Cloud Security Architect/Engineer Cloud Security Architect/Engineer Cloud Security Architect/Engineer - United Power Woodbridge, VA I am an IT Professional who is looking to secure a challenging position in an Information Systems and Technology field, which provides the opportunity for upward mobility based upon quality performance. I can utilize my skills in Cyber Security, Information Security, Intrusion Prevention, Pen Testing, Red Team, Blue Team, Vulnerability Assessments, Risk Assessment, Risk Mitigation, Network Disaster Recovery and Business Continuity, Cloud Architecture and Cloud Security to help organizations succeed in meeting their current needs as well as future expectations. Work Experience Cloud Security Architect/Engineer United Power - Las Vegas, NV January 2019 to Present Install of AWS CLI/Console to control various AWS services and secure our Cloud Environment. Use Python to automate software configuration. Setup and attach EBS volumes to EC2 instances for scaling up/down or scaling in and out based on throughput. Create multiple VPCs and public, private subnets as per requirement and distribute them as groups into various availability zones of the VPC. Create and configure elastic load balancers and auto scaling groups to distribute the traffic and to have a cost efficient, fault tolerant and highly available environment. Secure S3 buckets in the AWS environment to store files, sometimes which are required to serve static content for a web application. Configure S3 buckets with various life cycle policies to archive the infrequently accessed data to storage classes based on requirement. Create RDS instances to serve data through servers for responding to requests. Create snapshots and images to store launch configurations of the EC2 instances. Setup and manage Security Groups, VPC'S specific to environment. Monitor and work on alerts and issues related to server availability, disk issues, CPU, memory, processes etc. using Splunk. Manage and create User accounts, Shared Folders, provided day to day User support, Log management, Reporting, applying Group Policy restrictions etc., Identify root cause of Network problems. Develop Infrastructure on AWS using various services like EC2, S3, RDS, ROUTE 53, Cloud Formation, Cloud Watch, IAM, VPC etc., Work with VPC, Subnets, and Route tables, etc., Work with Continuous Integration (CI) and Continuous Deployment(CD) methodologies Provide support for developers by collaborating with the

development team using the agile methodology. Manage and automate all aspects of our AWS infrastructure (compute, storage, network, permissions, cost) using configuration management tools like Cloud Formation. Assist in designing, automating, implementing and sustainment of Amazon machine images (AMI) across the AWS Cloud environment. Work with AWS API Gateway and Rest APIs. Create and modify Cloud Formation templates to create/upgrade EC2 Instances to support specific needs Work with WAF and Firewall Manager and AWS Shield Advance to help protect resources across accounts. Information Security and Network Analyst Federal Home Loan Bank - Reston, VA January 2018 to December 2018 Created Web application vulnerability assessments following OWASP Pentest web applications performed password cracking using aircrack-ng, Hydra, John the Ripper Utilize Nessus /Tenable to Scan web application for vulnerabilities and viruses Deployed, configured, customized on Linux, Windows systems. Test Software applications and servers for vulnerabilities before deploying it to the network Identifies security risks, threats and vulnerabilities of networks, systems, applications and new technology initiatives. Provides technical support in the development, testing and Monitored, Configured, Scan/Patch Network TCP/IP, DNS, Telnet and DHCP. Utilize Nessus, Nmap, Web Inspect and Microsoft Surface Analyzer toolset to Scan all ports, access points, devices and software on the network. Managed/Secured and Scanned devices, software, Web applications following NIST 800-53 protocol & FIPS 140-2 Support security assessments [SA&A] and Certification and Accreditation [C&A] activities) and audit Identify, Manage and develop Plan of Actions and Milestones (POA&M) and mitigation strategies for potential Conducts complex security architecture analysis to evaluate and mitigate issues. Develops policies and procedures for securing the system infrastructure and applications. Develops complex technical and programmatic assessments, evaluates engineering and integration initiatives and provides complex technical support to assess security policies. Created vulnerability risk assessments for in house, COTS and 3rd party applications. Utilize Wireshark, Nessus to Pen-test, and Experience with security assessment tools such as Metasploit, and/or Netcat, Nikto, Burp Suite. analyze the network and software's. Utilize McAfee ePolicy/End Point Protection Suite administration including virus

