Information Security Manager Information Security Manager Information Security Manager, CISA, CISM, CISSP Savannah, GA 8 years of active duty military services including Operation Enduring Freedom in Afghanistan 10+ years of combined Information Technology Experience consisting of systems and network administration, IT security, and application development 9 years of IT security experience with over 6 years of experience in security assessments 8 years of leadership and management experience as a US Army Officer (Rank of Captain) CCNA, CISA, CISM, CISSP Familiar with COBIT, ISO 27001, SOX (302 & 404), SSAE 16 (SOC1), AT 101 (SOC2), PCI-DSS Security Clearance: SECRET (TOP SECRET Clearable) Active ISC2 and ISACA member Excellent verbal and written communicator, a proven motivating leader Specializes in IT Security, but well-versed in Systems administration (Virtualization), Application development, Networking, and Database administration Work Experience Information Security Manager US Army - Fort Stewart, GA July 2007 to Present Serves as the chief information (Cyber) security advisor (CISO equivalent) to senior executive management. Responsible for overseeing the enterprise's information security operations which entailed, full-spectrum, defense-in-depth management of the organization's information networks, systems, devices, and services all while complying with DoD standards and guidelines. Plans and participates in the military decision making process with the organization's senior leadership for all the military operations and exercises as the cyber security Subject Matter Expert. Plans, organizes, and manages staff & projects to ensure the high availability of enterprise IT infrastructure and related services to support the organization's business objectives (war fighting functions). This includes key areas such as: network infrastructure, server and storage infrastructure, data communications, and telecommunications systems. Developed an enterprise level incident response plan in accordance with DoD information security policies and handled over 300 security incidents ranging from security policy violations, malware, cross domain violations, and classified spillage incidents. Also implemented a unique internal security application and protection mechanism that resulted in 80% reduction in security-related incidents and classified information spillages. Leads assessment teams in the conduct of numerous internal and external comprehensive vulnerability and security assessments as well as the conduct of internal and external IT and IT security compliance audits. Developed, implemented, and manages an enterprise information security program ensured the confidentiality, integrity, and availability of over 4000 general users, privileged users, foreign national users, and over 2000 information systems across three separate classifications of DoD information networks (Unclassified, Coalition CENTRIX, and SECRET). The program addressed logical and physical access control, physical and personnel security, systems security, network security (to include wireless security), general and privileged user awareness and certification training, incident response, BCP/DRP, PKI, and management of classified systems (configuration, labeling, storage, and disposal procedures). Designed, implemented, and administered virtualized enterprise servers architecture with VMware ESX, NETAPP storage area network and provided high availability services such as Active directory, Exchange, SharePoint, databases, and various US Army Mission Command services for war-fighting, with integrated identity management access controls mechanisms aligned with enterprise security policies. Designed and implemented an enterprise vulnerability management solution using Tenable SecurityCenter with NESSUS vulnerability scanner and Passive vulnerability scanner (PVS), as well as managing the scanning and patching of over 2000 systems. Information Security Manager in Afghanistan (Operation Enduring Freedom): 1. Served as the Information Security Manager for US Forces Afghanistan (USFOR-A) in Regional Command East (RC-E), responsible for the overall information security of multiple forward operating bases and combat outposts consisting of four separate classifications of network (US Unclassified, US SECRET, US TOP SECRET, and Coalition CENTRIX-ISAF) which supported over 10,000 users (DoD uniformed service personnel, DoD Civilian, DoD Contrators, Coalition forces partners, and Afghan national personnel). Led a team of over 20 information security personnel composed of DoD military enlisted personnel and officers, DoD Civilians, and DoD contractors. 2. Led security teams and conducted numerous internal and external vulnerability and security assessments for US military units and Afghan National Army units across RC-E. These assessments included: a. Physical security assessments: gates, security checkpoints, military command posts, key IT facilities, and classified areas using social engineering tactics such as telephony, phishing/spear phishing, dumpster diving, fake badges, camera evasion, and lock picking, etc. b. Systems and network security assessments: malware, default systems and networking devices passwords, vulnerability scanning, known systems vulnerability exploitations, network packet captures, wardriving, rogue wireless devices, firewall and IDS evasions, network stress tests. c. Personnel and application security: general and privileged user accounts compromise, web applications security (SQL injection, access escalation, traversal attacks), and verification to determine if different levels of users have proper permission levels. d. Operations security: assessed current operations workflows, policies and procedures, IT operations, security operations for potential security weaknesses and vulnerabilities, performed risk and mission impact analysis (similar to a BIA), and provided recommendations. As the team lead, also prepared: Assessment in-brief, Assessment out-brief (with summary), recommendation reports, and follow-up assessments for senior unit personnel for all units assessed.   3. Implemented and managed Blue Coat ProxySG and WebFilter on DoD Unclassified network in order to enforce command security policies in web content filtering, bandwidth management, and data loss prevention.   4. Implemented and managed enterprise DoD Host Based Security System (HBSS), the DoD version of McAfee ePO and end point security suite. The implementation included a centralized ePO server, client Asset Configuration and Compliance Module (ACCM), Antivirus/Antisypware (AV/AS), Device Control Module (DCM), HIPS, Rogue System Detection, and Policy Auditor (PA) to enforce USFOR-A command cyber security policies (to minimize data loss, intrusion, and spillage of classified information).   5. Managed various large-scale IT security projects to include implementation of specialized persistent threat detection and analysis tools (which provided installation security from foreign hostile forces and insurgents), and physical security device installations across multiple command posts. 6. Assisted local allies - (Afghan National Army (ANA)) as the IT security advisor and performed comprehensive security assessments (physical, technical, and procedural) for their IT operations and identified associated risks, thereby recommending to ANA leadership the best and most relevant practices and solutions.

Active speaker in US Army Signal Leaders Forum, LandWarNet conferences, and other IT security conferences to share security best practices, and lessons learned from complex scenarios supporting tactical military missions. IT Security Analyst U.S. Bankruptcy Court - Central District of California, CA June 2005 to July 2007 Implemented the court's network and systems configuration management plan that ensured all systems were configured to a standardized baseline, and all changes to the configurations were controlled and documented. Provided advisory and technical support for the court staff and Security Management staff on all information security matters Assisted in security vulnerability assessments in the court's network, implemented Intrusion Detection Systems per Administrative Office's guidelines, and recommended security policies to better protect the court's network. Education BS in Computer Science University of California - Riverside, CA 2007 Certifications/Licenses CCNA CISM CISA CISSP Additional Information COMPUTING SKILLS Programming & Scripting: C/C++/C#, JAVA, Python, PHP, Ruby, Powershell, Bash shell Systems & Infrastructure Administration: VMware ESXi, Vsphere Client, Vcenter Server, Unix, Windows Server 2008R2, WSUS & SCCM, NetApp Storage Appliances Networking and Security: Cisco routers and Switches, Adaptive Security Appliance (ASA) 5500 series, SNORT, McAfee ePO, NESSUS, NMAP, Wire Shark, Kali/Backtrack, Metasploit/Meterpreter, Flying Squirrel, Kismet, Aircrack-ng

Name: Jennifer Roberts

Email: betty90@example.org

Phone: 747-406-4199x130