Kammi Kai Hefner, PMP, EDD, CISM, CEH
Post Office Box 104 Pleasant Hall, PA 17246
Day/Evening Phone: 304 216-3617 Email: DrHefner@pobox.com
Abbreviated "targeted" resume available upon request via email.

PROJECT MANAGEMENT PROFESSIONAL (PMP)
20+ YEAR TECHNICAL EDITOR/WRITER
SUMMIT TECHNOLOGIES, INC. MECH SITE LEAD
IT SPECIALIST (INFOSEC) PKI COMPLIANCE AUDITOR
ASQ CERTIFIED QUALITY AUDITOR (CQA)
INFORMATION SYSTEMS SECURITY MANAGER wCISM & CEH
(*WITH MS IN COMPUTER SCIENCE AND MS IN SOFTWARE ENGINEERING WITH DoD TOP SECRET CLEARANCE***)**

PROGRAM MANAGER | DOCTORATE IN CURRICULUM & INSTRUCTION | CYBER TRAINING & EDUCATION SPECIALIST | SITE LEAD | QA MANAGER | COMPUTER SCIENTIST | SOFTWARE ENGINEER | REQUIREMENTS ANALYST RESEARCH ANALYST | PROCESS ENGINEER | TESTING & EVALUATION ENGINEER | METRICS ANALYST

COMPETENCIES

- Biologist (Bachelor's degree)
- Change Management Specialist (5yrs, NDIA CCDM)
- Conference Researcher & Presenter (since 2007)
- Configuration & Data Manager (5yrs, NDIA CCDM)
- Compliance Processes (5yrs)
- Computer Scientist (5yrs, Master's degree)
- Cyber (6yrs, ISAAC CISM, E-Council CEH)
- Cyber Compliance (8yrs, ISAAC CISM, E-Council CEH)
- Cyber Warrior (8yrs, ISSM, CISM, CEH , PKI Auditor)
- Curriculum and Instruction (20+yrs, Doctorate)
- Deputy Program Manager (7yrs, PMI PMP)
- Documentation Specialist (20+yrs, Dissertation)
- Education and Training Specialist (21+yrs, Doctorate)
- Franklin Covey Time Management (since 1993)
- Information Systems Security Manager (ISSM, 3yrs)
- Instructor (8yrs, EDD)
- Instructional Designer (20+yrs, EDD)
- Learning and Development Consultant (20+yrs, EDD
- Manager (7yrs, PMP since 2005)
- Metrics Analyst (5yrs, published)
- PKI Compliance Auditor (4 months)
- Process Engineer (2yrs)
- Program Manager (7yrs, PMP since 2005)
- Property Custodian (2yrs)
- Publisher (20+yrs, Dissertation)
- Quality Auditor (7yrs, ASQ CQIA, ASQ CQA)
- Quality Assurance Manager (7yrs, ASQ CQIA & CQA)
- Risk Management Framework (2 yrs)
- Requirements Analyst (3yrs)
- Research Analyst (20+yrs)
- Site Team Lead (1 yr)
- Software Configuration Engineer (5yrs)
- Software Engineer (5yrs, Master's degree)
- Technical Editor/Analyst (20+yrs, Dissertation)
- Technical Writer (20+yrs, Dissertation)
- Test & Evaluation Engineer (5yrs)
- Training & Education Specialist (20+yrs, Doctorate)

PROFESSIONAL CERTIFICATIONS
- **Project Management Institute (PMI) Project Management Professional (PMP), 09/23/2005-09/22/24.**
- **ISACA Certified Information Security Manager (CISM) 03/26/2015-01/31/2022.**
- **EC-Council Certified Ethical Hacker (CEH) 12/07/2018-12/06/2021.**
- **American Society for Quality (ASQ) Certified Quality Auditor (CQA) 12/02/2006-12/31/2022.**
- **American Society for Quality (ASQ) Certified Quality Improvement Associate (CQIA) 12/02/2006.**

- National Defense Industrial Association (NDIA) Certified Configuration and Data Manager (CCDM) 05/22/2008 (e.g., CM activities, Standards-based, CI Tracking, CSR).
- IT Infrastructure Library (ITIL) V3 Foundations Certified, Loyalist Certification Services, UK, 2008.
- Clarksburg Police Department Citizens Police Academy, 12/15/2004.

· CPR for Family and Friends, American Heart Association, 11/30/2004.
· Hazardous Materials Operations, West Virginia State Fire Commission, 10/20/2004.

SUMMARY OF CYBERSECURITY EXPERIENCE

Joint Force Headquarters-Department of Defense (DOD) Information Network (JFHQ-DODIN), Letterkenny Army Depot, Chambersburg, PA US – Public Key Infrastructure (PKI) Auditor (08/03/2020-Present)
• Continuously working to create collaboration amongst all PKI Audit Team Members (recognizing member's strengths and areas to grow).
• Continuously working to build good relationships with outside PKI-related entities.
• Serving as PKI Auditor "in training" for conducting 11/14/20 Department of Commerce Audit, 11/18/20 DISA Defense Computing Facility Mechanicsburg (DISA-MECH), and 12/01/20 Defense Commissary Agency (DeCA).
• Serving as instrumental lead on updating the PKI Auditor Standard Operating Procedures (SOP) document by correcting Table of Contents auto-generation, creating several Figures to better illustrate the Work Flow of conducting a PKI Audit.
• Serving as lead in developing the Training Plan for the PKI Auditor.

Defense Information Systems Agency (DISA), Naval Support Activity, Mechanicsburg, PA US – Information Systems Security Manager (ISSM) (07/08/2019-07/31/2020)
• Server as ISSM for several eMASS packages (i.e., assess program security compliance via Risk Management Framework (RMF), support program briefs, coordinate and compile program security documentation for various programs), support A&As.
• Developed and managed the IT Cybersecurity program for each A&A Program MIAP, EPSS, and CAMS-FM via answering AI Controls via maintaining their eMASS Packages and subsequent accreditation.
• Developed program policies (i.e., created and delivered the "Tracking Expiring POA&Ms and Milestones TTP" in response to an SSAE Audit (October 2018 – June 2020) NFR IT-2019 CO2-001 and provided subsequent training to SEL721.
• Developed program policies (i.e., created and delivered the "Tracking Expiring POA&Ms and Milestones TTP" in response to an SSAE Audit (October 2018 – June 2020) NFR IT-2019 CO2-001 and provided subsequent training to SEL721.

DISA, Letterkenny, Chambersburg, PA US – Vulnerability Scanner (1 month)
• Conducted scans via BURP and developed training for BURP and WVS.
DISA, Letterkenny, Chambersburg, PA US – Operations Support Team Lead for the DoDIN Inspection Operational Support Branch (RS12) - DoDIN Defensive Cyber Operations (DCO) Analysis & Reporting Division (RS1) - DoDIN Readiness & Security Inspections (DRSI) – JFHQ DoDIN (10/2016 to 5/31/2019)
• Experience in developing and implementing policy while providing analysis and guidance to senior leadership concerning the development, implementation, or modification of planning and coordination initiatives within IT Cyberspace programs while serving two years plus on OST.
• Extensive experience in developing and implementing information systems security programs, policies, and procedures both as part of the Training Team, as an ALT ISSM for CHA Building 1, and as an OST Member. These numerous SOPs and TTPs are listed throughout this resume.
• Provided technical support and guidance to all staff/Team Leads/inspection site participants in matters relating to information technology (IT) issues surrounding all Inspections (CCRI, CSSP, PKI) that involved a wide range of Technologies that spanned the entire organization via assisting to service the DODIN-Inspections.Mailbox and manning the telephone Help Desk.
• Assisted GOV Lead in coordinating efforts between Combatant Commands, Services, Agencies, and Field Activities on all planning and strategy matters, communicating with DODIN contributors to arrange and schedule DODIN Inspections, and evaluating the inspected entities DCO-IDM effectiveness and cyber compliance (two years' worth of Schedules, related correspondence, and inspection reports can be found on the t: drive in the OST Folders).
• Assisted GOV Lead in collaborating with DOD-level working groups and initiatives to explore ongoing integration issues among the cybersecurity provider (CSSP) community.

• Assisted GOV Lead in recording meeting minutes, notes and discussion points from strategic engagements to create headquarters After Action Reports (AAR).
• Provided senior leadership with situational awareness via Weekly Dashboard generation and briefings (two years' worth of Dashboard briefings can be found on the t: drive in the OST Folders).
• Assisted GOV Lead in creating and reviewing strategic engagement foundational documents.
DISA, Letterkenny, Chambersburg, PA - ISSM (2/2015 – 10/2016)
• Served as GOV alt ISSM for OPS/RME/DISA CHA Building 1.
DISA, Letterkenny, Chambersburg, PA - Lead Cyber Security Trainer/ Cyber Training Content SME / TTP Writer (6/2012 – 11/2014)
• Planned, managed, organized, directed and supervised cyberspace program training strategies, activities and initiatives as the Lead Technical Editor and Quality Manager (Quality Control Reviewer) providing expert level advice and assistance (conducted speeches/briefs) and performed oversight for all Leidos DRAFT/FINAL Tactics, Techniques, and Procedure (TTP) documents published on the IASE Web Site (over 10,000 downloads across the DoD organization by the user community).
• Provided IT technical editing services (expert level advice and assistance) by performing oversight for over 95 IT TTPs, and supplemental support documents: Implementation Plans, Operational Validation Plans, DCO Briefs and Executive Briefs (conduct speech/brief).

