INFORMATION SYSTEM SECURITY MANAGER INFORMATION SYSTEM SECURITY MANAGER Lake Elsinore, CA 24-years Naval-Leader & Manager - experience in operations and operation management. Dynamic professional bringing over 15-years of Cyber and Information Security analyst/engineer/manager, Database software development, hardware and software installation, and troubleshooting of production servers, desktops and encrypted laptops for the federal government (Navy). Highly talented at resolving complex technical issues efficiently with root cause analysis. A personable team player offering advanced technical knowledge and a can-do attitude. Proactive and focused on cultivating positive and productive relationships for both internal and external clients with excellent customer service and support abilities. Active Top Secret clearance, SSBI Date: Aug 2018 Authorized to work in the US for any employer Work Experience INFORMATION SYSTEM SECURITY MANAGER NSWC Corona - Norco, CA October 2017 to July 2019 Develop and maintain a formal IS security program, policies, and oversee operational information systems security implementation policy and guidelines. Compose, edit and maintain technical documentation and policy portfolio including System Security Plans (SSP), Security Control Traceability Matrix (SCTM), Risk Assessment Report (RAR), SOPs, POA&M, site security plan, incident response plan, continuous monitoring plan (CONMON), and configuration management. Maintain a repository of all organizational or system-level cybersecurity-related documentation (including ATOs) for IS under their purview; Assess changes to the system, its environment, and operational needs that could affect the security authorization. Coordinate with PSO/CPSO or cognizant security official on approval of external information systems (e.g., guest systems, interconnected system with another organization). Ensure ISSOs under their purview are appointed in writing and provide oversight to ensure they follow established IS policies and procedures; ensure they receive the necessary technical and security training (e.g., operating system, networking, security management) to carry out their duties. Ensure System Administrators (SA) monitor all available resources that provide warnings of system vulnerabilities or ongoing attacks; Ensure proper measures are taken when an IS incident or vulnerability is discovered. Ensure a record is maintained of all security-related vulnerabilities and ensure serious or unresolved violations or vulnerabilities are reported to the AO/DAO. Ensure approved procedures are used for sanitizing and releasing system components and media. Coordinate IS security inspections, tests, and reviews. Ensure data ownership and responsibilities are established for each IS, and specific requirements (to include accountability, access and special handling requirements) are enforced. Ensure development and implementation of an effective IS security education, training, and awareness program. Maintain a working knowledge of system functions, security policies, technical security safeguards, and operational security measures. CYBER SECURITY ENGINEER ITELLISOLUTIONS INC - San Diego, CA May 2017 to October 2017 Serve as an Assessment and Authorization (A&A) Subject Matter Expert (SME) and apply knowledge of Risk Management Framework (RMF) to validate authorization packages for submission to the Authorizing Official. Compose, edit and maintain technical documentation and policy portfolio including System Security Plans (SSP), SOPs, POA&M, site security plan, incident response plan, continuous monitoring plan, and configuration management. Responsible for evaluating the organization's IT policies, standards and procedures, and the processes for their development, approval, release/publishing, implementation and maintenance to determine whether they support the IT strategy and comply with regulatory and legal requirements. Responsible for evaluating risk management practices to determine whether the organization's IT-related risk is identified, assessed, monitored, reported and managed. Continuous management and oversight for system hardening and STIG compliance requiring close communication with engineers, administrators, vendors and government personnel. Perform security information and event management through audit log collection and analysis using InTrust Events Manager and Windows event viewer. Planned, organized and conducted technical and non-technical inspections. Prepared reports and recommended improved methods and procedures. Researched and interpreted military security regulations. Employ technical knowledge and analysis when performing vulnerability assessments, leveraging ACAS tools and provide implementation guidance on the way forward regarding vulnerabilities, including the development of IAVA and STIG Plan of Action and Milestones (POA&Ms) and Mitigations. SENIOR CYBER SECURITY ENGINEER NEXAGEN NETWORKS INC - San Diego, CA March 2017 to May

