RMF Analyst, Defense Health Agency RMF Analyst, Defense Health Agency RMF Analyst, Defense Health Agency - Sentar Inc Dexter, GA Work Experience RMF Analyst, Defense Health Agency Sentar Inc - Huntsville, AL March 2019 to Present Huntsville, AL, Supervisor: Edward Escobedo Supervisor Phone: 858-225-9055 To Contact: NO Hours Per Week: 40 Support the Defense Health Agency (DHA) program throughout the DoD with efforts to manage cyber risk and protect medical devices and enclaves. Responsible for the development of Risk Management Framework (RMF) packages for DHA components and vendor developed systems. Provide subject matter expertise to Medical Logistics (MedLOG) clients concerning NIST and DoD publications in respect to RMF. Highly skilled in the use of eMASS, STIGS and other tools utilized to assist in the mitigation and cybersecurity risk posture of devices or systems. Perform Life Cycle activities Maintain day-to-day security posture maintenance support Maintain security enclaves within NIST 800-53 standards Develop and Maintain DHA Plan of Action and Milestones (POAM) Develop working relationship with vendor support staff (engineers, developers, procurement) Work to identify and mitigate potential logical/physical security weaknesses Maintain the site POAM, SOP, SSP, and RAR in support of the Risk Management Framework (RMF) directives Servers as Chief South East Regional Network Enterprise Center - Hinesville, GA October 2015 to Present Grade: GS-14 Series: 2210 Hinesville, GA Supervisor: Stephen Giza Supervisor Phone: 912-435-1876 Ok To Contact: Yes Hours Per Week: 50 Servers as Chief, Cyber Security Division, South East Regional Network Enterprise Center (SE RNEC), FT Stewart, GA. Responsible for all Information Assurance and Computer Security functions for the entire (SE RNEC) community to include, COMSEC, Information Management, Information Assurance Vulnerability Management (IAVA), RMF, DIACAP & DAIG compliance, US Army, DISA, and DOD Information Assurance compliance. EXECUTIVE LEADERSHIP: Leads and provides guidance to a combined workforce of 27 Information Technology Specialists (Federal) in the delivery of IT Services that are reliable, secure, and flexible to facilitate mission accomplishment. Transformed division into a high performing organization that routinely outperforms other regions in the execution of agency initiatives and directives. ? Chaired multiple working groups during this period in order to progress current security posture such as the patch

management, incident response, SIPRNet vulnerability, and other working groups. ? Appointed as a Security Control Assessor-Validator by NETCOM to review/validate RMF ICAN packages for the theater. ? Lead the Cyber Command Readiness Inspection (CCRI) for the Southeast Region (FT. Stewart, FT. Benning & FT. Jackson) to a successful rating in 2017. The inspection scope involved both Cyber, Personnel and Physical security for the entire region for both SIPRNET and NIPRNET enclaves. STRATEGIC PLANNING: Uses a continuing process of improvement philosophy to evaluate operations from a "People, Processes, and Systems" approach. Continues to be a voice for increased standardization and inter-departmental collaboration that includes participation from all levels of the organization. Volunteers to lead enterprise initiatives that facilitate the successful execution of the agency's strategic goals and objectives. ? Worked with multiple technical experts within 93rd Signal Brigade, 7th Signal Command, NETCOM, 2RCC and ARCYBER to improve the patch management process. Changed the target total number of local systems from 15,000 to 55,000 systems within the South East Region. ? Developed a training program thru the use of MS4X funds to improve regional education standards and overall education level of Cyber policies and processes such as vulnerability management, 8570 compliance and other Cyber security issues. FINANCIAL MANAGEMENT: Performs analysis on invoices and generates reports on program and budget execution. Reviews and approves contractor related overtime and travel requests to ensure expenditures are necessary for mission accomplishment. Maintains detailed accounting records for audit purposes. ? Manages funding for the South East Regional MS4X program (Baseline & Computing Environment Training) ? Assisted Branch Chief's in the development of Cyber Security acquisition packages for submission to higher headquarters OPERATIONS MANAGEMENT: Oversees service delivery and service support operations of patch management and vulnerability analysis to ~ 28800 customers in a region that consists of 1 Regional Network Enterprise Center (R-NEC) 3 Local NECs and 4 ADCON Installations. Earned the trust and respect of senior leadership by consistently meeting operational objectives on time and with minimal impact to business operations. Leads Business Process Reengineering efforts that increase organizational efficiency and effectiveness. ? Provided direct support and Supervisory oversight to