SUMMARY OF TEACHING/TRAINING EXPERIENCE

DISA, Letterkenny, Chambersburg, PA US – Vulnerability Scanner
• Conducted scans via BURP and developed training for BURP and WVS.
DISA, Letterkenny, Chambersburg, PA - ISSM (2/2015 – 10/2016)
• Served as GOV alt ISSM for OPS/RME/DISA CHA Building 1.
• Proactively created and presented several face-to-face training sessions on DISA Chambersburg (CHA) Building 1 Cybersecurity On-Board Briefings (TTP) to all personnel in Building 1 (05/18/18, 07/20/16, 08/25/16, 04/10/17. Aspiration was to finish presenting transition strategy to move course to an online platform via AICC, SCORM, xAPI. Research and prototype were completed.
DISA, Letterkenny, Chambersburg, PA - Lead Cyber Security Trainer/ Cyber Training Content SME / TTP Writer.
• Planned, managed, organized, directed and supervised cyberspace program training strategies, activities and initiatives as the Lead Technical Editor and Quality Manager (Quality Control Reviewer) providing expert level advice and assistance (conducted speeches/briefs) and performed oversight for all Leidos DRAFT/FINAL Tactics, Techniques, and Procedure (TTP) documents published on the IASE Web Site (over 10,000 downloads across the DoD organization by the user community).
• Provided IT technical editing services (expert level advice and assistance) by performing oversight for over 95 IT TTPs, and supplemental support documents: Implementation Plans, Operational Validation Plans, DCO Briefs and Executive Briefs (conduct speech/brief).
Shippensburg University, Shippensburg, PA US - Instructor of Computer Science
• Instructed undergraduate courses in computer literacy, microcomputer BASIC, and algebra.
Pennsylvania State University, Altoona, PA US - Instructor of Computer Science
• Instructed undergraduate courses in computer literacy, introductory programming in Watfiv FORTRAN and Pascal, and advanced assembler courses.
West Virginia University, Morgantown, WV US - Graduate Teaching Assistant
• Instructed undergraduate laboratory courses in IBM Assembler, VAX MACRO Assembler, and PL/I.
• Taught development workshops and modules required by the state for teacher certification.
West Virginia University Fire Service Extension Morgantown, WV - Training/Education Specialist
• Conducted the validation of the test bank questions for Swiftwater Rescue and Rope Rescue.
• Provided independent assessments of curriculum and wrote specific recommendations for certification.
Monongalia County Board of Education, Morgantown, WV US - Substitute Teacher
• Assisted teachers in incorporating computers and software into their courses, as courseware.
• Performed duties of Substitute Teacher at Secondary Education level.

Current ➔ Active DoD TOP SECRET
Reinvestigated and Granted 01/21/20
(Initially Granted 6/23/98 and Held Since)

EDUCATION

- Doctorate of Science, Cybersecurity, Capitol Technology University, Laurel, MD, expected graduation Dec 2020.
- **Education Doctorate, <u>Curriculum & Instruction</u>, <u>West Virginia University</u>,** Morgantown, WV, 2004
- **Master of Science**, **<u>Software Engineering</u>**, College of Engineering, West Virginia University, Morgantown, WV, 1999
- **Master of Science**, **<u>Computer Science</u>**, College of Arts and Sciences, West Virginia University, Morgantown, WV, 1987
- **Bachelor of Science, Biology,** <u>Fairmont State College</u>, Fairmont, WV, 1985 GPA: 3.4 out of 4.0
     Honors: cum laude Major: Biology Minor: Electronic Data Processing
- High School Diploma, Bridgeport Senior High School, Bridgeport, WV, 1980

A performance-driven, 30-year, customer-centric Computer Scientist/Software Engineer with strong skills in research, design, development, testing, evaluation, and maintenance of computer hardware and software systems. Twenty years' experience developing training courses under government contracts for the military and other adult learners. A 15-year Software Engineer specializing in requirements management. **Twelve years' experience in project planning and management (resources and tasks). A highly trained Research Analyst who has planned and conducted advanced work evidenced by a well received and published doctoral dissertation**. Six years' experience serving as Quality Assurance Manager/Specialist. A 5-year Lead Test Engineer at two National Institute of Standards and Technology (NIST)/National Voluntary Laboratory Accreditation Program (NVLAP) Common Criteria Testing Laboratories (CCTL). **A proven Technical Lead with an affective approach in guiding 45 colleagues to obtain their professional certifications. Six years serving as Cyber Defender of the DoDIN.** A dedicated Process Engineer of 5 years with an additional **three years of recent experience at DISA in defining Cyber Security P&Ps dedicated to protecting our DoDIN**. One and half years serving as the Alternate **Information Systems Security Manager (ISSM)** for the DISA Chambersburg location. An energetic, organized, motivated self-starter able to lead multiple, cross-functional projects while taking ownership of outcomes and applying creativity and innovative thinking. A dynamic player <u>able to tackle mission challenges</u> with adaptive flexibility, always producing <u>positive results on time</u>!

I have **Served as Program Manager (Work Group Leader) (perform oversight) for an IR&D Software Development Project I was awarded funding for via EWA. Was awarded continuing funding $33K for Independent Research & Development grant by EWA to develop and implement a Domain Engineering course for the World Wide Web (WWW). Was awarded a $25K Independent Research & Development grant by EWA to develop and implement a Domain Engineering course for the World Wide Web (WWW).**

I have two years and five months serving as team leader in a cybersecurity role as the **Lead Cyber Security Trainer/ Cyber Training Content SME / TTP Writer**. These TTPs address security architecture, systems auditing, and security tools that include Implementation Plans, Operational Validation Plans, DCO Briefs and Executive Briefs (conducting speeches/briefs). I provided IT technical support, guidance (expert level advice and assistance), and performed oversight on a wide range of IT issues that involve developing the content for DoD organizational DISA Cyber Protection Team (CPT) Training. **Across these efforts I developed instructions for conducting operations** [Assured Compliance Assessment Solution (ACAS)], risk assessments [ePO Disaster Recovery], **vulnerability management reviews** [Information Assurance Vulnerability Management (IAVM) Program Compliance], and **compliance validations** [HBSS Event Incident Analysis]. **I hold a CISM Certification which distinguishes me as having not only information security expertise, but also knowledge and experience in the development and management of an information security program.**

I have one year and eight months serving as the Alternate ISSM for DISA Chambersburg, PA.

I have two years' experience serving as the Contractor Operations Support Team Lead for the DoDIN Inspection Operational Support Branch (RS12) - DoDIN Defensive Cyber Operations (DCO) Analysis & Reporting Division (RS1) - DoDIN Readiness & Security Inspections (DRSI) – now residing with JFHQ-DODIN. I assist in providing technical support and guidance to staff/Team Leads/inspection site participants in matters relating to information management (IT) issues that involve a wide range of IT management that span entire organizations or components of the organization via assisting to service the DODIN-Inspections Mailbox and man the telephone Help Desk. I assist in reviewing detailed results from traditional security disciplines, network security, operating system security (multiple technologies), application security controls and general Information Assurance requirements via assisting in generating CCRI Compliance Reports. I develop, review, and tech edit numerous policies and procedures (P&P) and process guides to ensure information system reliability and accessibility and to prevent and defend against unauthorized access to systems, networks and data. I assist in creating technical reports (e.g., Compliance Reports, CCORI/CCRI/CSSP/PKI weekly dashboards, metrics, ESM Trends) that accurately capture inspection results, vulnerabilities, lessons learned, and actions that can be taken to prevent recurrence (i.e., Plan of Action and Milestones (POA&M)). I assist in monitoring existing information systems for compliance via calculating Vulnerabilities per Host (VPH) within established policies and guidelines. I assisted in developing the first pilot report for CCORIs that identify areas of residual risk.

I have completed four advanced degrees including a **Master's degree in Computer Science** (programming) and a **Master's degree in Software Engineering.**

WORK EXPERIENCE

Chenega Decision Sciences, LLC
DSCA Mechanicsburg
Navy Support Activity
Mechanicsburg, PA US

8/30/2021 to Present

Hours per week: 40

Cyber Security Analyst

• Assists with development and maintain Operational Level Agreements (OLAs) and end-to-end Standard Operating Procedures (SOPs) to identify collaborative responsibilities and support process interaction with other government and contractor IT groups.
• Develops and maintains a detailed policy matrix mapping federal, DoD, and local policies to the required security controls as identified by National Institute of Standards and Technology (NIST) SP 800-53and DoDI 8510.01.
• Administers CS training, including the annual Cyber Awareness Challenge training per DoDD 8500.1and compliance with the requirements of DoDD 8570.1 and DoD 8570-M for the IA Workforce Improvement Program (WIP).
• Provides operational risk management support for CS-managed systems, whether networked or standalone. Networks include varying security classifications, architectures, mobile devices, VirtualPrivate Networks (VPNs), and other remote access architectures and technologies, including SecureSocket Layer.
• Provides CS' portion of the Tier 3 Computer Network Defense (CND) services in accordance with DoDIO-8530.2, CJCSI 6510.01E, and CJCSM 6510.01.
• Supports enterprise level Information Assurance Vulnerability Management (IAVM) and DoD Reporting Management and Support, including vulnerability management oversight activities for all assets in the "Test" and "Production" enclaves and all standalone systems.
• Participates in the CS change management process, including attending the weekly Enterprise Change Control Board (ECCB) meetings, reviewing Requests for Change (RFCs) distributed in email, and performing risk assessments on hardware and software.
• Evaluates all newly deployed servers and applications in the "Test" and "Production" enclaves and verifies that the asset entries have been created in the DoD DPMS and ensure vulnerabilities have been mitigated and STIGs have been applied.

WORK EXPERIENCE

Department of Defense
DISA JFHQ-DODIN
Letterkenny
Chambersburg, PA US

8/3/2020 to 04/30/21

Hours per week: 40

Lead PKI Auditor

• Participated in on-line Speed Mentoring Program (08/28/20).
• Conducted PKI Audit of MECH OCSP Responder CSP.
• Solely created presented OUT-BRIEF for MECH & SATX PKI Audit (12/15/20 & 02/25/21).