2017 Employ technical knowledge and analysis when performing vulnerability assessments, leveraging ACAS tools and provide implementation guidance on the way forward regarding vulnerabilities, including the development of IAVA and STIG Plan of Action and Milestones (POA&Ms) and Mitigations. Serve as an Assessment and Authorization (A&A) Subject Matter Expert (SME) and apply knowledge of DIACAP or Risk Management Framework (RMF). Perform ongoing A&A activities in support of the program by developing and maintaining A&A packages using the Enterprise Mission Assurance Support Service (eMASS). Provide Security Test and Evaluation (ST&E) operational support services, to generate the related DoD Information Assurance Certification and Accreditation Process, Risk Management Framework (DIACAP/RMF) documentation. Evaluates a wide array of IT devices for Security Technical Implementation Guide (STIG) compliance using ACAS/ Nessus, SCAP Compliance Checker, and manual checklist reviews. This includes Windows and Linux servers and desktops, routers, switches, firewalls, IDS, etc. Provide support in NIST, DoD RMF and DIACAP by oversight of the implementation of processes and distribute information, standards and requirements consistent with NIST, DIACAP, and ICD 503 policies. CYBER SECURITY ANALYST Engility - San Diego, CA January 2015 to February 2017 Successfully led the effort to complete the Command Cyber Readiness Inspection (CCRI) for the company's local SIPR enclave achieving an excellence (88.9%) in their compliance review, the highest score received to date for ENGILITY. Responsible for employing security tools, technologies, best practices, and the deployment of solutions protecting multiple classification systems and information assets. Managed, configured and maintained compliance of Host Base Security System (HBSS) through the McAfee ePolicy Orchestrator (ePO) portal which included client deployment, signature updates and incident response and analysis. Installed, implemented and manage SourceFire IDS system and Tenable ACAS vulnerability and compliance scanning systems.

Compose, edit and maintain technical documentation and policy portfolio including System Security Plans (SSP), SOPs, POA&M, site security plan, incident response plan, continuous monitoring plan, and configuration management. Responsible for evaluating the organization's IT policies, standards and procedures, and the processes for their development, approval, release/publishing, implementation and maintenance to determine whether they support the IT strategy and comply with regulatory and legal requirements.   Responsible for evaluating risk management practices to determine whether the organization's IT-related risk is identified, assessed, monitored, reported and managed.   Continuous management and oversight for system hardening and STIG compliance requiring close communication with engineers, administrators, vendors and government personnel.   Perform security information and event management through audit log collection and analysis using InTrust Events Manager and Windows event viewer.   Planned, organized and conducted technical and non-technical inspections.   Prepared reports and recommended improved methods and procedures.   Researched and interpreted military security regulations.   Instrumental in successfully completing the transition to RMF and achieving Authority to Operate for government program office SWAN.   Responsible for the design, development, documentation, security, and maintenance of 21 databases located on 3 separate classified and unclassified networks that comprise of Financial Budgeting and Management, Contract Management, Risk Management, Security and Document Control, Program Management, and Personnel Management.   SQL Server Database manager, responsible for the maintenance and management of the program office databases.   Responsible for the maintenance, security, upkeep, supervision, and customer technical support for 140 NMCI and 95 SIPR computer network assets and support equipment to include printers, scanners, mutli-function devices.   SIPRnet Trusted Agent responsible for the user authentication process of acquiring a SIPR PKI token. DATABASE ARCHITECT / ISSO / IT SERVICE MANAGER TASC - San Diego, CA 2010 to February 2015   Responsible for employing security tools, technologies, best practices, and the deployment of solutions protecting multiple classification systems and information assets.   Ensuring systems are operated, maintained, and disposed of in accordance with internal security policies and practices as outlined in the accreditation/certification support documentation package.   