Information Assurance Lead Information Assurance Lead Information Assurance Lead - Perius. Inc Accokeek, MD Over 15 years of analyzing information security environments while implementing strategic solutions to reduce risk and improve processes in all phases of system and software development. Technical background is complemented by strength in project management and project team development. Currently working as an Information Assurance Lead for the Department of Navy (DON) at Military Sealift Command (MSC). Years of experience managing the Certification & Accreditation (C&A) process has played an integral part developing an information security team to meet DON robust security requirements. Currently holds a Top Secret Clearance, DoD 8570 Information Assurance Technician III (IAT III), working on Information Assurance Management III (IAM via GSLC). I previously worked for Department of Transportation National Highway Traffic Safety Administration (NHTSA) as the Security Operations Manager. Providing support to NHTSA s security program areas of Policy & Standards and Engineering to include security compliance, enforcement, systems engineering, technical and analytical support. Items of primary focus is risk management, technical enforcement, monitoring, problem resolution, continuous monitoring, vulnerability testing and remediation, reporting, configuration management, security monitoring and research and analysis. Work Experience Information Assurance Lead Perius. Inc - Washington, DC February 2009 to Present Responsible for providing oversight and monitoring to the Department of Navy Information Assurance program. Develop and maintain strong business and technology relationships as a liaison between MSC, DISA, DON and CYBERCOM. Partner with DOD and MSC to ensure program consistency, develop information security risk strategies, implement action plans, and recommend policy and procedural changes for risk avoidance and mitigation. Using Security Technical Implementation Guides (STIGs) and Secure Configuration Compliance Validation Initiative (SCCVI) guidance provided subject matter expertise, guidance and direction to MSC information assurance policy, standards, controls, and IT Risk programs. Conducted security assessments via manual and automated DoD provided tools, such as ACAS, DISA GoldDisk, and Retina. Created and maintained a continuous high level of system security through the Information Assurance Vulnerability Management (IAVM) process and use of the Vulnerability Management

System (VMS). Responsible for providing oversight, monitoring, and reporting compliance of DON MSC ePo environment through compliance with DON Communications Tasking Order (CTO's). Provided Certification and Accreditation (C&A) support for MSC, to including web-based systems, distributed systems, and legacy systems, using Department of Defense (DoD) Information Assurance Certification and Accreditation Process (DIACAP) guidelines. Developed necessary C&A documentation and assisted through coordinated data calls with System Owners and Data Stewards. Performed remediation activities by providing leadership with recommendations for and implement the closure of Plan of Action and Milestones (POAM) items. Coordinated vulnerabilities with the C&A team to support required activities of Annual Security Reviews (ASR). Perform vulnerability scans, assessment, and analysis for all the department of Navy operational systems and validate scan results to mitigate and reduce the risks. Responsible for writing POAM and perform audits to support Certification and Accreditation (C&A) packages. Write Standard Operating Procedures (SOPs) for Information Assurance related processes and procedures. Evaluate the security posture of computer/network information systems against all Department of Navy (DoN) regulations and best standard practices. Update certification and accreditation documentation as needed for all network packages. Develop technical and programmatic procedures for security assessments. manages McAfee ePo application on multiple network operations and coordinate with DISA to maintain situation awareness of changes to policy, waivers and exceptions at all DoD ePo Tiers in MSC. security mandates. Perform research and make recommendations on cyber security best practices, new technologies, and protection capabilities Assist in security audits and assessments Review and manage testing activities related to disaster recovery and COOP plansTrain and assist users with the use of the internal risk management tool and security tools used at the department level Produce professional presentations and conduct presentations at an executive level Provide support to annual security training for users and administrators Secuirty Operations Manager VersaTech - Washington, DC October 2016 to October 2017 Interpret and enforce National Institute of Standards and Technology (NIST), Federal Information Processing Standard (FIPS), Identity, Credential and Access Management (ICAM),