the Goose Creek and Fort Jackson Cyber Command Readiness and Risk Management Inspections that presented numerous challenges. ? Provided direct support for FT Benning and FT Gordon's SIPR eMASS development. Lead multiple Staff Assistance Visits to both locations to develop over 100 IA controls to over 1,700 Control Correlation Identifiers (CCIs) and 32 Control families for both locations. ? Delivered valuable input and recommendation on bridging the gap on the RNEC's ability to scan the entire network with in the required time lines emphasizing the need for more scanners. Recommendation that were used to create an Executive Summary that was staffed at the RNEC and forwarded to 2RCC as an RFC. After several follow up inquiries the RFC was approved for 4 additional ACAS scanners which will greatly enhance our scanning capabilities and reduce the overall number of vulnerabilities on the network. ? Management of computer assets of the Southeast Region lead to the designation of RNEC FT Stewart as the 93rd Signal BDE appoint as Large Facility of the Year award for 2017. HUMAN CAPITAL MANAGEMENT: Promotes an environment of inclusion, teamwork, and empowerment in which employees are encouraged to be creative and innovative in the development of solutions. Fosters an environment of professional and self- development where the importance of personal goals and objectives is stressed. Led Integrated Project Teams comprised of members from various departments in the successful completion of several high-visibility projects. COMMUNICATIONS: Briefs senior Military/Government Civilians (GS-15/O-6 and above) and other senior level staff on IT related issues and their impact on business operations. Develops regional cyber scorecard and metrics to measure organizational performance and implementation of agency initiatives. Responds to requests for information and provides briefings during quarterly information management officer's meetings. Chairs weekly staff and daily operations calls. ? Developed Plan of Action and Milestones (POA&M) to support Risk Management Framework (RMF) certification of key NIPR and SIPR networks throughout the South East region. ? Utilized his expertise with eMASS to develop a strategy for the implementation of over 1500 CCI's for both FT Gordon and FT Jackson's RMF effort. Assisted in each sites coordination efforts with higher commands and DISA on development and submission of POAM documentation. Supervisor Credence-LLC, ISSM, JSTARS Robins - Robins

AFB, GA October 2018 to March 2019 Ricky Wimsatt Supervisor Phone: 478-201-2686 Ok To Contact: YES Hours Per Week: 40 Support the Joint Surveillance and Target Attack Radar System (JSTARS) program at Robins AFB, GA efforts to manage cyber risk and protect Intelligence, Surveillance and Reconnaissance (ISR) missions. Responsible for managing risk protection for TS/SCI and ISR networks, systems, and applications. Perform Life Cycle activities Maintain day-to-day security posture maintenance support Perform continuous monitoring of information systems Accomplish Configuration Management procedures for "classified" networks Maintain security enclaves within NIST 800-53 standards Develop and Maintain systems in the Security Controls Tractability Matrix (SCTM) Work closely with the Contracting Officer Representative to identify and mitigate potential logical/physical security weaknesses Maintain the site POAM, SOP, SSP, and RAR in support of the Risk Management Framework (RMF) directives Work cooperatively to meet the needs of JWICS and SAP/SAR customers. Ensures the overall operation of the Special Compartmented Information Facilities (SCIF) are maintained to meet system security features and that security controls are applied to the systems within AF JWICS standards. Lead Information Security Analyst AVTC Group - Aberdeen Proving Ground, MD August 2018 to October 2018 Supervisor: Alice Brierley Supervisor Phone: 410-963-2129 Ok To Contact: YES Hours Per Week: 40 - Perform Information Assurance (IA) policy development, implementation and oversight for the CECOM-SEC in support of the Army Software Sustainment mission - Provide guidance on integration of security risk and management activities into ongoing Software Life Cycle management activities - Assist in Accreditation and Certification activities to support organizational transition from DIACAP to RMF Disabled American Veterans DAV (Volunteer) Carl Vinson VA Medical - Ctr, GA, US January 2018 to July 2018 Salary: $00.00Hr. Supervisor: Burl Jimerson Supervisor Phone: 478-954-2115 Ok To Contact: Yes Hours Per Week: 20 Provide personal transportation and escort services to US Veterans within the Carl Vinson VA Medical Center. Assist vets, their family members and visitors to/from the many clinics, imaging services and rehabilitation facilities on the complex. Be that compassionate ear for many vets during daily or long term stays. Division Chief Network Enterprise Center - Fort Sill, OK October 2014 to October 2015 Supervisor: Kathy Monroe