- Assisted fellow PKI Teammate Mr. Hershey in all communications with US Navy Audit, DISA PAC, OKC and Headquarters by providing a review of email, FINAL In-Brief 10-Day Notice & Out-Brief PPTs.
- Assisted fellow PKI Teammate Mr. Klein in conducting the Defense Commissary Agency (DeCA) PKI Audit.
- Assisted Supervisor in conducting the DISA Defense Computing Facility Ogden (DISA OG) PKI Audit.
- Submitted updated multiple versions of the PKI Audit Program SOP.
    - Proactively created **Figure 2-1** to show the hierarchal development of the DOD PKI PMO Approved Certification Practice Statement (CPS) and Registration Practice Statement (RPS).
    - Proactively created **Figure 3-2** to show how the PKI Auditor orchestrates the PKI Audit Steps.
    - Proactively created ___ 1. ___ 2., etc. checklist steps to facilitate PKI Auditors using a team approach to conduct a PKI Audit.
    - Proactively pulled all the acronyms of the DOD PKI Audit Program together in to one list of Acronyms.
- Updated PKI Auditor Training Strategy Letter for submission to the DOD PKI PMO, Mr. JT Taylor for approval.
- Provided marked-up code-like OCSP Checklist to entire PKI Audit Team.
- Continuously working to create collaboration amongst <u>all</u> PKI Audit Team Members (recognizing member's strengths and areas to grow):
    - Proactively requested permissions to the PKI Portal for use by the entire PKI Audit Team.
    - Proactively wrote initial version of the PKI Training Plan.
    - Proactively established the folder structure and uploaded supporting Training Materials for the entire PKI Team.
    - Proactively provided marked-up code-like OCSP Audit Tool (checklist) to the entire PKI Team as a suggested "new" way of more smoothy running the checks during an audit interview.
    - Proactively developed self-paced "interactive" training for RA/LRA Certified Practice Statement (CPS) via an animated PPSX Slide Show.
    - Proactively emailed significant comments/suggestions on the 2019 MECH OUT-BRIEF to the entire PKI Team to use be used in updating slides for future use (i.e., USMC, MECH, DeCA).
    - Proactively created a highlighted "Audit Tool for National Security Systems Public Key Infrastructure Department of Defense and Common Service Provider Subordinate Certification Authority System Certification Practice Statement" document with notes and Action Items from a meeting with Supervisor and emailed it out to the entire PKI Team. Currently tracking and working to resolve all Action Items with entire PKI Team.
    - Proactively emailed the PKI Team "Steps on How to Generate a Live Org Chart for JFHQ."
    - Proactively requested the Conference Bridge for our PKI Team from Supervisor to support PKI Team meetings while teleworking.
- Continuously working to build good relationships with outside PKI-related entities:
    - Attend DOD PKI Operations Synch/CCB Meetings
    - Air Force's Enterprise Protection Risk Management (EPRM) Meetings
    - Worked with MECH POC to setup DCS Session for OUT-BRIEF.
- Continuously developing and implementing information systems security programs (milDrive & Intelink Folder Structures for CA, OCSP & RA Audits) (Tracking Requirements Status Spreadsheets for CA, OCSP & RA Auidts) and policies (e.g., TTPs, SOPs)
- Certified to Open/Close DISA Building 1, Letterkenny, Chambersburg, PA.

• Maintain audit checklists for Registration Authorities (RAs) and Local Registration Authorities (LRAs) in accordance with Natural Security Systems (NSS) and DoD Registration and Certification Practice Statements (CPS).
• Identify PKI Controls from NIST 800-53 Security Controls as they map to NSS and DoD PKI Audit requirements.
• Conduct at least six PKI Audits within a six-month period.
• Provide SME guidance conducting compliance audits of NSS and DoD Public Key Infrastructure at all levels of implementation.
• Exercise sound judgement in evaluating audit evidence with audit steps and intent of the appropriate practice statements.
• Conduct PKI Audit In-Briefs and Out-Briefs.
• Attend PKI PMO conference calls/meetings.

WORK EXPERIENCE

**Summit Technologies, Inc.
DoD DISA Mechanicsburg
Navy Support Activity
Mechanicsburg, PA US**

7/8/2019 to 7/31/2020

Hours per week: 40

Information Systems Security Manager (ISSM) (SEL721) & Summit Site Lead for MECH

• Served as ISSM for the MIAP, EPSS, and CAMS-FM Programs. Submitted eMASS package 11/27/19. Submitted ATO Extension for CAMS-FM 04/03/20 and A&A eMASS package July 2020.
• Demonstrated enterprise level (EcsoSystem) experience representing an organization (SEL721) while working in close coordination with multidiscipline teams across teg EcoSystem to accomplish security goals, initiatives and projects.
• Developed and implemented information systems security programs and policies as an ISSM (e.g., expired POA&Ms).
• Developed and implemented information systems security programs and policies for SEL721.
• Created and delivered the "Tracking Expiring POA&Ms and Milestones TTP" in response to an SSAE Audit (October 2018 – June 2020) NFR IT-2019 CO2-001 and provided subsequent training to SEL721.
• Analyzed the development and modification of Assessment and Authorization (A&A) documentation in compliance with DISA and DoD policy and guidance, including DoDI 8510.01, NIST SP 800-53, and CNSSI 1253.
• Assess program security compliance, support program briefs, and coordinate and compile program security documentation for various programs via RMF.
• Administered Risk Management responsibilities to include implementing DoD multi-tiered Cybersecurity risk management process.
• Established personal ISSM processes and internal controls (e.g., monitoring expired POA&Ms, OPORDs) to provide reasonable assurance that information network and systems (Accreditation Programs: MIAP, EPSS, and CAMS-FM) cyber deficiencies are tracked, reviewed, and responded to via teaming with program SAs.
• Developed and managed IT Cybersecurity program for each A&A Program MIAP, EPSS, and CAMS-FM via answering AI Controls via maintaining their eMASS Packages and subsequent accreditation.
• Analyzed production tasks relative to information system security via RMF IA Controls.
• Implemented, maintained, and analyzed procedures and security requirements via maintaining eMASS packages (i.e., assessing all controls).
• Directed, developed, maintained and implemented standard processes applied throughout DISA in support of the Cybersecurity mission area (i.e., created and delivered the "Tracking Expiring POA&Ms and Milestones TTP" in response to an SSAE

Audit (October 2018 – June 2020) NFR IT-2019 CO2-001 and provided subsequent training to SEL721.
• Developed program policies (i.e., created and delivered the "Tracking Expiring POA&Ms and Milestones TTP" in response to an SSAE Audit (October 2018 – June 2020) NFR IT-2019 CO2-001 and provided subsequent training to SEL721.
• Analyzed the security of equipment and systems currently in use via maintaining eMASS packages (i.e., assessing all controls).
• Contributed to high quality deliverables or tasks, offer ideas, probe for additional information, clarify assumptions, confirm agreed upon actions, and execute against defined data gathering and analytic approaches.
• Presented ideas clearly and logically, convey comprehension of the appropriate context, perform extensive on-the-job training and research, and work well as part of a fast-paced, highly productive team.

WORK EXPERIENCE

Booz | Allen | Hamilton
DoD DISA CHA Letterkenny
Chambersburg, PA US

6/3/2019 to 7/3/2019

Hours per week: 40

Vulnerability Scanner

• Began creating and updating training for BURP and WVS (still in use).
• Spent one month's time initiating the following tasks in support of conducting scans:
  • Investigated various organizations' public facing websites for pages that resolve to sites without the appropriate credentials.
  • Corresponded with organization's point of contacts for notification of websites requiring examination.
  • Administered web application security tools (Burp Suite) to scan websites while ensuring no abnormal responses occur.
  • Conducted analysis of findings that contain threats and/or vulnerabilities.
  • Executed analytical thinking and critical judgment of vulnerabilities that require various reporting and remediation method.
  • Accrued data from scan results and divulge them to organizations point of contacts.
  • Registered organization information and scan results into spreadsheet for government delivery.
  • Sent weekly status reports about scan production to Team Lead.

WORK EXPERIENCE

Booz | Allen | Hamilton
DoD DISA CHA Letterkenny
Chambersburg, PA US

10/2016 to 5/31/2019

Hours per week: 40

Operations Support Team Lead for the DoDIN Inspection Operational Support Branch (RS12) - DoDIN Defensive Cyber Operations (DCO) Analysis & Reporting Division (RS1) - DoDIN Readiness & Security Inspections (DRSI) – JFHQ DoDIN

• Extensive experience in developing and implementing information systems security programs, policies, and procedures both as part of the Training Team, as an ALT ISSM for CHA Building 1, and as an OST Member. The numerous SOPs and TTPs I have written are listed throughout this resume.
• Experience in developing and implementing policy while providing analysis and guidance to senior leadership concerning the development, implementation, or modification of planning and coordination initiatives within IT Cyberspace programs while serving two years plus on OST.

• Assisted GOV Lead in coordinating efforts between Combatant Commands, Services, Agencies, and Field Activities on all planning and strategy matters, communicating with DODIN contributors to arrange and schedule DODIN Inspections, and evaluating the inspected entities DCO-IDM effectiveness and cyber compliance (two years' worth of Schedules, related correspondence, and inspection reports can be found on the t: drive in the OST Folders).
• Assisted GOV Lead in collaborating with DOD-level working groups and initiatives to explore ongoing integration issues among the cybersecurity provider (CSSP) community.
• Assisted GOV Lead in recording meeting minutes, notes and discussion points from strategic engagements to create headquarters After Action Reports (AAR).
• Provided senior leadership with situational awareness via Weekly Dashboard generation and briefings (two years' worth of Dashboard briefings can be found on the t: drive in the OST Folders).
• Assisted GOV Lead in creating and reviewing strategic engagement foundational documents.
• As Team Lead assessed security architectures, developed project milestones, and managed/controlled resources.
• As Team Lead ensured completion of assigned projects within the scope of command objectives, priorities and time and resource constraints.
• Designed/created the CSSP Open POAM Tracker.
• Provided technical support and guidance to staff/Team Leads/inspection site participants in matters relating to information management (IT) issues that involve a wide range of IT management that spans entire organization or components of the organization via assisting to service the DODIN-Inspections .Mailbox and man the telephone Help Desk.
• Assisted in reviewing detailed results from traditional security disciplines, network security, operating system security (multiple technologies), application security controls and general Information Assurance requirements via assisting in generating CCRI Compliance Reports from the nSPECT Tool.
• Developed policies and procedures to ensure information systems reliability and accessibility.
• Developed policies and procedures to prevent and defend against unauthorized access to systems, networks and data.
• Developed, reviewed, and tech edited numerous policies and procedures (P&P) and process guides to ensure information system reliability and accessibility and to prevent and defend against unauthorized access to systems, networks and data (i.e., prepares, reviews, and edits cybersecurity documentation).
• Developed and implemented information systems security programs and policies (TTPs, SOPs).
• Assisted in creating technical reports (e.g., Compliance Reports, CCORI/CCRI/CSSP/PKI weekly dashboards, metrics, ESM Trends) that accurately capture inspection results, vulnerabilities, lessons learned, and actions that can be taken to prevent recurrence (i.e., POA&Ms).
• Assisted in implementing, maintaining, and conducting onsite and remote analyses of information system standard security products and associated systems.
• Assisted in created technical reports that accurately capture diagnosed incidents, associated threats, lessons learned, and actions that can be taken to prevent recurrence.
• Assisted in monitoring existing information systems for compliance via calculating Vulnerabilities per Host (VPH) within established policies and guidelines.
• Assisted in developing the first pilot report for CCORIs that identify areas of residual risk.
• Assisted in developing policies and procedures (TTP) to ensure information systems reliability and accessibility, and to prevent and defend against

