Cybersecurity Risk & Vulnerability Analyst Cybersecurity Risk & Vulnerability Analyst Winchester, VA Authorized to work in the US for any employer Work Experience Cybersecurity Risk & Vulnerability Analyst Leidos - Reston, VA May 2019 to Present Identifies and classifies vulnerabilities as applicable to the government clients information systems. Conducts vulnerability scans using Tenable Nessus (Security Center), WebInspect, and other vulnerability management tools. Aids in the management and administration of vulnerability scanning infrastructure (hardware and software). Conducts detailed risk analysis based on enterprise vulnerability footprint. Correlates system risk using cross-team collaboration with Incident Response. Manages inbound information system vulnerability management (ISVM) reports from the government client. Provides supplemental support to the incident handling lifecycle through identifying potential means of adversary access Senior Information Security Analyst Nuix North America - Herndon, VA July 2018 to May 2019 Working with the CISO to determine and translate strategic goals into actionable and measurable activities. Provide incident response for all internal information security incidents. Work with the CISO and respective teams to maintain a current and accurate inventory of all IT assets. Work with the CISO and respective teams to deploy and monitor other information security assets to include antivirus solutions, firewalls, intrusion detection products, etc. Responsible for the deployment and maintenance of vulnerability scanning tools such as Nessus Security Center, and automated pentetration testing tools such as XM Cybers' HaXM. Cybersecurity Analyst - Tier 2 ALTA IT Services - Rockville, MD December 2017 to July 2018 Monitoring various security tools (e.g., Splunk, SourceFire, Cisco ASA) to identify potential incidents, network intrusions, and malware events, etc. to ensure confidentiality, integrity, and availability of information systems are protected Reviewing and analyzing log files to report any unusual or suspect activities. Utilize incident response use-case standard operating procedures to follow established and repeatable processes for triaging and escalating. Generating trouble tickets and performing initial validation and triage to determine whether incidents are security events using open source intelligence (OSINT). Following established incident response procedures to ensure proper escalation, analysis and resolution of security incidents. Analyzing and correlating incident event data to develop preliminary root cause

and corresponding remediation strategy Providing technical support for new detection capabilities, recommendations to improve upon existing tools/capabilities to protect the network, and assessments. Research Analyst FCi Federal - Ashburn, VA September 2017 to December 2017 Review and analyze potential identifiable documents to determine whether a specific individual has been the subject of or mentioned in any investigation(s), and if so, what information may be disseminated to the requesting agency. Conduct numerous name searches in direct support of the counterterrorism, counterintelligence, and homeland security efforts. IT Support Engineer N & L Enterprises - Fairfax, VA August 2016 to September 2017 Provide end user support through ticketing system with issues ranging from hardware/software issues, VOIP QoS, and networking issues. Installation of network hardware such as switches, patch panels, and cable management systems. Installation and initial setup of servers for various applications. Develop and manage an updated inventory of all company equipment for an up-to-date asset management system. Service Desk Analyst TalentWise Solutions - Winchester, VA March 2015 to August 2016 Provided end-user IT support for users by installing tools, applications, system updates, patches, and configuration changes. Fixing IT equipment including PC s, printers, and screens. Performs troubleshooting and resolution to address various internal network related issues. Experience with installing, testing, and troubleshooting switches and routers, as well as monitoring capacity utilization for IT resources. Prepare equipment for reuse or surplus of property assets. Education BS in Information Systems Security American Public University System - Charles Town, WV July 2014 to May 2016 AAS in Computer Support Hagerstown Community College - Hagerstown, MD August 2009 to December 2011 Skills Nist, Splunk, Network Security, Fisma, Information Security, Information Assurance, Palo Alto, Cissp, PCI, Juniper Certifications/Licenses CompTIA Security+ January 2017 to August 2020 CompTIA Server+ June 2017 to Present CompTIA Cybersecurity Analyst+ August 2017 to August 2020 EC-Council Certified Incident Handler January 2018 to January 2021 Additional Information Active Top Secret clearance.

Name: Brenda Fitzgerald

Email: emilyanderson@example.net

Phone: +1-537-953-6613