Supervisor Phone: 580-442-3617 Ok To Contact: Yes Hours Per Week: 50 Served as Division Chief of the Information Assurance (IA) Division of the Network Enterprise Center (NEC) at Fort Sill, OK; a large multi-mission installation. Oversaw the installation, configuration, testing, implementation, and management of the systems environment supporting the installation's computer security and operational business needs. Ensured the integration of IT/IA programs and services with business needs through monitoring and fine-tuning of the systems environment to meet service level agreements. Developed solutions to integration and interoperability issues. Maintained a viable Continuity of Operations Plan (COOP). EXECUTIVE LEADERSHIP: Managed a staff of 18 in the delivery of IT/IA Services and Support (Vulnerability Management, Configuration Management, Server and Application Support, and Cyber awareness) for 10,000 customers. Established and nurtured beneficial relationships with TRADOC and IMCOM that resulted in funding of key infrastructure projects including Network Intrusion Detection systems implementation. Improved perception of the NEC and quality of service provided with the implementation of SOP's, TTP, and user guides for classroom account creation, cyber training and cross domain solution violations. STRATEGIC PLANNING: Developed strategic goals and objectives that aligned with the 106th Signal Brigade Campaign Plan and that supported the Senior Mission Commanders' requirements. Commissioned and executed transformational projects that increased effectiveness and efficiency by successfully exploiting available technologies. Praised for ability to close gaps between requirements and technology by designing optimum solutions that were effective and met budget constraints. FINANCIAL MANAGEMENT: Developed Service Level Agreements and billing mechanisms for reimbursable above baseline services. Prepared inputs for inclusion into higher headquarters Program Objective Memorandum (POM). Identified and validated budget requirements and prepared and submitted acquisition packages to higher headquarters for funding approval. OPERATIONS MANAGEMENT: Executed Computer Network Defense by ensuring timely compliance with DISA STIGs, IAVAs, and other Information Assurance policies and regulations. HUMAN CAPITAL MANAGEMENT: Performed staff management functions to include hiring, assignment of work, development of training plans and writing performance appraisals and award

recommendations. Served as mentor and coach in assisting staff in achieving both personal and professional goals. COMMUNICATIONS: Served as a trusted advisor to senior leadership on critical IT issues and maintained rapport with key IT leaders by chairing monthly Information Management meetings with the G6/S6/IMO community. Established and maintained beneficial vendor relationships. ? Played a pivotal role in obtaining passing scores on DIACAP and DAIG Information Assurance Inspections; received laudatory comments from inspection team on the maturity of internal procedures ? Delivered high levels of customer service by resolving 81% of service issues within two days which exceeds C4IM SLA guidelines despite a 10% increase in service ticket volume and staff shortages ? Developed and implemented a robust IAVA management program; successfully remediated 95% of deployed workstations within 13 days ? Designer of FT Sill's Vulnerability Management Plan and (POA&M) to support Risk Management Framework (RMF) certification of NIPR and SIPR networks. ? Implementation of over 1500 CCI's in FT Sill's RMF effort. Directed, coordinated and managed all communication efforts with higher command, NETCOM and DISA on development and submission of POAM documentation. Supervisor CNE-CNA - Naples, IT October 2012 to October 2014 LCDR Lynor Duncan Supervisor Phone: Ok To Contact: Yes Managing information resources for the US Navy Command and Control (C2) and C4I systems: NIPRNET thru JWICS communications and local area networks. Develops Patch & Vulnerability management procedures for the life-cycle and Certification & Accreditation (DOD 8500) of over 25 C2 systems. STRATEGIC PLANNING: Interfaced directly with Major DOD vendors, Navy Office of Designated Approval Authority (ODAA) and Navy Cross Domain Solution Office (NCDSO) to develop acquisition and implementation strategies for Navy C2 and Intelligence systems. Working hand experience with US NAVY and Coalition systems such as DCGS, GCCS-J/M, Water Space Management, BICES, and Common Operational Picture (COP) systems. FINANCIAL MANAGEMENT: Project Manager, budget of $1M for the acquisition and implementation Water Space Management Cross Domain Solution system. Developed budgetary guidance to lines of business on what it would cost to complete required tasks associated with the project. Managed acquisition contracts for the purchase of hardware, software, supplies, and