unauthorized access to systems, networks, and data:
  Remote Network and ACAS Review Process Guide
  Windows Remote Process Guide
  Remote Reviewer Process Guide
• Functioned as subcontractor supporting the Department of Defense Information Networks (DoDIN) Inspection Operational Support Branch - DoDIN Defensive Cyber Operations Analysis & Reporting Division - DoDIN Readiness & Security Inspections (DRSI) with their cyber operational inspection/audit/assessment programs for information networks and systems throughout the Department of Defense that are connected to the DoDIN.
• Assisted in conducted on-site and remote analyses of information systems standard security products and associated systems via the CCRI, CSSP, CCORI, PKI Programs (i.e., conducting cyber security operations evaluations, audits, and reviews).
• Promoted awareness of security issues among management by submitting updates to TTPs and Dashboard Reports.
• Ensured best practice security principles were reflected in organizations' visions and goals via creating TTPs with ISSM reflected requirements.
• Populated centralized database with inspection data (start/end dates, status, inspection results, etc.) on a weekly basis.
• Generated, proof-read and printed/distributed all weekly dashboards.
• Attended the weekly GOV OST Meeting to review all cyber Trackers/Reports/Deliverables (dashboards) generated from the centralized database.
• Identified/designed new entries and dashboards for the centralized database.
• Provided relevant documentation and help desk support to all inspection sites.
• Provided direct customer support by fielding both telephone and email inquiries regarding inspection processes (application packages, review actions, deliverables).
• Updated specific trending spreadsheet with inspection results.
• Distributed dashboards for comment.
• Serviced all inspection-related mailboxes.
• Processed delinquent deliverables (e.g., Risk Reports, ACAS Scans).
• Conducted risk and vulnerability assessments of planned and installed information systems to identify vulnerabilities, risks and protection needs.
• Calculated Vulnerabilities Per Host (VPHs) for all inspection sites every 45 days.
• Maintained tracker of all sites and their corresponding VPHs.
• Completed the DoDIN Inspection Analysis Tool (DIAT) eMASS package (software tool that automates the assessment only and authorization processes) via addressing the authorization processes as defined by the Risk Management Framework (RMF). Addressed all controls via NIST SP 800-53 as defined.
• Completed a mapping from Cyber Threat Emulation (CTE) to NIST SP 800-30 via XLS.
• Tested new tracking tool from User perspective
• Designed new database tables to manage all plans of action (including incoming due & outgoing validations)
• Professionally Tech Edited and Delivered 12+ Cybersecurity-related documents
• Continuously attended/completed educational events/activities to maintain "renewable" Professional Certifications: ISACA CISM & PMI PMP & ASQ CQA.

WORK EXPERIENCE	**Booz	Allen	Hamilton** **DoD DISA CHA Letterkenny** **Chambersburg, PA US**	**2/2015 to 10/2016** **Hours per week: 40**

Alternate ISSM for OPS/RME/DISA CHA Bldg 1

• Proactively created and presented several face-to-face training sessions on DISA Chambersburg (CHA) Building 1 Cybersecurity On-Board Briefings (TTP) to all personnel in Building 1 (05/18/18, 07/20/16, 08/25/16, 04/10/17. Aspiration was to finish presenting transition strategy to move course to an online platform via AICC, SCORM, xAPI. Research and prototype were completed.

• Attended the weekly "Monday" RME OPS Meetings (SIPR) to prep for the Tuesday IA/DCO Sync and Wednesday Standup with the Director, **Mr. Hickey**. **Briefs** the RME ISSM RISK ISSUES slide on behalf of Mr. Kenton on alternating weeks.

• **Delivered** the DISA CHA Chambersburg (DISA CHA) DITPR Account Activation **TTP** V1R1, the SNAP-SGS Account Activation **TTP** V1R1, and the CMRS-DPMS Account Activation **TTP** V1R1. Each have been published and are available for review on the DISA CHA Building 1 Security Features User Guide (SFUG) SharePoint site (https://disa.deps.mil/org/RE7/RE73/DISA%20CHA/DISA%20CHA%20SFUG/default.aspx)

• Proactively created the DISA CHA Building 1 RE7 LAN Support **Departing Employee Checklist** for use by RE7 LAN Support to address defects discovered in the process during ISSM audit reviews (04/07/15).

• Proactively created initial DRAFT of the Quality Assurance Product Review & Final Inspection Report For TTPs **to ensure standardized repeatable processes in developing TTPs** (06/01/15).

• Proactively created Record of Tech Editing **Checklist to ensure standardized repeatable processes in tech editing TTPs** (06/09/15).

• Proactively provided a detailed set of comments/suggestions to the CYBERSECURITY STRATEGY (CSS) PROGRESS SUMMARY (**reflects recent cybersecurity-related policy changes**) from a Program Manger's perspective and from a presenter's perspective via upper leadership back to the DoD CIO. This Cybersecurity Strategy (CSS) (formerly the Acquisition IA Strategy) provides guidance and a template, in light of revised DoD issuances including DoDI 8500.01, 8510.01, and 5000.02 (04/27/15).

• Ensured the implementation and compliance of DISA's Cybersecurity Program within the Center/Element as defined by the Authorizing Official (AO) and Senior Information Security Officer (SISO).

• Ensured the Center/Element compliance with all applicable DoD Cybersecurity Instructions, directives, manuals, and policies.

• Ensured all Program/Project Managers (PM), System Managers (SM), and Information System Security Managers (ISSM) and Information System Security Officers (ISSO) are appointed in writing for all Information Systems (IS) and Platform Technology (PIT) systems.

• Coordinated with the Center/Element's Security Manager to ensure compliance with Center/Element's overall security posture.

• Reviewed and endorsed Security Authorization Packages (SAP).

• Ensured all DoD Information Technologies were registered in appropriate systems (DoD Information Technology Portfolio Repository (DITPR), Enterprise Mission Assurance Support Service (eMASS)).

• Ensured validity of Risk Management Framework (RMF) controls for eMASS Packages via review and testing of Compelling Evidence (all systems within RME).

• Ensured PMs identify a data owner in DITPR for each Center/Element managed information system.

• Advised and supported the PM, SM and/or PM in implementing the DISA Cybersecurity Program (Defense Security Accreditation Working Group (DSAWG), DoDIN).

• Ensured PM/SMs maintain positive configuration control of all Center/Element information system s and assets.

• Ensured all PM/SMs complete all required Federal Information Security Management Act (FISMA) requirements and mandates.

• Ensured owned and/or managed Information Systems and devices were configured IAW applicable Instructions and Security Technical Implementation Guides (STIG) and Security Requirement Guides (SRG).

• Ensured all Cybersecurity, Computer Network Defense (CND) tools and/or capabilities were deployed, implemented and configured per USCYBERCOM and DISA direction.

• Ensured USCYBERCOM, DCC, and RE orders are available to PM/SMs and the lowest level ISSMs, ISSOs and System Administrators.

• Ensured implementation and compliance with all USCYBERCOM and DISA orders and directives.

• Ensured noncompliances were documented in an approved Plan of Action and Milestones (POA&M).

• Continuously monitored and tracked Cybersecurity compliance.

• Ensured incidents adhered to the Incident Handling Program.

• Ensured all external-facing internet services or Internet-based Capabilities (IbC) on unclassified networks adhered to whitelist policies and were registered in the Ports, Protocols, and Services Management (PPSM) registry.

• Ensured all personnel performing Cybersecurity duties within the Center/Element were identified appropriately and documented within the Joint Table of Distribution (JTD), Corporate Management Information System (CMIS) and the IA Tracking Tool.

• Ensured all personnel performing Cybersecurity duties within the Center/Element were properly qualified and documented in the IA Tracking Tool.

• Ensured all personnel within the Center/Element completed all required Cybersecurity training annually (documented in CMIS).

• Acted as the OPS ISSM in the event of the primary ISSM's absence.

- Provided cybersecurity meeting minutes, statistics, reports, and other metrics reports as required.
  - Created and distributed weekly DITPR report to field sites
  - Monitored monthly OPC Cybersecurity compliance (e.g. CMRS, HBSS, ACAS, DITPR)
  - Monitored FISMA validation/reporting
- Ensured all privileged users received the necessary technical and Cybersecurity training, education, certification and user agreements to carry out their Cybersecurity duties.
- Integrated and applied Department/Agency missions, organization, function, policies, and procedures within the enclave.
- Ensured that protection and detection capabilities were acquired or developed using the IS security engineering approach and were consistent with DoD Component level IA architecture.
- Ensured IAT Levels I – III, IAM Levels I and II, and anyone with privileged access performing IA functions received the necessary initial and sustaining IA training and certification(s) to carry out their IA duties.
- Prepared and/or oversaw the preparation of IA certification and accreditation documentation.
- Participated in an IS risk assessment during the C&A process.
- Ensured information ownership responsibilities were established for each DoD IS and implement a role-based access scheme.
- Analyzed, developed, approved, and issued enclave IA policies.
- Evaluated proposals to determine if proposed security solutions effectively addressed enclave requirements, as detailed in solicitation documents.
- Identified IT security program implications of new technologies or technology upgrades.
- Evaluated cost benefit, economic and risk analysis in decision making process.
- Interpreted and/or approved security requirements relative to the capabilities of new information technologies.
- Interpreted patterns of non-compliance to determine their impact on levels of risk and/or overall effectiveness of the enclave's IA program.
- Analyzed identified security strategies and selected the best approach or practice for the enclave.
- Ensured that security related provisions of the system acquisition documents met all identified security needs.
- Evaluated and approved development efforts to ensure that baseline security safeguards were appropriately installed.
- Evaluated the presence and adequacy of security measures proposed or provided in response to requirements contained in acquisition documents.
- Took action as needed to ensure that accepted products meet Common Criteria requirements.
- Monitored and evaluates the effectiveness of the enclaves' IA security procedures and safeguards to ensure they provide the intended level of protection.
- Developed systems security contingency plans and disaster recovery procedures.
- Provided enclave IA guidance for development of the COOP.
- Ensured all IAM review items are tracked and reported.
- Advised the DAA of changes affecting the enclave's IA posture.
- Obtained and maintained IA baseline certification appropriate to position.
- Developed policy, Standard Operating Procedures (SOP), Techniques, Tactics and Procedures (TTP) and other documentation to support compliance with all applicable DoD/DISA Cybersecurity instructions, directives, manuals, and policies.
- Provided ISSM validation, tracking and signatory to various account provisioning DD Form 2875 to include, but not limited to VMS, CMRS, DPMS, IS, HBSS and eMASS.
- Provided administrative support in development and maintenance of SharePoint sites, web sites, email distribution list/mailboxes.
- Continuously attended/completed educational events/activities to maintain "renewable" Professional Certifications: ISACA CISM & PMI PMP & ASQ CQA.

