IT Security Consultant IT Security Consultant Cyber Information Assurance Analyst - Northrop Grumman Corporation Perry Hall, MD Work Experience IT Security Consultant CyberBalance, LLC. - Arlington, VA September 2013 to Present Responsibilities - Perform Security Certification & Assessments (C&A) on information systems using the NIST Special Publication 800 series - Develop software functionality and security test procedures for FISMA reporting software - Interpret and analyze functionality and security stakeholder requirements - Manage delegation of tasks to software developers - Perform Quality Assurance (QA) measures to discover, report, and address software issues - Interface directly with project stakeholders via meetings, conference calls, and email to incorporate their feedback into the software - Write official user guide provided to stakeholders and user base - Develop official training material that is provided to the user base - Assist in the preparation and technical writing of proposals Cyber Information Assurance Analyst Northrop Grumman Corporation - Arlington, VA April 2013 to September 2013 ? Perform DIACAP audits on DoD information systems. The audits include using the vulnerability scanners Retina, DISA Gold Disk, Unix SRR, SCAP, WASSP, SECSCN, and Nessus. Vulnerability scans are performed on Red Hat Linux; Microsoft Windows Server 2003 and 2008; Windows XP, Vista, and 7; and Solaris 10 ? Research recently discovered vulnerabilities via cybercom.mil, mitre.org, and nvd.nist.gov ? Publish official Information System Vulnerability Assessments to clients. Reports include: o Explanations of system vulnerabilities o The severity of each vulnerability o Methods of vulnerability remediation and fix information ? Prioritize workflow and multitask to satisfy client C&A deadlines ? Collaborate with the other Vulnerability Management Team members comprised of various government, contractor, and military representatives ? Travel and interface directly with system administrators at client worksites multiple times a week ? Deliver exemplary customer support, as the position is 100% client-facing ? Consult and interpret DCID 6/3, AR 25-2, NIST SP 800-53, and other standards publications Field Service Security Engineer Northrop Grumman Corporation - Kandah?r March 2012 to March 2013 ? Administer HBSS (Host Based Security System) for two systems of over 30 servers each ? Install monthly Information Assurance Vulnerability Alert (IAVA) patches on all servers and workstations, which includes Windows Server

2008, Windows XP, Windows 7, Red Hat Enterprise Linux, CentOS and Solaris ? Execute DIACAP vulnerability scans on all servers and workstations using the security scan tools Eeye Retina, DISA Gold Disk, and DISA UNIX Security Readiness Review (SRR) ? Perform manual security checks, and implement fixes on all virtual and physical servers and workstations using VMware vCenter and the corresponding ESX servers. ? Monitor user account activity ? Assure the availability of the systems by performing maintenance of the systems ? Interface directly with CENTCOM, and government agency representatives on a daily basis ? Maintain regular communications with my Information Assurance team CONUS ? Deliver exemplary customer support, as the position is 100% client-facing ? Consult and interpret DCID 6/3, AR 25-2, NIST SP 800-53, and other standards publications Information Assurance Systems Engineer Northrop Grumman Corporation - Baltimore, MD June 2009 to February 2012 ? Manage security vulnerabilities of multiple computer systems, and systems of systems ? Generate DIACAP vulnerability documentation to provide to internal and external customers, which includes Plan of Action and Milestones (POA&M), System Security Authorization Agreement (SSAA), and Trusted Facilities Manual (TFM) ? Present vulnerability and mediation information to internal customers, external customers, and sub-contractors ? Research and implement security fixes on Windows, Linux, and Solaris operating systems ? Execute DIACAP vulnerability scans on various operating systems using the security scan tools Eeye Retina, DISA Gold Disk, DISA UNIX Security Readiness Review (SRR), SECSCN, WASSP and Nessus ? Supervise Vulnerability Assessment Team (VAT) and Certification Engineer (CE) assessments in the research and development laboratory ? Perform Security Test and Evaluations (ST&Es) at United States military bases around the world ? Consult and interpret DCID 6/3, AR 25-2, NIST SP 800-53, and other standards publications Education Master of Science in Information Technology: Information Assurance University of Maryland University College 2012 to 2015 Bachelor of Science in Physics University of Maryland, Baltimore County (UMBC) - Baltimore, MD Certifications/Licenses CompTIA A+ October 2010 to August 2015 CompTIA Network+ CE August 2012 to August 2015 CompTIA Security+ CE June 2012 to June 2015 CISSP October 2013 to October 2016 ISC2 Certified Information System Security Professional (CISSP) Additional

Information Possess an active TS/SCI clearance with Counter-Intelligence Polygraph issued by the United States Department of Defense.

Name: Emily Davis

Email: denise83@example.net

Phone: 641-680-7742x2009