services. OPERATIONS MANAGEMENT: Maintained high levels of system availability that resulted in no missed publishing deadlines. Successfully planned and executed large and complex IT projects from inception to completion that met stakeholder requirements and contributed to the achievement of corporate goals and objectives. Improved customer service by reorganizing the department into a structure that provided more depth and flexibility to meet rapid changing requirements in an environment driven by external market conditions. HUMAN CAPITAL MANAGEMENT: Routinely led cross departmental teams in the successful completion of 6TH FLEET TASKERS impacting projects. Performed staff management functions to include development of cyber mission and plans. Served as mentor and coach in assisting military and civilian personnel in achieving both personal and professional goals. COMMUNICATIONS: Led efforts in the collection and analysis of validated requirements, project plan development, and justification and allocation of resources. Conducted regular meetings with customers and staff. CyberSecurity Workforce (CSWF) Manager oversees the training program for the N6 staff, ensuring personnel meet the objectives of DOD 8570. ? Results - 80% N6 staff exceeded DoD 8570 requirements and 95% meet Information Assurance annual training guidelines in FY 13. ? Reorganized the CNE-CAN-C6F training program into a cross-departmental and command structure. Results--Organization successful completed the CCRI inspection in Mar 2013. ? Formulate briefs to Navy and Coalition customers on IA and technical security matters; metrics on system capabilities and findings from evaluations of networks utilizing DOD security tools. ? Successful integrating Risk Management Framework (RMF) in the organization's Software Development Life Cycle (SDLC) Division Chief Network Enterprise Center - Fort Sill, OK October 2009 to October 2012 Supervisor: Kathy Monroe Supervisor Phone: 580-442-3617 Ok To Contact: Yes Hours Per Week: 50 Served as Chief, Information Assurance Division (IA), Network Enterprise Center, FT SILL, OK. Responsible for all Information Assurance and Computer Security functions for the entire Ft. Sill community to include, COMSEC, Information Management, Information Assurance Vulnerability Management (IAVA), DIACAP & DAIG compliance, US Army, DISA, and DOD Information Assurance compliance. EXECUTIVE LEADERSHIP: Directed the

garrison and NEC in multiple roles such as the AT/FP (Level-II) and Threat Management representative, SEDA Training, and UDCI lead for all information violations. Provides support services to military, government civilian, and contractor personnel and continually coordinates with various directors, special staff elements, and tenants. STRATEGIC PLANNING: Participated in the development of strategic plans required to meet future business goals and objectives. Performed ROI analysis on all proposed infrastructure projects and funding requests to ensure they were in alignment with corporate strategy and would yield the desired results. FINANCIAL MANAGEMENT: Managed annual capital expenditure budget of $500K. Negotiated and managed acquisition contracts for the purchase of IT/IA hardware, software, supplies, and services. Developed IT/IA budget requirements to support execution of strategic plan. Reviewed and approved invoices for accuracy before submitting to finance for payment service. OPERATIONS MANAGEMENT: Lead the NEC to the successful completion of the DIACAP certification of both NIPR and SIPR networks in Jan 2012; DIAG inspection (Aug 2011) and the COMSEC inspections (Command Inspection Sept 2011; CSLA Apr 2012). Core Vulnerability Assessment Management Program (CVAMP) experience supporting vulnerability assessments of garrison and tenant organizations. HUMAN CAPITAL MANAGEMENT: Performed staff management functions to include hiring, assignment of work, development of training plans and writing performance appraisals and award recommendations. Practiced a style of leadership that promoted creativity while requiring accountability. Stressed the importance of individual empowerment and the importance of teamwork. COMMUNICATIONS: Established and maintained collaborative relationships with internal and external partners. Routinely briefed executive team on status of projects and execution of IT strategy. Served as liaison between IT and other departments to ensure that IT delivered the support required for successful execution of corporate strategy. Effectively communicate to multiple levels of audiences (Local Unit, Garrison, Cmd) the importance of IA/ IT strong security practices. Additionally, very active in the garrison community, author of many info grams, newsletters and articles providing up-to-date information concerning computer vulnerabilities and malicious applications, while assisting user with mitigation actions. The NEC liaison officer to