Kami-Oh! Konsultants   **09/22/2014 to 02/10/2015**
Pleasant Hall, Pennsylvania US   **Hours per week: 40**
Program Manager / IT Training Consultant / Research Analyst
- Recertified Project Management Professional (PMP) professional certification via Project Management Institute (PMI) Professional Development Units (PDUs).
- Recertified American Society for Quality (ASQ) Certified Quality Auditor (CQA) professional certification.
- Provided consulting services to private organizations in IT, technology, programming, training and proposal development (08/2011 "X-ray imaging").
- Received several contingent offers: contracts were not awarded.

LEIDOS "formerly SAIC"   **6/2012 to 11/2014**
DoD DISA FSO Letterkenny
Chambersburg, PA US   **Hours per week: 40**
Lead Cyber Security Trainer/ Cyber Training Content SME / TTP Writer
- Planned, managed, organized, directed and supervised cyberspace program training strategies, activities and initiatives as the Lead Technical Editor and Quality Manager (Quality Control Reviewer) providing expert level advice and assistance (conduct speech/brief) perform oversight for all Leidos DRAFT/FINAL **Tactics,**

Techniques, and Procedure (TTP) documents published on the IASE Web Site (currently over 10,000 downloads across the DoD organization by the user community). Each document is geared towards preventing and defending against unauthorized access to the DoDIN (Department of Defense Information Network "formerly known as the DoD Global Information Grid (GIG)" systems, networks, and data (ensure that all CND functions relate to overarching strategy for the Department) and supports the Network Defense Division (ensure CND functions) dedicated to providing network assurance and network defense. The executable tasks known as procedures ensure information systems' reliability and accessibility (ensure that all CND functions relate to overarching strategy for the Department). These include security architecture, systems auditing, and security tools, and all areas related to INFOSEC (Information Security). These TTPs directly address security architecture, systems auditing, security tools, and all areas related to INFOSEC by providing strategic network defense guidance (ensure that all CND functions relate to overarching strategy for the Department) dedicated to providing network assurance and network defense (i.e., prepares, reviews, and edits cybersecurity documentation).

o The development of a TTP begins with an exhaustive search of any and all related Mission Essential Tasks (METLs) to execute a Requirements Analysis activity. The ideal list of policies I review include strategic network defense guidance and policy, such as: CONOPs, CTOs, Directives, Instructions, METLs, OPORDs, SOPs, TASKORDs and training plans. I have specialized experienced with all of the following (and many more) to ensure the defense of information networks and systems and to prevent and defend against unauthorized access to systems, networks, and data (ensure that all CND functions relate to overarching strategy for the Department) dedicated to providing network assurance and network defense through the planning, analysis, development, implementation, maintenance, and enhancement (implement, maintain, and conduct on-site and remote analyses) of information systems security programs, policies, procedures and tools:

- · ***Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01F, Information Assurance (IA) and Support to Computer Network Defense, 9 February 2011***
- · ***Chairman Joint Chiefs of Staff Manual (CJCSM) 6510.01, Defense-In-Depth: Information Assurance (IA) and Computer Network Defense (CND), 25 March 2003***
- · *CJCSI 6510.01F, Information Assurance (IA) and Support to Computer Network Defense, 9 February 2011*
- · *Communications Tasking Order (CTO) 09-002, Directive for Disabling Autorun throughout the DoD Global Information Grid (GIG)*, 15 May 2009
- · *CTO 08-005, Directive for Automated Scanning, Remediation and Reporting of Network Vulnerabilities throughout the DoD Global Information Grid (GIG)*
- · ***DoD Instruction 8500.2, Information Assurance Implementation, 6 February 2003***
- · ***Department of Defense Instruction (DODI) 8530.2, Support to Computer Network Defense (CND), 9 March 2001***
- · *USCYBERCOCM OPORD 12-1016, HBSS Deployment and Operations*, 31 August 2012
- · *USCYBERCOM TASKORD 13-0670, Implementation Of Assured Compliance Assessment Solution (ACAS) For The Enterprise*, 1 August 2013
- · *USCYBERCOM WARNORD 13-0107, HBSS Baseline*, 14 February 2013

• Provided IT technical support and guidance (expert level advice and assistance) (conduct speech/brief) perform oversight to all TTP Writers on a wide range of IT issues that are geared towards preventing and defending against unauthorized access to the DoDIN systems, networks, and data and supports the Network Defense Division dedicated to providing network assurance and network defense. The executable tasks known as procedures ensure information systems reliability and accessibility. These TTPs address security architecture, systems auditing, and security tools: Assured Compliance Assessment Solution (ACAS), Asset Configuration Compliance Module (ACCM), DIACAP, DIACAP Independent Verification and Validation (IV&V), DIACAP Security Testing and Evaluations (ST&E), NSA Whitelist, HBSS Device Control Module (DCM) for the IAM, FireSIGHT, ePO Disaster Recovery, HBSS Enhanced Reporting (ER) Extension Capability, Supply Chain Risk Management (SCRM), HBSS Tier 3 Operations, Continuous Monitoring and Risk Scoring (CMRS), HBSS Event Data Processing, HBSS Event Detection, HBSS Event Preliminary Analysis, HBSS Preliminary Response, HBSS Event Incident Analysis, HBSS Response and Recovery, HBSS Infrastructure, Operational Attribute Model OAM, Maintaining a Healthy Rogue System Detection (RSD) Infrastructure, Information Assurance Vulnerability Management (IAVM) Program Compliance, Implementing Incident Response and Recovery Team (IRRT) Policy Auditor (PA) Benchmarks, Joint Incident Management System (JIMS), Rogue System Detection (RSD) Port Spanning (currently over 10,000 downloads across the DoD organization by the user community).

• Provided IT technical editing services (expert level advice and assistance) perform oversight for over 95 IT TTPs, and supplemental support documents: Implementation Plans, Operational Validation Plans, DCO Briefs and Executive Briefs (conduct speech/brief). Each supplemental support document is geared towards preventing and defending against unauthorized access to the DoDIN systems, networks, and data and supports the Network Defense Division (ensure CND functions) dedicated to providing network assurance and network defense. The Implementation Plans and Operational Validation Plans' Use Cases ensure information systems reliability and accessibility. The DCO Briefs and Executive Briefs address security architecture, systems auditing, and security tools, and all areas related to INFOSEC in the form of a verbal presentation (conduct speech/brief).

• I have experience planning managing, organizing, directing and supervising cyberspace program training strategies, activities, and initiatives.

• Wrote content for Operational Attributes Manager (OAM) TTP as SME after conducting Training Gap Analysis. Specifically, the executable tasks known as procedures ensure information systems reliability and accessibility by providing the DoD a unique perspective into ePO-managed asset ownership and responsibility thus, ensuring information systems reliability and accessibility (dedicated to providing

network assurance and network defense). OAM is considered to be an auditing tool.
• Recorded DCO Session (conduct speech/brief) for OAM.

● Responsible for redesigning the HBSS Event Data Processing Phase documents. This sets precedence for a cyber security methodology.

● Responsible for redesigning the ACAS TTP (which is available the IASE Web Site). This sets precedence for a cyber security technique.

• Assisted in the design and development of tool used in the analysis of the effectiveness of TTPs.
• Instantiated (beginning in 06/2012) the Leidos QA/CM for all deliverables.
• Provided IT technical support and guidance (expert level advice and assistance) (conduct speech/brief) perform oversight on a wide range of IT issues that involve developing the content for DoD organizational DISA Cyber Protection Team (CPT) Training (solely geared towards preventing and defending against unauthorized access to the DoDIN systems, networks, and data and supports the Network Defense Division) dedicated to providing network assurance and network defense. These are Assured Compliance Assessment Solution (ACAS) Introduction to Vulnerability and Compliance Auditing, Asset Configuration Compliance Module (ACCM), Reporting Functionality of Asset Publishing Service (APS), Anti-Virus/Anti-Spyware (AV/AS), Continuous Monitoring and Risk Scoring (CMRS) Management Approach to Cyber Security Oversight, HBSS Device Control Module (DCM), Enterprise Mission Assurance Support Services (eMASS), HBSS Reporting in ePolicy Orchestrator (ePO), Flying Squirrel Wireless Discover Application (FWSDA), HBSS Protection and Detection Using Host Intrusion Prevention System (HIPS), Information Assurance Vulnerability Management (IAVM) System, Joint Incident Management System (JIMS), Operational Attribute Model (OAM), HBSS Compliance and the Role of McAfee's Policy Auditor (PA), Secure Configuration Compliance Validation Initiative (SCCVI)/Retina, Vulnerability Management System (VMS), and Virus Scan Enterprise (VSE).
• Developed systems security contingency plans and disaster recovery procedures and common network and host-based forensics activities.

• Received "Special Letter of Recognition" from PEO MA4 for my work! All developed content is available on the DEPS.

