

Cybersecurity Analyst/Information Systems Security Officer (ISSO) Cybersecurity Analyst/Information Systems Security Officer (ISSO) Cybersecurity Analyst/Information Systems Security Officer (ISSO) - Walter Reed National Military Medical Center Columbia, MD Accomplished IT professional with demonstrated success implementing strategic IT initiatives that improve business functionality with positive impacts on the bottom line. Skilled in Cybersecurity System/Network Administration, Leadership & Mentorship. Technology savvy self-starter, adept at moving into new environments stemming from personal experience to quickly adapt to new technologies. Possesses first-rate communications and collaboration skills to work in concert with diverse groups effectively. Work Experience Cybersecurity Analyst/Information Systems Security Officer (ISSO) Walter Reed National Military Medical Center May 2018 to Present * Provide security oversight for WRNMMC and subordinate commands. Coordinating WRNMMC security measures including analysis, periodic testing, evaluation, verification, accreditation, and review of information system installations. * Cybersecurity lead for WRNMMC's Enterprise network migration of over 15,000 assets, to include the completion, validation and submission of Ports, Protocols & Services (PPS) documentation. * Provide oversight of Plan of Action and Milestone (POA&M) compliance-POA&M management, mitigation statement formulation, interfacing with system administrators to resolve open findings of high and at-risk systems. * Ensure information ownership responsibilities are established for each WRNMMC information system, to include accountability, access approvals, and special handling requirements. * Coordinate security measures to include analysis, periodic testing, evaluation, verification, incident response/incident handler and review of information system installation at the appropriate classification level within the command or organizational network structure. * Provides oversight and compliance reporting for the Information Assurance Vulnerability Management (IAVM) program, to include compliance/vulnerability scans via Assured Compliance Assessment Solution (ACAS). * Develop reporting procedures and ensure security violations and incidents are properly reported to the Cybersecurity Defense Service Provider (CDSP), Navy Cyber Defense Operations Command (NCDOC), and the DOD reporting chain, as required. * Ensure compliance monitoring occurs, and review the results of such monitoring, notifying the AO of

significant, i.e., CAT I findings. * Develop and maintain the necessary technical documentation and standard operating procedures (SOPs). Lead PKI System Administrator/Lead IT Support Administrator Naval Communication Security Material System (NCMS) June 2015 to May 2018 * Performed custom development for Navy PKI systems to provide a secure operating system for NCMS PKI Program of Record (POR), Registration Authority (RA) and Local Registration Authority (LRA) systems including engineering images to support 20 closed network assets throughout five detachments with four different hardware platforms in service. * Conducted ACAS vulnerability/compliance scanning and performed patch management ensuring standardization to meet or exceed DISA's secure host baseline requirements across the Navy's closed PKI enterprise, to include the distribution of all software and hardware to NCMS detachments. * Planned and implemented the upgrade of four nationwide sites, from Windows 7 and Windows 10. Developed DISA and Navy Marine Corps Intranet (NMCI) compliant images for four asset models across two enclaves. * Trained and managed System Administrators to provide efforts across the enterprise to maintain a high level of system efficiency and security. Supported the NCMS IT Support Team with ongoing training to include system and network troubleshooting as applied to NCMS and associated NMCI networks. Lead System Administrator/Information System Security Officer USS Makin Island (LHD8) February 2012 to June 2015 * Maintained and administered 18 Windows/Redhat Linux servers, 40 Alcatel switches, two Cisco routers and 650 workstations supporting the mission of 1300 customers. * Responsible for conducting weekly Information Assurance inspections and reporting discrepancies to military leadership. * Managed two 600-gigabyte (GB) share drives, to include the permission settings of user accounts across 100 security groups. * Planned and executed a Host Based Security System (HBSS) hardening project, tailored to exceed DISA's baseline, providing a higher level of security and security-based reporting while ensuring customer quality remained unaffected. * Conducted scheduled software and hardware maintenance on all network and endpoint devices. Naval Information System Technician US Navy April 2011 to February 2012 Developed a strong working knowledge on topics such as A+, Security+, Cisco routers, network switches, Windows/Unix operating systems and Naval communications/telecommunication to

include satellite communication systems. Education Business Management Howard Community College - Columbia, MD 2006 to 2009

Name: Michelle Young

Email: maxwellkristen@example.com

Phone: (471)338-9537