the Emergency Operations Center and an active member of the Installation Threat Working Group. ? Experience with the architecture, configuration, and support of systems that provide vital communication to our coalition forces and NATO (ABCS Officers). ? Very active in the garrison community, author of many info grams, newsletters and articles providing up-to-date information concerning computer vulnerabilities and malicious applications, while assisting user with mitigation actions. ? The NEC liaison officer to the Emergency Operations Center and an active member of the Installation Threat Working Group. ? Developed SOP and guidelines for the seamless flow of exercise and real-world record traffic in support of our national and global interest. Dept of US Army IT Specialist US Army - Fort Huachuca, AZ July 2008 to October 2009 Supervisor: Joseph Valladeres Supervisor Phone: 520-538-6687 Ok To Contact: Yes Hours Per Week: 45 EXECUTIVE LEADERSHIP: As Project Manager; reviews DOD contracts for compliance with the US Army Acquisition Programs Coordinates with US Army Customers, IPT Leads, and System Engineers to develop a strategy for the implementation of Classified and Sensitive systems for the warfighter. STRATEGIC PLANNING: Conducts detailed analysis of security requirements for new systems or modifications to existing systems. Recommend and documents total spectrum of security requirements from Federal, DOD and Dept. of the Army regulatory guidance, higher level policies, and system unique concerns. OPERATIONS MANAGEMENT: Serves as a senior Information Assurance (IA) system security certification specialist or systems security analyst in accordance with the Dept. of Defense Information Assurance Certification and Accreditation (DIACAP) and other statutory and regulatory requirements. Supervised a variety of IA personnel performing computer security/analysis tasks. COMMUNICATIONS: As team lead; plans, coordinates and provides information system security analysis or certification/validation to Program Executive Office (PEO), Major Commands (MACOM) or Dept. of the Army enterprise level projects. Performs duties as either an active participant or by monitoring the work of others. Analyzes vulnerabilities to determine risks to the system and the Global Information Grid (GIG), considering system development and operational environments, threats, and vulnerabilities. Develops detailed risk assessments for senior leadership and CIO/G6. Sr Information Assurance - Huntsville, AL October 2003 to November 2007

Supervisor: Brice "Kelly" Sparks Supervisor Phone: 256-313-9759 Ok To Contact: Yes STRATEGIC PLANNING: Supports the Information Assurance (IA) efforts for Fixed Station, Tactical, and Unmanned Aerial Vehicle Certification and Accreditation (C&A) testing efforts for the GMD and PATRIOT program. Manager for all contracts, budget and personnel resources that support 14 different Department of Army customers located throughout the United States. Coordinate the C&A test schedule with Prime/Subordinate contractors to complement work associated with the DITSCAP/DIACAP process. Develop the System Security Authorization Agreement (SSAA) OPERATIONS MANAGEMENT: Integrate the Unmanned Aerial Vehicles under the DIACAP process with other US Army systems for interoperability. Initiates and supervises the coordination of the Certification and Accreditation process with the IPT leads to ensure that US Army Acquisition and Procurement procedures are maintained. COMMUNICATIONS: Coordinates the development and updates of system security and accreditation plans and tracking systems, directs management reviews, and make Risk and Vulnerability Assessments, along with providing Security Awareness and Training. Develops Certification and Accreditation plans for multiple Ground-based Missile Defense (GMD) components such as Vulnerability Mitigation Plans, POA&Ms, and Security Requirements Traceability Matrix (SRTM) in conjunction with DOD 5200 and DOD 8500.1/2 requirements. Coalition Support Systems Combined Enterprise Regional Information Exchange System (CENTRIXS) U.S. Battlefield Information Collection and Exploitation (US BICES) Linked Operations-Intelligence Centers (LOCE, JAC Molesworth) Crisis Response Operations in NATO Operating Systems (CRONOS) Project Support Engineer General Dynamics May 2001 to May 2003 Public Company; 10,001 or more employees; Computer & Network Security industry) Served as a Project Support Engineer reporting directly to the Chief Information Officer for the Joint Analysis Center (JAC) RAF Molesworth UK. Provided a full range of computer systems analysis, planning, and computer system security activities to the JAC and HQ European Command (HQ EUCOM). Coordinated all the JAC efforts towards Certification and Accreditation within the DITSCAP and NIAP process. Experienced with System Security Authorization Agreement (SSAA) development. INFOSEC Engineer TELOS Corp October 1999 to June 2000 Public Company; 5001-10,000

employees; Computer & Network Security industry) Lead Security Engineer; responsible for the security policy, security testing, risk analysis, and all other documentation necessary for accreditation of classified and unclassified military systems. These systems are both Windows NT and UNIX (Solaris). Recommendations for improving security posture are also provided. The main function is to utilize Department of Defense (DOD) procedures and US Army regulations to determine if/how the system meet the certification and accreditation (C&A) criteria. Education Masters in Network Security Capitol College Bachelor in Information Technology American Intercontinental University Skills training, Excel, Management Military Service Branch: United States Air Force Rank: E7 Certifications/Licenses CISM July 2004 to June 2021 Security+ June 2020 CRISC June 2022 ITIL-3 Present Additional Information TS/SCI Active dates 05 Jun 2019

Name: Dawn Webster

Email: kimberlycallahan@example.net

Phone: 973.546.1362