• Visited Scott ABF DISA CONUS to gather over-the-shoulder training content for Securify OJT to support ESD CND Implementation of organizational DoD DISA OPORD 12-061 out of DISA Network Defense Division FS4. This product is directly geared towards preventing and defending against unauthorized access to the DoDIN systems, networks, and data and supports the Network Defense Division (ensure CND functions) dedicated to providing network assurance and network defense. The product is available on the SIPRNet. This represents a focused effort to enhance synergy between DISA FSO and DISA CONUS.
• Wrote Securify Training Manual, available on SIPRNet to support DISA Network Defense Division FS4.
• Initiated processes for standing up organizational Department of Defense's (DoD) Cyber Defense University (CDU) via Defense Information Systems Agency (DISA) [similar to the DAU] by providing IT technical support and guidance (expert level advice and assistance) (conduct speech/brief) from an educational perspective on a wide range of IT Management topics.
• Utilized Curriculum and Instruction background (technical support and guidance) (expert level advice and assistance) (conduct speech/brief) to create organizational CONOPS and Strategic Plan for the CDU.
• On behalf the Government, audited (implement, maintain, and conduct on-site and remote analyses) the organizational DISA FSO Security Readiness Reviewer class for UNIX (passed), earning credit hours towards my CISSP. The entire focus is on-site and remote analyses of information system standard security products and associated systems via STIGs (dedicated to providing network assurance and network defense) (to ensure that all CND functions relate to overarching strategy for the Department). These STIGs provide standard security protection required for information systems and networks processing at all levels of information security. This represents a focused effort to enhance synergy between DISA FSO F3 and DISA Training Content.
• On behalf the Government, audited (implement, maintain, and conduct on-site and remote analyses) the organizational DISA FSO Security Readiness Reviewer class for Windows (missed by 2 pts), earning credit hours towards my CISSP. The entire focus is on-site and remote analyses of information system standard security products and associated systems via STIGs (dedicated to providing network assurance and network defense) (to ensure that all CND functions relate to overarching strategy for the Department). These STIGs provide standard security protection required for information systems and networks processing at all levels of information security. This represents a focused effort to enhance synergy between DISA FSO F3 and DISA Training Content.
• Analyzed and identified technical training requirements and coordinated execution of training plans.
• I have experience planning managing, organizing, directing and supervising cyberspace program training strategies, activities, and initiatives.
• Continuously attended/completed educational events/activities to maintain "renewable" Professional Certifications: PMI PMP & ASQ CQA.

Kami-Oh! Konsultants   **12/2010 to 6/2012**
Fairmont, WV US   **Hours per week: 40**

Program Manager / IT Training Consultant / Research Analyst
• Prepared to take Microsoft® Certified Systems Engineer (MCSE) Certification: first exam is "Designing a Windows Server 2003 Active Directory and Network Infrastructure" Exam 70-297.
• Recertified Project Management Professional (PMP) professional certification via Project Management Institute (PMI) Professional Development Units (PDUs) 60 of 60 units are completed.

• Recertified American Society for Quality (ASQ) Certified Quality Auditor (CQA) professional certification.
• Served as Principal Investigator for on-line study "Assessing the Awareness and Utilization of the Scale of Points to Rank Rhodesian Ridgeback Breed Characteristics."
• Provided consulting services to private organizations in IT, technology, programming, training and proposal development (08/2011 "X-ray imaging").
• Received contingent offer for full time employment from SAIC in 02/2011 for their Technical Training Specialist position with the BTF in Clarksburg, WV: contracts were not awarded.
• Received contingent offer for full time employment from DSD Labs in 12/2011 for their Technical Trainer/Production Lead position in Clarksburg, WV: contracts were not awarded.
• Asked to be PMI West Virginia / Ohio Valley Chapter Inc. Newsletter Editor, 04/12.
• Received contingent offer for full time employment from IMTAS in 04/2012 for their Senior Test Engineer position in Clarksburg, WV: contract not awarded.

SAIC   **3/2006 - 12/2010**
Morgantown, WV US   **Hours per week: 40**
Quality Assurance Manager II
• As QA Manager II (Quality Control Review), led the continued execution of comprehensive appraisal programs (e.g., performing product reviews; developing evaluation/information assurance plans and procedures; providing IT technical support and guidance; conducting process audits via interviews; implement, maintain, and conduct on-site and remote analyses; and ensure that functions relate to overarching strategy) across six information management (IT) organizational contracts (i.e., Project Start-Up, Software Lifecycle Phases (Software Development, Requirements, Design, Testing), through Project Close-Out) using Microsoft® Project to track all milestones and CDRLs in conjunction with the Integrated Master Schedule (MPP).
o Wrote and implemented Project Quality Plans (e.g., QA Plan, Quality Assurance Program Plans (QAPP), Quality Control Plans (QCP), Quality Management Plans (QMP), and other administrative technical plans (i.e., System Checklist, Migration Instructions, IAR, User Manual, Technical Manual, SVDD).
• As a Documentation Specialist, wrote/produced (provided technical support and guidance across a wide range of IT Management documents) the following CDRLs:
   ❖ Administration Installation Guide
   ❖ Administration Properties
   ❖ Administration Users Guide
   ❖ Configuration Guide
   ❖ Developer Coding Standards
   ❖ Developer Usage Guide
   ❖ Information Assurance Review (IAR) P&P
   ❖ Payload Compression
   ❖ Release Audit
   ❖ Scenario Description
   ❖ Scenario Player Installation Guide
   ❖ Scenario Player Users Guide
   ❖ Service Requirements
   ❖ Services Installation Guide
   ❖ Services Integration Guide
   ❖ Services Quick Guide
   ❖ Software Version Description Document
   ❖ Testing Procedures
   ❖ Backup Restore Manual
   ❖ Migration Release Instructions
   ❖ Offline Editor User Manual
   ❖ Project Management Plan / Strategy (PMP)
   ❖ Server Load Sum
   ❖ Software Requirements Specification (SRS)
   ❖ Software Version Description Document (SVDD)
   ❖ Software Test Report
   ❖ Technical Manual
   ❖ User Manual
   ❖ Web Services Description Document
o Reviewed and approved all project documentation (e.g., CMP, PMP, QRAM, RMP, Test Plans, IARs, Test Reports) (e.g., implement, maintain, and conduct on-site and remote analyses).
o Two main organizational focus projects were 1) Airborne Web Services (AWS), directed by United States Air Force (USAF) Air Force Materiel Command (AFMC) 653 Electronic Systems Wing (ELSW)/EID, had through its initial spirals of research and development a vision of enabling Net Centric Operations between air and ground nodes across the Enterprise (the communications backbone that interconnects all nodes on a network) utilizing prototype web services and a Services Oriented Architecture (SOA) approach & 2) Command and Control Manager (C2MM) application provided the Air Force Special Operations Forces (AFSOF) with a Web-enabled tool set to manage the submission of Special Operations Forces (SOF) Air Support Requests (ASRs) and to plan and schedule the SOF air missions generated from those requests. Across both agile IT projects implemented scrum methodology. Witnessed the use of SOAPUI testing.
o Played integral part of the Seay Business Unit's (BU) Organization Integrated Process Group (IPG) in identifying opportunities via research and analysis (i.e., implement, maintain, and conduct on-site and remote analyses) on process improvement activities by providing expert advice and guidance (conduct speech/brief) on QA principles, practices,

and procedures via written reports and oral presentations. **Awarded First Place Winner of the organization's 2006 IPG Process Improvement Award ($1000), 3/15/2006. This represents a focused effort to enhance synergy between the BU and all underlying projects.**

o **Founded (i.e., perform oversight, established objectives, schedules, and deadlines; secured resources and funding) and served as ASSET BU Organization's Quality Training & Certification Program Coordinator (mentored and motivated 45 QA/CM/PI Division Staff remotely located to obtain their Professional Certifications in QA, CM, PM and ITIL; reported status orally in bi-weekly staff meetings to upper line management; represented staff to management on daily basis (e.g., conduct speech/brief, resolved conflicts); provided IT technical support and guidance "in layman's terms" ; (implement, maintain, and conduct on-site and remote analyses) across a wide range of IT Management topics where QA was a focus, managed staff to ensure timeliness in meeting assigned deadlines and completing training exercises; evaluated completed work); used Microsoft® Project to track all milestones and CDRLs; and taught classes.** This represents a focused effort to **enhance synergy** between the BU and all QA/CM/PI Staff.

o **Presented (conduct speech/brief) multiple times on behalf of our QA/CM/PI Division to the Quality Community of Excellence (Quality CoE) a major component of the SAIC, beginning in 07/07 and the Quality Managers Forum in 2008.** This represents a focused effort to **enhance synergy** between the BU QA/CM/PI Staff and all other SAIC Quality Managers (Quality Control Review).

o **Fielded/provided IT technical support and guidance (conduct speech/brief) inquiries from our geographically-dispersed organizationally-wide QA/CM/PI Division Staff on SAIC P&Ps (e.g., strategies, goals, objectives and priorities – representing a wide range of IT Management issues) in the execution of our comprehensive appraisal programs on a daily basis.**

o Coached/provided technical support and guidance (implement, maintain, and conduct on-site and remote analyses) (conduct speech/brief) to Project Staff on execution of major component of organization CMMI® requirement: Peer Reviews.

o **Managed the development and on-time delivery of Management Volumes, Quality Assurance and Quality Control Plans, Configuration Management Plans and Metrics Plans on a 30-day turn around schedule.**

• Continued to serve as QA Process Work Group Lead (perform oversight) (see QA Manager position).

o Implemented and wrote QA processes for the Seay BU Organization Legacy P&Ps by providing expert advice and guidance (implement, maintain, and conduct on-site and remote analyses) (conduct speech/brief) on QA principles, practices, and procedures representing major components of the SAIC QAS.

o **Served as QA Process Work Group Lead (perform oversight) in the Engineering Edge (EEdge) Rollout (02/07) and ESBU (Peck) Process Asset Set Rollout (06/06) by providing expert advice and guidance (conduct speech/brief) on QA principles, practices, and procedures.**

• Continued to serve as Metrics Analyst Working Group Lead (see QA Manager position) (i.e., implement, maintain, and conduct on-site and remote analyses).

• Supported the improvement and deployment of a CMMI® Level 5 BU Quality System.

• Participated as Team Member of a Standard CMMI® Appraisal Method for Process Improvement (SCAMPI) (i.e., implement, maintain, and conduct on-site and remote analyses) (conduct speech/brief). This represents a focused effort to enhance synergy between BU Qa and under lying projects.

• Received SEI Certificate of Completion for CMMI® V1.2 Upgrade Training 09/05/07.

• Participated at organizational-level as developer/writer/reviewer by providing technical support and guidance (i.e., implement, maintain, and conduct on-site and remote analyses) (conduct speech/brief) on twelve information management technology (IT) proposals using SAIC's Virtual Proposal Center (VPC), Proposal Information Exchange (PIE), Microsoft® Office: Access, Excel, PowerPoint, Project, SharePoint, and Word. Writing focus was on QA Plans and procedures, Metrics Plans and Configuration Management Plans. Received training on IBM's Rational Toolset (e.g., ClearCase – SCM and ClearQuest - bug tracking and process automation).