protection, HIDS/HIPS, firewall, encryption and other workstation security technologies. Address known exploits using the Host Intrusion Prevention System (HIPS) also, configured, monitored, installed and updated the application as well. Denied/Approved Software applications after testing the software for vulnerabilities and malware. Operation of firewalls, intrusion detection systems, enterprise anti-virus, Web Application Firewall(WAF) and software deployment tools. Perform day-to-day activities required to distribute application/software/patch packages and deploy operating systems using BigFix to end user hardware. Utilize BigFix for software Usage and Analyze Operating Systems Deployment and Bare Metal Imaging and Software Distribution. Utilize BigFix for Security and Compliance (SCA) Vulnerability Management, Configuration Management and Patch Management. Perform weekly git pull of our web application code (Static/Dynamic) for code review to examine bugs in code after sprints. Utilize PowerShell, SCCM for scripting, Imaging Windows OS, 7 & 10 machines. Manage and monitor ticketing system ensuring tickets are completed in a timely manner. Manage system backup Manage email, spam, and virus protection Administer servers, desktop computers, printers, routers, switches, firewalls, phones, personal digital assistants, smartphones, software deployment, security updates and patches. monitor network usage and security, undertake routine preventative measures to ensure network security. resolve technical problems with LANs, WANs, network segments, internet, intranet and other data communication systems; ensure network connectivity is on par with technical considerations Install, modify, and repair server / computer hardware (cables, hubs, routers, wireless adaptors.) and software. Manage and maintain VMware virtual server environment Manage and maintain the VMware virtual client environment Manage and maintain the SAN/NAS (e.g. NetApp) storage systems Setup, configure, and maintain hosted environments such as Microsoft Azure and Amazon Web Services. Manage and maintain Active Directory, User Accounts, Group Accounts, Computer Accounts, DHCP DNS and Domain Controllers. Manage and maintain the Microsoft System Center Configuration Manager(SCCM) for server updates as well as for client updates and automated builds and deployments. Ensure the proper execution of regular system backups Manage, maintain and patch Windows/Linux server operating systems and the applications running

on those servers. Remain up-to-date on security concerns and implement solutions as necessary Oversee and manage the Office 365 based email solution. Cyber Security Analyst The United States Government Publishing Office - Washington, DC July 2017 to December 2017 Use SIEM to monitor indicators of compromise, hunt potential threats within the network. Manage SIEM, server upgrades, back and front-end configurations, and application deployments. Create and modify queries to extract time sensitive data. Create SIEM applications from terminal Perform security operations support including monitoring, remediation, implementation, configuration, planning, encryption, and tracking in compliance with FISMA and other security-related statutes, regulations, rules, and standards. Provide proactive and scheduled console monitoring of infrastructure and systems in read-only in near real time (e.g., hardware, network, batch schedule, interfaces, and table spaces), respond to messages, and take corrective action as required. Utilize, operate, maintain, configure, secure, support, and update a Government security suite for tracking compliance; and for remote support, shall implement and sustain real-time data feeds and/or access as required by the SOC for security monitoring and analysis, and will provide access to archived security data for forensics and incident discovery. Work with the customer to modify and maintain firewall rule sets, implement those rule sets, and monitor the log files as well as the normal operation and maintenance of firewalls. Assist the customer in planning and executing the certification and accreditation of its critical systems in compliance with customer, Federal, and NIST guidelines and policies. Support both the review of information systems management, physical, and/or technical security controls and depending on the results of the review, the authorization by management for the system to operate. Assist the customer in fully complying with all FISMA reporting requirements and other security audits Assist in the implementation of comprehensive set of IT security-related operational policies, procedures, and guidelines that will support the customer's mission and ensure compliance with Federal and customer security requirements. Through the SOC, operate and maintain a collaborative dashboard where authorized Government personnel can view security-incident data, vulnerability data, compliance data, and security reports and related data. Enter and track security incident reports, enter service desk queue data to initiate ticketing in

