Senior Network Security Systems Engineer - Full Time Senior Network Security Systems Engineer - Full Time Senior Network Security Systems Engineer - Full Time - CGI Work Experience Senior Network Security Systems Engineer - Full Time CGI - Fairfax, VA August 2018 to Present Supporting the DHS (Department of Homeland Security) on Continuous Diagnostics and Mitigation Program (CDM) ? Providing assistance with a number of agencies through the 4 phases of the CDM project Working closely with team members to support the needs of these agencies while working with agency stakeholders to meet the requirements set in place Provide Tier 2/3 support for incidents relating to security tools/solutions ? Assisting with the implementation and configuration of security/network tools such as Forescout, CyberArk, SolarWinds, Wireshark and more Have supported on a number of agency specific task to meet the needs of the clients Applying technical expertise in implementing efficiencies to help improve the day to day operations Cyber Security Subject Matter Expert Acclaro Research Solutions, Inc June 2018 to Present - Part Time Providing guidance and recommendations to FEMA's National Training and Education Division (NTED) for their emergency management and homeland security training courses for its Terrorism and Catastrophic Events Preparedness Training Program Evaluating courses varying in the cyber security field Conducting information security risk assessments based on industry standards Working with course developers to further enhance and improve the material Lead Information Assurance Security Officer (IASO) Moss Cape - Fort Belvoir, VA April 2018 to August 2018 - Full Time Supporting client with vulnerability assessments of current and future applications and network tools Providing assurance of network security controls are in place and in current standards of NIST 800-53 Promote security awareness among Federal and non-Federal staff through scheduled training Work closely with Federal employees to ensure current security guidelines on all systems are being held in place Providing technical support when needed to the System Administrator on any escalated security related matters Cyber Security Incident Analyst Northrop Grumman - McLean, VA December 2015 to March 2018 - Full Time Subject Matter Expert

Conducted system security assessments based on NIST 800-53 and ISSO ? Wrote and developed security plans to meet the requirements for the client ? Monitoring access control,

computer security, security awareness and training, incident response and system and communications protection ? Advising the CISO, CIO and ISM on day-to-day security related matters ? Assisting with weekly audits on numerous IT systems and security incidents verifying with the US Cert to meet OMB requirements Data Loss Prevention analyzing using DLP Symantec ? Analyzing all inbound and outbound email traffic to environment by verifying proper methods of encryption are used in accordance to the CIA triad, Confidentiality, integrity and availability ? Incident reporting on any event that is considered to be a loss of SI or PII ? Clearing false positives from queues to ensure of any new events are marked and cleared of any SI or PII Investigating spam emails verifying the source of the email by analyzing the headers ? Raising security awareness by quarterly phishing emails and assisting in the development of PhishMe Conducting malware analysis by identifying and using techniques to investigate and remove from machines and servers ? Investigating and reporting any events that may appear to be an Advanced Persistent Threat (APT) to proper channels and working to conduct the removal and finding the source of the threat Monitoring data in real time using Splunk ? Searching, reporting and investigating security driven events in triage ? Using Splunk to assist in investigations of any potential compromised machines or accounts Using many IPS (Intrusion Prevention System) and IDS (Intrusion Detection System) tools to assist with analyzing and investigating security driven events ? McAfee ePolicy Orchestrator - Monitoring and protecting machines on network ? Bit9 - File monitoring tool Ensuring all cyber related policies are adhered to and that required controls are implemented and facilitated continuous monitoring system Creating/Providing daily/weekly reports to the upper management including the and Chief Information Officer (CIO) and Chief Information Security Offices (CISO) of the FDIC with daily updates of current security related incidents and potential OMB reportable events Technical writer creating and modifying new and existing SOPs for the SOC to meet the client's needs and in compliance of current Federal regulations ? Created Playbooks with step by step handling guidance of different event driven events Assisting in the transition from a 15x5 CSIRT to a 24x7 Extensive Experience as being the Lead Trainer for the CSIRT ? Trained 10+ employees ? Creating/modifying/improving training documentation and

process Continually working with Team Leads and Managers to address and improve CSIRT procedures to help increase productivity and team morale IT Specialist - Full Time American Technology Services - Fairfax, VA May 2013 to December 2014 Served as a network and security support to over 10,000 clients across several hundred companies. Provided 24x7 network support across Tiers I, II, and III while maintaining high levels of customer satisfaction. Maintained servers, hardware, and software on Windows platform including Exchange, Application and Active Directory servers Performed restorative and maintenance tasks either remotely or at the end user's location to resolve problems, using basic troubleshooting and technical skills. Managed and maintained Group Policy, Security Policies, Active Directory, Symantec Backup Exec, Symantec Endpoint, creation and deletion of user accounts, access controls, and domain structure configuration. Troubleshot and resolved user incidents and requests dealing with the Microsoft operating system, Active Directory, Microsoft Office Suite, Blackberry, iPhone, VPN. Provided on-site tech support and remotely to include installation, maintenance and repairs of servers, desktops, laptops, and peripherals. Troubleshot, documented and resolved all technical issues pertaining to MS Windows 2000, XP, 7 and 8; Office 2007, 2010 and 2013; Network Connectivity, and hardware related issues. Education Bachelor of Science degree in Cyber Security George Mason University - Fairfax, VA 2014 Associate of Science degree in Information Technology Northern Virginia Community College - Woodbridge, VA 2012 Skills Dlp (2 years), encryption (2 years), incident response (2 years), Security (5 years), Symantec (3 years), Information Security, Nist, Cyber Security

Name: Janet Hall

Email: deborahhaas@example.com

Phone: (718)988-5773x067