situational awareness. Utilize security tools to perform investigative correlations such as Splunk, FireEye(HX, EX, NX), McAfee ePO, Nessus, Wireshark, RSA Security Analytics, and more. Perform investigations and evaluations of network

traffics, read & interpret log, sniffer packets, and PCAP analysis with RSA Security analytics and Wireshark Identify and ingest indicators of compromise (IOC s) (e.g., malicious IPs/URLs, etc.) into network security tools/applications. Investigate all security alerts received by making use of all tools and log files possible to determine if the alert is a false positive, a security event, an actual attack, and/or a security incident Quarantine the machines with suspicious behavior and initiate triage Create and track incidents and requests with ServiceNow, Remedy, and JIRA Process and complete tickets received from ServiceNow such as Non-Standard Software Require, Unblock Request, Lost and Stolen, etc. Escalate any security incident (the confidentiality, integrity, or availability of any information or information asset is negatively impacted) to Incident Response (IR), Incident Management team (IMT), Forensics Management Analysis Team (FMAT) as needed Perform investigations and evaluations of network traffics, read & interpret log, sniffer packets, and PCAP analysis with RSA Security analytics and Wireshark Collaborate with technical and threat intelligence analysts to provide indications and warnings, and contributes to predictive analysis of malicious activity Identify and ingest indicators of compromise (IOC s) (e.g., malicious IPs/URLs, etc.) into network security tools/applications. Investigate malicious phishing emails, domains and IPs using Open Source tools and recommend proper blocking based on analysis. Investigate all reported suspicious emails and determine whether the email is malicious, non-malicious or legitimate and reply to the user who reported the suspicious email with a message reporting the determination and any recommendations Perform shift handoff at the end of every shift to provide situational awareness to the incoming shift IT Specialist & Business Analyst Reside One Corporation - Lanham, MD May 2014 to Present Diagnosed, troubleshot, and resolved a wide range of software, hardware, and connectivity issues ? Researched and solved problems on workstation and LAN, including IP resolution, cabling problems, and peripheral malfunctions ? Provided configuration support for both Office 365, Google Docs & Quickbooks ? Implemented new software and data migration ? Created and managed website, housing listing database, and software ? Review logs and defended against cyber attacks such as Malware and Phishing Information Technology Engineer Smart Computing Solutions - Annapolis, MD February 2019 to

April 2019 ? Provided Desktop, Application, and Network support to 1500+ end users within the company head office and remote locations ? Provided excellent customer service and ensure quick resolution to concerns ? Performed Active directory services remotely and onsite for over 100 clients using both physical servers and cloud environment ? Monitored and Configured workstations using SolarWinds MSP ? Assisted in installing complete network environment ? Deploy/Install IT equipment, including personal computers, scanners, laser jet printers, peripheral devices, etc. ? Researched and solved problems on workstation and LAN, including IP resolution, cabling problems, and peripheral malfunctions ? Triage, troubleshoot and resolve issues concerning network communications such as internet connectivity, email communications, printers (local/network), and/or VPN communications. ? Managed daily activities to include user support and systems administrator tasks ? Reviewed logs for security for security incidents ? Performed email analysis to defend against malware and ransomware Cyber Security Analyst Intern Encompass IT Security Soltuions - Bowie, MD June 2018 to August 2018 Applied cyber security policy with company procedures using NIST 800-37 & 800-53 standards Creating proposals for new GSA schedule 70 contract Utilized virtual machines for remote penetration testing using Metasploit and Tenable Nessus Utilized Security Information and Event Management (SIEM), Intrusion Detection (IDS) & Prevention (IPS) Formulated past performance reviews & quality controls Utilized virtual machines using Kali-Linux and VMware Workstation Worked in both Linux and Windows Environments Adapted and quickly learned a new position and industry to further develop analytical and technical skills. Education Bachelor's in Information Systems University of Maryland, Baltimore County - Baltimore, MD Skills JUNIPER, NESSUS, SPLUNK (3 years), VLAN, WIRESHARK (3 years), IDS (3 years), IPS (3 years), SIEM (3 years), Virtual Machines, Excel, database, Microsoft Excel, Management, Snort, MS Office (10+ years), Remedy (3 years), SolarWinds (2 years), Cyber Security (3 years), Security Operation Center (2 years) Certifications/Licenses CompTIA Security+ Additional Information Skills Highlight: Security Assessment & Authorization ? POA&M Management Vulnerability Assessment Tool ? Authorization-to-Operate (ATO) operating systems ? System Security Documentation ?

Vulnerability Management ? Risk Assessment & Compliance GRC Risk Vision ? Security Requirement Traceability Matrix Technical Skills: Windows 2000, XP, 7, 10, Windows Server 08/16, Windows Active Directory, TCP/IP, DNS, WINS, Telnet, RDP, VLAN, Switches, Routers, Wireless Routers and Hubs, Microsoft Office, Outlook, Word, Excel, HTML, DHCP, RSA Security Analytics, Splunk, Wireshark, Kali Linux, McAfee ePO, SolarWinds, Nitro, FireEye (EX, NX, HX), Juniper, Nessus, Bro, RSA Archer, Suricata, ServiceNow, Datto AutoTask Remedy, and JIRA

Name: Jamie Carter

Email: harrellryan@example.com

Phone: 339-284-7434x90591