response to security incidents or compliance issues, and manage remediation of detected vulnerabilities by correlating scanning results against asset management data and intrusion detection system (IDS) incident reports. Systems Administrator LightGrid, LLC - Virginia Beach, VA August 2016 to June 2017 Serve as an initial point of contact via face to face and VoIP for troubleshooting hardware/software PC and printer problems, research solutions and provide solid answers easily understood by all employees. Assist 100+ employees with computer software errors/issues and conduct problem determination for the Technology areas; including WANs, LANs, PCs, Laptops and configuring printers. Support over 100+ employees with installing, updating, and maintaining software, network, hardware, and external peripheral equipment. Receiving project management training to abide by ISO 9000 standards. Actively backed up company data via in-house system to create redundancy. Run diagnostic programs to resolve problems and conducts preventative maintenance on all equipment, including hard drive maintenance and virus and spyware removal. Document, track and monitor computer problems to ensure a timely resolution. Review and evaluate corporate policy directives to ensure program compliance. Execute IT software installments and ability to use remote management tools to resolve issues. Deploy software, installed hardware equipment, configured and troubleshoot user machines to provide the latest system requirements. Maintain an inventory and database of IT assets and assists in developing customer support policies, procedures, and standards. Analyze and reported quarterly data using Microsoft Excel and PowerPoint. Recognized for expertly diagnosing and replacing defective hardware by utilizing new testing tools. Content Analyst/Data Analyst Booking.com - Norfolk, VA June 2016 to August 2016 Worked to increase conversion, average days booked and average transaction value. Effectively communicated to senior management about the status of various projects through status reports and presentations. Worked on optimizing the listing quality and conversion on MyBookingPal.com, AirBnB and Booking.com software and programs. Created account strategies from data analysis and worked 150+ websites to increase profit margins for clients. Provided expert advisory services to partners by understanding key partner objectives, need periods, yield IT Security Analyst Dominion Enterprises -

Norfolk, VA August 2013 to June 2016 Defining system security plans and creating POA&Ms to ensure systems are in line with the Risk Management Framework and NIST standards. Providing systems engineering support to Agile development teams establishing and maintaining development, integration, and test, as well as production environments. Manage and administer Windows systems in a VMware, NFS environment. Review policies and procedures and provide impacts of revisions as necessary. Installing, configuring, troubleshooting and patching web servers, application servers (Apache Tomcat, IIS), databases (MS SQL) and Java applications in a Windows environment. Working knowledge of Networking, Storage, and Active Directory. Managing and administering applications in a Windows domain with PKI authentication. Debugging complex enterprise systems including clients, servers, routers, databases in a variety of configurations. Coordinating and advising CIO on best practices and matters of Cyber Security. Manage the continuous monitoring phase which includes monitoring and mitigating POAM and conducting self-assessments. Develop IT security policies, guidelines and procedures for company to reflect their respected IT governance adherence. Assist in the writing and review of organizational security policies to support internal control (access management, contingency planning and testing, security awareness, intrusion detection, patch management, anti-virus, etc.) Classification and categorization of Information Systems using the RMF processes to ensure system Confidentiality, Integrity and Availability. Manually review logs and provide documentation guidelines to business process owners and management. Determines enterprise information assurance and security standards. Develops and implements information assurance/ security standards and procedures. Coordinates, develops, and evaluates security programs for an organization; Recommends information assurance/ security solutions to support customers' requirements. Identifies, reports, and resolves security violations. Establishes and satisfies information assurance and security requirements based upon the analysis of user, policy, regulatory, and resource demands. Performs vulnerability/risk analyses of computer systems and applications during all phases of the system development life cycle. Education Masters of Science in Cloud Computing Architecture in Cloud University of Maryland University College May 2021 Bachelors of

Science in Information Systems and Technology Old Dominion University - Norfolk, VA May 2017 Certifications/Licenses Amazon Web Services- Certified Developer Associate CompTIA Security+ CompTIA Network+ EC Council Certified Ethical Hacker EC Council Certified Network Defense Architect ITIL v3 Certified Cisco Network Associate - Routing and Switching Amazon Web Services - Certified Architect Associate

Name: Nina Ford

Email: nicholas00@example.com

Phone: 306.874.0637x26630