• Served ASSET BU Organization's QA Web Portal Web Mistress (Microsoft® SharePoint).

• Served as entire ASSET BU Web Portal Web Mistress (Microsoft® SharePoint).

Contact Supervisor: Yes, Supervisor's Name: Mrs. Anita Henderson-Carlos, Supervisor's Email: ANITA.K.HENDERSON-CARLOS@saic.com

SAIC   **1/2005 - 3/2006**
Morgantown, WV US   **Hours per week: 40**
Quality Assurance Manager I

• As QA Manager (Quality Control Review), led the continued execution of comprehensive appraisal programs (i.e., performing product reviews; developing evaluation/information assurance plans and procedures; providing IT technical support and guidance; conducting process audits via interviews; implementing, maintaining, and conducting on-site and remote analyses; and ensuring that functions relate to overarching strategy) across six information management (IT) organizational contracts (i.e., Project Start-Up, Software Lifecycle Phases (Requirements, Design, Testing), through Project Close-Out) using Microsoft® Project to track all milestones and CDRLs in conjunction with the Integrated Master Schedule (MPP).

o Wrote and implemented (provided technical support and guidance) Project Quality Plans (i.e., QA Plan, Quality Assurance Program Plans (QAPP**),** Quality Control Plans (QCP), Quality Management Plans (QMP), and other administrative technical plans (e.g., System Checklist, Migration Instructions, User Manual, Technical Manual, SVDD).

o **Conducted hundreds of internal product inspections (implement, maintain, and conduct on-site and remote analyses) of deliverable products (researched CDRL requirements as defined in the SOW) across six information management (IT) organizational contracts and verified compliance against the SOW.**
o **Reviewed and approved all project documentation (e.g., PMP, CMP, RMP, Test Plans, IARs, Test Reports).**
o **Conducted hundreds of process audits (implement, maintain, and conduct on-site and remote analyses) using standard QA techniques (e.g., inspections, Test & Measurement, metrics, and sampling).**
o Provided an objective, independent view (implement, maintain, and conduct on-site and remote analyses) of the quality of software products and execution against BU Organization IT procedures via written reports and oral presentations (conduct speech/brief).
o Conducted QA process and product audits (implement, maintain, and conduct on-site and remote analyses) and wrote and orally presented (conduct speech/brief) Process Reviews, Product Reviews & Final Inspection Reports for six contracts on a regular weekly basis to the Project Manager and to the customer and upper line management during SAIC Project Management Reviews (PMR) on six different information management (IT) organizational contracts.
o Conducted independent research on a regular basis (i.e., new Task Orders) (implement, maintain, and conduct on-site and remote analyses) in order to identify, assimilate, interpret, and analyze specific policies and procedures to identify any complex issues, draw conclusions, report findings and recommend detailed steps (e.g., white paper) to resolve unprecedented situations (i.e., performance-based acquisition).
o **Developed policies and procedures, and QA Checklists for conducting simultaneous process audits at BU- and CMMI®-Level.**
o Conducted in-coming inspection (implement, maintain, and conduct on-site and remote analyses) of vendor and customer provided products.
o Witnessed and approved product information assurance/acceptance testing (i.e., FAT, SAT).
o **Led effort as Work Group Leader (perform oversight) for implementing and writing QA processes to support the CMMI® Process Rollout, September 2005 by providing expert advice and guidance on QA principles (provided technical support and guidance), practices, and procedures.**
● **Work Group Leader (perform oversight) serving as Process Lead, made regular oral presentations to the customer and upper line management during SAIC Project Management Reviews (PMR) on six different contracts**.
● Work Group Leader (perform oversight) serving as Metrics Analyst and Lead, researched, developed, collected, managed, wrote (implement, maintain, and conduct on-site and remote analyses) and orally presented (conduct speech/brief) reports for Project- and BU-level metrics via DataDrill to customer and upper line management during SAIC Project Management Reviews on six different contracts.
● Continued to serve as Metrics Analyst Working Group Lead (i.e., implement, maintain, and conduct on-site and remote analyses) (conduct speech/brief).
● Served as Work Group Leader (perform oversight) for QA/CM/PI Division Staff to create and maintain up-to-date searchable repository for past proposal assets.
● Interfaced and coordinated with project staff: project management, systems engineer, developers and testers on a daily basis.
o **I WAS THE QUALITY ASSURANCE MANAGER (QAM), (Quality Control Review) Process Lead and Metrics Analyst and Lead on six contracts at SAIC (2005-2010). As the QAM I kept the PM and project engineering organization apprised of all quality issues and areas requiring attention (e.g., non-conformance concerns). I was an integral part of the development process and project team in delivering compliant, high-quality products. I MAINTAINED A COOPERATIVE RELATIONSHIP WITH THE PROJECT TEAM TO ENSURE THAT ALL QA RECOMMENDED ACTIONS FOR POLICY COMPLIANCE, PROCEDURE UPDATES AND PROCESS IMPROVEMENTS WERE CONSTRUCTIVE AND ADOPTED. In this capacity I wrote the Quality Assurance Program Plan (QAPP)** (using Adobe® Acrobat Professional, Bank Street Writer, Adobe® FrameMaker, MacWrite, Microsoft® Word, Webster's New World Writer, WordPerfect®, and Writing Assistant) addressing each contract's SOW that identified the minimal documentation required, methodologies I USED ANALYZING MANAGEMENT PRACTICES, STANDARDS, AND PRACTICES AND DETAILS ABOUT THE QUALITY ASSURANCE (QA) TASKS, REVIEWS, AND AUDITS I CARRIED OUT TO ENSURE THAT THE FINAL PRODUCT WAS RELIABLE AND NOT ONLY MET SAIC STANDARDS, BUT ALSO MET CONTRACT AND USER REQUIREMENTS. As the Process Lead, I provided expert advice, ANALYSIS AND GUIDANCE ON QA PRINCIPLES, practices, and procedures in the Engineering Edge (EEdge) Rollout (02/07) and ESBU (Peck) Process Asset Set Rollout (06/06). I addition, I supported the improvement and deployment of a CMMI® Level 5 BU Quality System. I WAS THE METRICS ANALYST AND LEAD.
Contact Supervisor: Yes, Supervisor's Name: Mrs. Anita Henderson-Carlos, Supervisor's Email: ANITA.K.HENDERSON-CARLOS@saic.com

West Virginia University Fire Service Extension (WVU FSE)   **11/16/2004 – 01/19/2005**
Morgantown, WV US   **Hours per week: 20**
Training/Education Specialist
● Conducted the validation of the test bank questions for Swiftwater Rescue and Rope Rescue and used these results to update test bank based on evolving curriculum and certification requirements.
● Provided independent assessments of curriculum.
● Wrote specific recommendations for certification updates based on roles.

Kami-Oh! Konsultants   04/06/2004 to 01/19/2005
Fairmont, WV US   Hours per week: 40
Program Manager / IT Training Consultant / Research Analyst
• Provided IT consulting services (technical support and guidance) to private clients in technology, IT Management, programming, and training (covering a wide range of IT Management issues) at an organizational level.
• Developed framework for on-line IT training program via WEB CT.
• Posted content and performed administrative functions with IT WebCT (a LMS) for two years (e.g., Physics Department at Fairmont State University and Dr. Pat Obenauf (Curriculum & Instruction) at West Virginia University). Used all of the IT Web CT features: Course Utilities, Course Components, Designer Map and Tools.
• Conducted assessments of the LMSs: Blackboard, Blended Schools, IBM's Lotus Learning Management System, eCollege, Eledge, Intelladon, moodle, OnPoint's Learning Suite, and Ziiva.
• Developed content with/for LMS using IT WebCT, Georgia State University's Excel Macro, Makequiz, Jack Yensen's IBM HotMedia 3.5, Impatica for PowerPoint, Horizon Live, and Alan Shapiro's WebCT Calendar Tool.
• Member of Questionmark Communities.

Electronic Warfare Associates, Inc.   4/1992 - 4/2004
Fairmont, WV US   Hours per week: 40

Project Management
• **Served as IT Program Manager (Work Group Leader) (perform oversight) for an IR&D Software Development Project I was awarded funding for via EWA!**
• Assisted program manager in managing government and commercial technical contracts' resources for five years.
• Assisted program manager as Task Work Group Lead (perform oversight) for five years by defining budgets and resolving personnel issues (i.e., conflict resolution).
• Assisted program manager in managing sub-contracts' SOWs, deliverables, and schedules using Microsoft® Project.
• Assisted program manager in managing and in supervising 27 sub-contractors in all areas of producing CDRLs.
• Assisted program manager in developing and maintaining strategic plans, policy assessments and recommendations, cost analyses, specification documents, various studies, and IT budget inputs.
• Assisted program manager in reviewing contractor proposals for modifications and enhancements to systems or applications to ensure compliance with specifications.
Manages and coordinates the acquisition of information technology assets, i.e. computer hardware/software, network and reuse assets for major systems.
• Assisted program manager in developing standards and criteria for performance management, capacity management, content management, knowledge management, and problem management.
o Plans and coordinates all phases of the acquisition, implementation, and integration of assets.
o Conducts extensive research and analytical studies and develops specifications, justifications, and economic analyses in support of selection and acquisition actions.
• Wrote Monthly Technical Reports for all sub-contracts for government prime.
• Represented EWA to the Government (Organizations: Navy, NASA, Air Force), WVHTFC, and Prime Contractor (DN America and DSD Labs.) (conduct speech/brief) during all Program Management Reviews, In Progress Reviews, IT Technical Interchange Meetings, and Staff Meetings by serving as a principal/support presenter; and briefed all pertinent aspects of EWA tasks and specific contributions to support contract mission/goals.
• Provided leadership and mentorship (technical support and guidance) for the EWA subcontractors; specifically Azimuth, Inc. & New-Bold Enterprises by instilling the desire to develop skills for identifying long term, goal oriented visions for all contract tasks; the desire to contribute to the BEWT Team approach to completing Phase I of the contract; and the desire to effectively communicate with EWA any concerns/problems/issues or questions associated with any/all contractual tasks.
• Provided vision, direction, and leadership (technical support and guidance) for other EWA employees, including those personnel not contributing to the BEWT/SORT/NPLACE effort by sharing software/teaming/management related seminars/products/training that may be beneficial, providing technical computer assistance, discussing the goals and missions of EWA and ways of implementing them, and allowing time for others to discuss concerns/problems/issues.
• Mediated problem solving/resolution events amongst staff from four sub-contractors.
• Served as Library Administrator, Training and Education Project Work Group Lead, and Library Operations Project Work Group Lead (perform oversight) for seven years on CARDS.
• Serviced inquiries concerning administrative issues from all contract staff.
• Conducted interview process for identifying new employees under EEO guidelines.
• Obtained quotes, made recommendations, and purchased HW/SW to support government contracts.
• Orally presented program progress results to Government customer at monthly Integrated Process Team (IPT) Meetings.
• Served as Quality Coordinator (Quality Control Reviewer), Training Coordinator, and Lead Auditor (Work Group Leads) (perform oversight) for four years on NVLAP.
• Edited IT technical/administrative documents as a consultant providing expert advice and guidance.
• Identified requirements for, designed and produced marketing brochures.
• Conducted in-depth Market Survey and Analysis for identifying COTS solution and selected vendor after presenting findings to customer and clients.

