Computer Network Defense Analyst Computer Network Defense Analyst Computer Network Defense Analyst Laurel, MD Work Experience Computer Network Defense Analyst TEK Systems Inc - Linthicum, Maryland October 2018 to Present Army Research Laboratory Cybersecurity Service Provider (ARL CSSP) Monitor client networks to detect suspicious and hostile activity Monitor client cloud networks to detect suspicious and hostile activity Review logs from various security tools and network traffic analyzers Compile information and prepare computer security incident reports Work closely with infrastructure engineers, information assurance engineers, and system administrator Provides assistance in computer incident investigations Assist in troubleshooting and problem solving a wide variety of client issues Review non-government web sites and other sources of information for threat/warning notifications Check counterpart organizations web sites for threat and warning notifications Provide quality customer service Computer Network Defense Analyst Phacil - Arlington, VA March 2017 to Present High Performance Computing Modernization Program (HPCMP) Works as a Vulnerability Assessment Team Analyst Constant monitoring of intrusion detection systems (Bro logs) Receive and analyze network alerts from various sources within the network environment or enclave and determine possible causes of such alerts (Kibana, CEDAR) Characterize and analyze network traffic to identify anomalous activity and potential threats to network sources Provide information security support through vulnerability identification and testing, and perform assessment and mitigation of vulnerabilities, internally and externally Perform event correlation using information gathered from a variety of sources within the network environment or enclave to gain situational awareness and determine the effectiveness of an observed attack Check counterpart organizations' web sites for threat and warning notifications Review non-government web sites and other sources of information for threat/warning notifications Provides assistance in computer incident investigations Work in an integrated team environment, manage and administer automated and manual vulnerability scan tools, and ensure appropriate reports are delivered on-time Create technically detailed reports based on intrusions and events (Incident Report Tracker) Maintain appropriate relationships with subject matter experts inside and outside of organization to ensure they adhere to

internal and industry best practices Use and administer various scanning and assessment tools to identify system vulnerabilities and test security controls. Provide recommended remediation steps and countermeasures to reduce risk exposure and strengthen defense in depth Utilize Redmine for team collaboration and to track project activity Assist in troubleshooting and problem solving a wide variety of client issues Provide quality customer service Systems Administrator / IASO STG - Reston, VA November 2007 to March 2017 Army Research Laboratory - Applications Management Development Branch (AMDB) Analyze, install, deploy, integrate, and support the Enterprise Information Management (EIM) system and eARL framework products in the development, staging, and production environments Support, maintain, and utilize a testing environment. Integrate tested products into production environment Provide day to day operations of the ARL AMDB development, testing, staging, and production environments Prepare and maintain documentation and SOPs for each system Configure and maintain servers, software and provide a full-service networked environment for the EIM system and eARL framework Configure and maintain VMWare servers to reduce cost of operations Employ server and network monitoring tools such as Nagios, OSSEC, and Splunk to ensure servers are functioning properly Utilize Splunk to provide log data to AMDB developers and senior leadership for multiple projects Utilize OSSEC to provide host base intrusion detection. Review alert logs and emails for abnormalities Utilize Nagios to provide monitoring of server hardware and system processes. Review alert logs and emails to address any issues Utilize Security Center tool within Assured Compliance Assessment Solution (ACAS) to scan AMDB servers for vulnerabilities Perform DIACAP on production servers (web and application) using Security Technical Implementation Guides (STIG) checklist and Security Readiness Review (SRR) scripts provided by Defense Information Systems Agency (DISA) Perform Information Assurance Security Officer (IASO) function. Ensure systems are operated and maintained according to DoD, Army, and local policy. Approve installation and use of organization unique software, verify software vulnerabilities, implement and report IAVA compliance Resolve escalated CA Unicenter Service Desk tickets Track project activity, progress, and issues using Redmine Provide IT technical support to ARL AMDB staff Monitor backup and restore operations

Managing and reviewing user accounts access (Windows and UNIX) Maintain, administer, and support ARL's automated multi-facility, multi-site Technical library infrastructure Install, migrate, upgrade, backup, and maintain library server (UNIX) and database (Oracle) Perform library system administration functions Systems Analyst / Help Desk Specialist TMSI / STG - Gaithersburg, MD October 2005 to November 2007 Army Research Laboratory Configures servers and workstations to communicate with the network by setting up network protocols Dell computer replacement program. Performs data transfer from old pc to the new, along with the setup of any additional software. Dissembles old machine and prepares it for excess after customer has verified new machine installed properly. Utilizes Ghost cast server to perform new images and rebuilds of Windows platforms (Win 2k, XP) Performs system administration duties to include adding, deleting and changing user profiles on domain and email servers using Active Directory 2003. Creates tickets using the CA Unicenter Service desk ticketing system, and accurately imputing updating tickets with all pertinent actions and data. Downloads and installs compatible drivers from the Internet (for various hardware devices) Supporting customers with configuration and hardware installations that ensure 100% customer satisfaction. Responsible for upgrading software applications, performing anti virus checks, and providing efficient customer service for approximately 3500 end users. Performs installation and repair of hardware to include printers, scanners, Blackberries, PDA's, Monitors and CPU's Conducts informal end user training Installation and support of COTS software Supports Microsoft Windows XP and Vista as well as Microsoft Office 2003 and 2007 Installation of Microsoft Security patches Education Bachelor of Science in Computer Networking in Computer Networking Strayer University - Alexandria, VA 2004 to 2007 Associates in Arts degree in Computer Information Systems Strayer University - Washington, DC 1998 to 2000 Maryland University - College Park, MD 1993 to 1995 Certifications/Licenses CEH Certified February 2017 to February 2020 VCA-DCV Certified September 2014 to Present SSCP Certified April 2017 to April 2020 Linux+ Certified March 2010 to Present Security+ Certified August 2017 to August 2020 ITIL Certified June 2012 to Present Additional Information InfoTech Training Institute, Silver Spring, MD MCP Certified June 2004 Digital Corporation, Silver Spring, MD

CCNA Course September 2001 Network+ Course February 2001 A+ Certified March 2000 Signal Corporation, Fairfax, VA PKI Certified Local Registration Authority (LRA) February 2002 PKI Certified Trusted Agent (TA) November 2001 U.S. Army DISA ACAS v5.3 September 2018 DISA HBSS Advanced (301) ePO5.3 August 2018 DISA HBSS Admin (201) ePO5.3 July 2018 Vulnerability Assessment and Mitigation July 2018 CSSP CEDAR March 2017 PCAP Analysis March 2017 CEH Certified February 2017 DISA ACAS v4.6 March 2015 VCA-DCV Certified September 2014 SSCP Certified April 2014 ITIL Certified June 2012 Server+ Trained April 2010 Linux+ Certified March 2010 Security+ Certified August 2009 IAT Level I Training May 2008 Information Assurance Security Officer (IASO) November 2007

Name: Stacey Garcia

Email: nsmith@example.org

Phone: (406)918-3130x61686