Federal Information Security Management Act (FISMA), and department compliance throughout the information technology (IT) environment. Provide the Director of Security senior-level advisory on solutions best to meet CIO's requirements for meeting all security mandates while meeting the business mission. Perform and manage vulnerability scans and the remediation of all negative results. Assist project managers with updating security plans for IT investments. Provide assistance for the review and development of recommendations for security policies, guidelines and procedures. Assist with the development and review of risk assessments and risk management plans in support of continuous monitoring (C&A) activities. Provide data calls for Office of Management and Budget (OMB) exhibits, IT Vital Dashboard, and FISMA. Produce and maintain documentation as it relates to the client's security program. Produce professional presentations and conduct presentations at an executive level. Manage the internal risk assessment tool CSAM Engineer and administer all toolsets that are used to monitor, assess, and protect the client's networking environment (IBM BigFix, Lieberman password, Symantec Data Loss Prevention (DLP) Varonis) Manage the process of conducting password resets for all agency networking devices. Utilize toolsets to identify malware and spyware that has possibly penetrated the network. Work with the department's enterprise security team, DHS and FBI to identify, escalate, diagnose and resolve security related incidents. IT Security Analyst Center for Internet Security Benchmark Tool (CIS) - Upper Marlboro, MD January 2008 to February 2009 Provide technical solutions to Engineers and Administrators on a Linux and Windows platform to assist with design projects to help them meet the necessary 1/2008 - 2/09 Upper Marlboro, MD NIT. IT Security Analyst Responsible for projects conducting IT Security Assessment for government and private sector clients. Responsible for conducting vulnerability assessments using a wide rand of security tools including Nessus, Retina, ACAS, App Detective, Air Defense, Center for Internet Security Benchmark Tool (CIS), Microsoft Baseline Security Analyzer (MBSA), and Web Inspect. Responsible for developing IT security Assessment reports and documentation in accordance with NIST, ISO2700, PCI, HIPPA, and DoD guidelines. Responsible for evaluating and upgrading IT Security Policies, Procedures, and Practices for private and government systems. Responsible for

all NIT corporate IT security activities including Security Audits, Risk Assessments, and Contingency Planning. Responsible for developing and maintaining corporate IT Security policies and procedures. Responsible for conducting annual security assessments using Nessus vulnerability assessment tool. Responsible for developing and implementing the System Security Plan, Security Awareness Training Plan, and Incident Response Plan. Responsible for Security Assessments based on NIST 800-53, 800-59, 800-60, 800-37, 800-53, and 800-53A guidelines. Responsible for creating ST&E packages, POAM's, based on NIST controls: Access Control, Awareness and Training, Audit and Accountability, Certification , Accreditation and Security Assessments, Configuration Management, Contingency Planning, Identification and Authentication, Incidence Response, Maintenance, Media Protection, Physical and Environmental Protection, Planning, Personal Security, Risk Assessment, System and Services Acquisition, System Communication, and System and Information integrity. Project Manager University of Maryland - College Park, MD July 2006 to January 2008 Responsible for project development, resource scheduling, planning and administration of multiple off site networks, monitoring of network systems requirements, priorities and coordination with Department of Human Resources. Managed 5 Network Engineers located at different locations. Responsible for managing crisis situations involving complex and technical hardware or software problems, mentoring and training new network engineers and support staff, obtaining competitive prices from vendors, scheduling upgrades and security backups of hardware and software systems, planning, developing and implementing upgrades as the budget allowed, researching and installing new systems keeping up to date with the latest technologies. Designed, implemented, and monitored Windows 2003 servers with Active Directory. Configured, Implemented, and maintained a DNS forwarding, and Microsoft WSUS server. Support VPN connections through a Cisco Checkpoint VPN client. Monitored and maintained a local area network for over 500 users. Work with layer 2 switches to monitor LAN activity. Monitored and maintained a local area network for 500 users using Windows XP. Configured, administrated, and set up new users computers. Installed, upgraded, and maintained software hardware as needed. Created, maintained, and updated laptops and desktops

images with ghost. Education Master of Science in Information Technology in Information Technology University of Maryland University College Certificate in Project Management University of Maryland University College BS degree in Computer Engineering Clemson University Skills Cyber Security, Information Security, Nist, Network Security, Siem Certifications/Licenses Project Management Professional (PMP) Driver's License Additional Information Over 15 years of analyzing information security environments while implementing strategic solutions to reduce risk and improve processes in all phases of system and software development. Technical background is complemented by strength in project management and project team development. Currently working as an Information Assurance Lead for the Department of Navy (DON) at Military Sealift Command (MSC). Years of experience managing the Certification & Accreditation (C&A) process has played an integral part developing an information security team to meet DON robust security requirements. Currently holds a Top Secret Clearance, DoD 8570 Information Assurance Technician III (IAT III), working on Information Assurance Management III (IAM via GSLC). I previously worked for Department of Transportation National Highway Traffic Safety Administration (NHTSA) as the Security Operations Manager. Providing support to NHTSA's security program areas of Policy & Standards and Engineering to include security compliance, enforcement, systems engineering, technical and analytical support. Items of primary focus is risk management, technical enforcement, monitoring, problem resolution, continuous monitoring, vulnerability testing and remediation, reporting, configuration management, security monitoring and research and analysis.

Name: Max Wilson

Email: katiewells@example.org

Phone: 369-311-8085x761