Continuous management and oversight for system hardening and STIG compliance requiring close communication with engineers, administrators, vendors and government personnel.   Compose, edit and maintain technical documentation and policy portfolio including System Security Plans (SSP), SOPs, POA&M, site security plan, incident response plan, continuous monitoring plan, and configuration management. Perform security information and event management through audit log collection and analysis using InTrust Events Manager. Initiating protective and corrective measures when a security incident or vulnerability is discovered, with the approval of the ISSM. Conducting periodic reviews to ensure compliance with the accreditation/certification support documentation package. Ensuring Configuration Management (CM) for IS software and hardware, to include IS warning banners, is maintained and documented. Planned, organized and conducted technical and non-technical inspections. Prepared reports and recommended improved methods and procedures. Researched and interpreted military security regulations. Responsible for the design, development, documentation, security, and maintenance of 5 financial databases located on 3 separate networks that manage a combined 500 million dollar annual budget. Responsible for the design, development, documentation, security, and maintenance of 2 Contract Databases located on 2 separate networks that manage 1.1 billion dollars in contract obligations. Responsible for the design, development, documentation, security, and maintenance of 14 program management databases located on 3 separate networks that comprise of Risk Management, Security/Document Control, Program Management, Personnel and Training management. SQL Server Database manager, responsible for the maintenance and management of the program office databases. Responsible for the design, development, documentation, and maintenance 2 Security/Document control databases for Engility CPSO and FSO. Responsible for the maintenance, security, upkeep, supervision, and customer technical support for 125 NMCI and 50 classified computer network assets and support equipment to include printers, scanners, multi-function devices. SIPRnet Trusted Agent responsible for the user authentication process of acquiring a SIPR PKI token. DATABASE ARCHITECT / IT SERVICE MANAGER Northrop Grumman - San Diego, CA 2006 to 2010 Responsible for the design, development, documentation, security, and maintenance of 8 Financial, 2 Risk Management, 1 End of Life, and 1 Security/Document Control databases for program office. Responsible for the design, development, documentation, security, and maintenance of 3 Security/Document Control databases for Northrop Grumman. SQL Server

Database manager, responsible for the maintenance and management of the program office databases. Program office IT Service Manager responsible for the maintenance, security, upkeep, supervision, and customer technical support for 65 NMCI and 5 classified computer network assets and support equipment to include printers, scanners, multi-function devices. Manager / Senior Instructor / Facilities Manager / Safety Officer U.S. Navy - San Diego, CA 2003 to 2006 Database Manager and Designer / ADP Manager Location: U.S. Navy Fleet Anti-Submarine Warfare Training Center / Center for Surface Combat Systems, San Diego CA Managed the $350,000 command maintenance budget. Responsible for the maintenance and upkeep of 9 buildings in 2 locations. Military representative and project manager for a 5 million-dollar 10 month building and classroom renovation project. Created and maintained commands student database to track more than 10,000 students annually, a personnel database to track professional qualifications and career goals of more than 300 instructors, and a Facilities database to track maintenance of individual buildings and for budget tracking. NMCI Assistant Contract Technical Representative (ACTR) responsible for the maintenance, upkeep and supervision of 144 NMCI computer network assets. Implemented Electronic Safety and Management Systems (ESAMS), which automated training and mishap reporting and tracking. Managed the operational and training schedule for 23 military and 3 civilian contractor instructors. Oversees development and training of C4I courses ranging for Tactical Data Systems, ACDS, GCCS (M), TDC Link 11, Link 16 and TBMCS. Operations Center Management Senior Manager US Navy 1982 to 2006 with: Retired with numerous CONUS, OCONUS and at-sea assignments Operations Center Management Senior Manager Talents and Skills in ? Qualified Trainer ? Management and Supervisor * Large number of People, processes and procedures * High valued resources * High level of responsibility * Cost effective readiness * High valued mission assurance and readiness ? Demonstrative ability to overcome challenges ? High valued resource and assets ? Leadership Responsible Manager / Trainer / Senior Enlisted Advisor COMPHIBRON SEVEN - San Diego, CA 2000 to 2003 Managed and supervised 4 Chief Petty Officer and 15 staff personnel in 5 different ratings. Managed the planning and execution of all command operational commitments. Designed professional MS PowerPoint and MS Excel presentations for flag level briefings. Authored a 52 line item Job Qualification Requirement for Enlisted Watch Stander - Tactical Flag Command Center. Operations Department Head / Training Liaison Officer Afloat Training Group Middle Pacific - Pearl Harbor, HI 1998 to 2000 Managed and supervised 6 personnel in Operations Department. Responsible for briefing, debriefing and tailoring tactical training for U.S. Navy Ships and Coast Guard Cutters. Personally supervised over 200 ATG MIDPAC shipboard training team members during ships' Basic Phase Training. Operation Department Leading Chief Petty Officer USS LEFTWICH (DD-984) - Pearl Harbor, HI 1996 to 1998 Managed and supervised a department of 105 personnel. Trained junior officers and senior enlisted personnel in the procedures, and tactics of the Command, Control, Computers, Communications and Intelligence (C4I) system. Combat System Training Team Leader. Managed and trained Combat System Training Team. Mentored and directed the successful completion of Naval Gunfire Support System (NGFS) Qualification and all phases of graded Anti-Submarine Warfare Team training events. 1992-1996 > Leading Chief Petty Officer OI Division Location: USS LAKE ERIE (CG 70) - Pearl Harbor, HI Managed and supervised a division of 45 personnel. Trained junior officers and senior enlisted personnel in the procedures, and tactics of the Command, Control, Computers, Communications and Intelligence (C4I) system. Member of Combat System Training and the Damage Control Training Teams. Mentored and directed the successful completion of Cruise Missile Qualification Test and all phases of graded Anti-Submarine Warfare Team training events. Member of the SM2 Block 4 VLS certification team Lead Instructor AEGIS 1989 to 1992 Officer and Operator Training Location: AEGIS Training Unit, Wallops Island VA. Managed and supervised a division of 12 instructors. Stood up the AEGIS Baseline 4 Operator and Officer courses. Volunteer Fireman for Wallops Island community and NASA Flight facility. Member of Combat System Training Team USS ANTIETAM (CG-54) - Long Beach, CA 1986 to 1989 Long Beach, CA. Managed and supervised a division of 45 personnel. Trained junior officers and senior enlisted personnel in the procedures, and tactics of the Command, Control, Computers, Communications and Intelligence (C4I) system. Member of Combat System Training Team. Mentored and directed the successful completion of Cruise Missile Qualification Test and all phases of graded Anti-Submarine Warfare Team training events.   Member of the Test and Evaluation of the CG AEGIS VLS certification process, supervisor the data collection and secure shipment of the material collected for evaluation. Education Advanced Master Certificate in Cyber Security in Cyber Security Villanova University December 2014 to July 2015 Masters Certificate in IT Service Management Villanova University October 2014 to May 2015 Masters Certificate in Information Security Management Villanova University October 2014 to March 2015 Masters Certificate in Information Systems Security Villanova University October 2014 to March 2015 Associates of Science Degree in Applied Computer Science Penn Foster College - Scottsdale, AZ March 2005 to March 2007 Skills Microsoft Office (10+ years), Windows 10 (10+ years), Windows 7 (10+ years), Microsoft Server 2008R2 / 2012R2 / 2016 (10+ years), SQL (10+ years), SCAP, STIG, Digital Certificates; Anti-Virus Tools (Symantec, McAfee, Windows Defender, etc.), Host Based System Security (HBSS), Assured Compliance Assessment Solution (ACAS), Nessus (10+ years), Risk Management Framework (RMF), NIST, CNSSI, JSIG, NISPOM, JAFANs, DCID, and DOD 5205.07 (10+ years), Patch Management/Remediation, (10+ years), vulnerability assessment tools (10+ years), Cyber Security, Information Security, Siem, Nist, Network Security Military Service Branch: United States Navy Rank: E-8 Certifications/Licenses Certified Information Systems Security Professional (CISSP) 2015 Certified Information Systems Auditor (CISA) August 2016 CompTIA Security+ December 2014 CCNA Security October 2016 CCENT October 2016 NSTISSI 4011 Information Systems Security (INFOSEC) Profession October 2016

Name: Sharon Tapia

Email: rjones@example.com

Phone: 357.372.1545x05410