Electronic Warfare Associates, Inc　　　　　　　**4/1992 - 4/2004**
Fairmont, WV US　　　　　　　　　　　　　　　**Hours per week: 40**

Senior Software Engineer

• Designed, developed, and delivered complete Quality Systems (Quality Control Review) to support two Common Criteria Testing Labs.
• Served as principle author (and book boss manager for coordination) in writing suite of BEWT/BFTT Software CDRLs:
  ❖ Configuration Management Plan (CMP)
  ❖ Computer Operation Manual (COM)
  ❖ CLIN 0001-0033 Increment 1 Engineering Development Models (EDM) Builds
  ❖ CLIN 0001-0033 Increment 2 Engineering Development Models (EDM) Builds
  ❖ Computer Software Configuration Item (CSCI) Test Descriptions
  ❖ CSCI Traceability to SRS/IRS
  ❖ Development Environment Definition (DED)
  ❖ EDM1 Generic BMCS Software Unit Test Procedures
  ❖ Engineering Change Proposals (ECP) No. 2053, 5010
  ❖ Entity Modeling and Motion (EM&M) CSCI
  ❖ Factory Acceptance Test (FAT) Plan
  ❖ Information Assurance Review (IAR) P&P
  ❖ Installation Documents (for *32 different applications*)
  ❖ Integration and Test Methodology
  ❖ Interface Design Document (IDD)
  ❖ Interface Requirements Specification (IRS)
  ❖ Operator Processor Console and VME Power Up/Down Instructions
  ❖ Site Acceptance Test (SAT) Plan
  ❖ Software Design Document (SDD)
  ❖ Software Development Environment
  ❖ Software Requirements Specification (SRS)
  ❖ System Development Plan (SDP)
  ❖ System Hardware Unit Level Tests
  ❖ System Development Plan (SDS)
  ❖ Software Test Description (STD)
  ❖ Software User Manual (SUM)
  ❖ System Integration Test (SIT) Plan
  ❖ CSCI Test Descriptions
  ❖ Test Environment
  ❖ Version Description document (VDD)

• Participated as key presenter (conduct speech/brief) in code walkthroughs for government customer.
• Analyzed, interpreted and defined software and system requirements for new applications (i.e., software development).
• Completed long and short-range projects in the modification of systems, software, hardware, and networks.
• Conducted risk assessment and system reliability studies (implement, maintain, and conduct on-site and remote analyses) & produced final reports and recommendations.
• Conducted Factory Acceptance Tests (FAT) and Site Acceptance Tests (SAT) (Test Plans) and wrote and presented final Information Assurance Reviews/Test Reports to government customer.
• Served as Configuration Manager (CM) (Work Group Leader) (perform oversight) for BEWT software and hardware by managing/administering all CM activities (i.e., maintained baselines, identified/reported metrics, tracked/documented CIs, scripted software builds).
O Developed standards and criteria for configuration management and change management.
o Developed processes for and built software loads and ensured correct hardware configuration (i.e., writing/modifying scripts, development of hardware and software systems developing techniques, procedures, and processes).
o Participated in control boards (i.e., provided agendas, recorded minutes, served as lead for EWA).
• Defined, collected and reported metrics in support of process improvement for government contracts.
• Wrote Policies & Procedures for employee performance management system under CCTLs.
• Conducted audits of all systems under CCTLs (i.e., training, CM, evaluation, employee performance, process).
• Conceived and established three new Process Improvement Programs.
• Reengineered assembler and C++ firmware on a Motorola MPC860 processor using IDA for recoding.
• Instituted Symantec's GHOST procedure for production of multiple Engineering Development Models.
• Implemented data warehouse solution using Microsoft SQL Server 2000.
• Collected metrics to establish required resources for model-based library development and support.
• Coordinated and oversaw production, delivery, and installation of manufactured BEWT Units.
• Developed Information Assurance Review (IAR) Plans and Procedures (P&P) for Network Managers (e.g., Command/POST, SPECTRUM, Konfig, and Enterprise Manager), Mapping Services (GIS) (e.g., MapInfo, OpenMap), and Database Managers (i.e., Oracle).
• Performed functional testing on Network Managers (e.g., Command/POST, SPECTRUM, Konfig, and Enterprise Manager), Mapping Services (GIS) (e.g., MapInfo, OpenMap), and Database Managers (i.e., Oracle).

• Designed, developed unit level test procedures and facilitated resolution of BEWT software/hardware to BFTT interface (i.e. development of hardware and software systems developing techniques, procedures, and processes.
• Designed, developed Information Assurance Review (IAR) Plans and Procedures (P&P) and Software Test Plans for the qualification of components for the Air Force's Qualified Product List.
• Designed, developed and modified test protocols (i.e., scripts) for Database Managers components.
• Configured test environments and secured test input/output for Engineering Development Models.
• Provided real-time responses/technical support and guidance to Technical Assistance Requests (TARs) and System Trouble Reports (STRs).
• Coordinated and conducted in-depth Market Survey for identifying COTS solution and selected vendor.
• Designed, acquired, installed, and administered Pentium PC LAN using Windows NT and HP-UX 10.x.
• Planned and coordinated all phases of the acquisition, implementation, and integration of assets.
• Conducted research (i.e., analytical studies) and developed specifications, justifications, and economic analyses in support of selection acquisition assets.
• Designed and coded many Web sites (i.e., BEWT, EWA, National Product Line Asset Center (NPLACE)).
• Updated NASA's Technology Transfer Strategy Document.

Electronic Warfare Associates, Inc   **4/1992 - 4/2004**
Fairmont, WV US   **Hours per week: 40**
Training/Education Specialist
• As the IT Training and Education Project Lead for the Comprehensive Approach to Reusable Defense Software (CARDS) (Work Group Leader) (perform oversight) contract (Air Force, 1992-1995), created and conducted four major training programs (Policies & Procedures, Library Administration, Domain Engineering, FODA, and Intro to Reuse) and coordinated and sponsored the West Virginia Reuse Education Workshop(s). Materials from all of these training programs were delivered to the customer as CDRLs. The main focus of the workshop was to coordinate and develop means to enhance synergy amongst those interested in Software Reuse.
o Managed the West Virginia Reuse Education Workshop (coordinated advertising, logistics, registration, hotel/lodging/transportation) effort among several high level organizations including West Virginia University and SAIC). The main focus of the workshop was to coordinate and develop means to enhance synergy between industry and academia. Synchronized the Domain Engineering series of topics, selected presenters, defined the requirements, coordinated this effort among a dozen presenters from several different companies, prepared all the slide presentation/course materials, made strong recommendations for reinforcement exercises and developed these for each section of the series, created the evaluation criteria and forms, distributed to each participant and analyzed, each course was a success and met the training objectives.
o Gathered data to support my metrics research "An Experienced-Based Optimization of the Goal/Question/Metric Paradigm," which was published by the University of California's Irvine Research Unit in Software and the University of Southern California's Center for Software Engineering, 30 March 95.
• Served as the Training Lead (Work Group Leader) (perform oversight) on EWA's Software Optimization and Reuse Technology contract (1995 – 1997).
o Organized, led and served as the primary contact for organizing the SORT Domain Engineering and Technology Transfer Workshop held in January 1997 at the NASA Ames Research Center. The main focus of the workshop was to coordinate and develop means to enhance synergy amongst those interested in Software Reuse. Coordinated all aspects of the workshop by working with many unfamiliar agencies and individuals (i.e., proposed curriculum, oversaw the development of marketing brochures and marketing strategies; developed a database to manage the logistics of the workshop; identified and scheduled presenters, scribes and panelists; assigned all working groups; conducted the registration and tracked cancellations; designed and printed all attendee badges; assisted attendees with food, lodging reservations, and travel accommodations; presented at the Workshops; and, organized and conducted Birds-of-a-Feather sessions.) Evaluations indicated this workshop was a success. Coordinated all efforts between many sponsors (i.e., DISA, NASA, SAIC, WVU) and built long-lasting partnerships.
• Supervised several teams of trainers throughout my career at EWA.
• Designed (via Navy SOW requirements) curriculum, coded, conducted assurance reviews, tested and maintained the GUI WBT Training System for the ship fielded BEWT System (identified learning objectives, instantiated appropriate learning style delivery for seaman, evaluated effectiveness based on Navy end user feedback, updated CBT course materials per EDM release, authored training manuals and documents, taught on-sight classes at Norfolk and San Diego bases).
o Managed the BEWT Fleet Support Office (BFSO - a customer service center) that maintained a bi-directional communication interface with the Navy that addressed customer feedback and complaints. Serviced all incoming requests from Navy personnel and orally presented requests, recommendations, modifications and alternative viewpoints to the customer for incorporation into the next software release. Used this avenue to update the Navy's curriculum in training/certifying end users in use of the Navy's onboard AN-SLQ32.
o I WAS THE DIRECTOR OF THE BEWT FLEET SUPPORT OFFICE (BFSO) (EWA, Navy, 1997-1999), where I ESTABLISHED THIS OFFICE [THE FOCAL POINT BETWEEN THE NAVY FLEET USER AND THE BEWT DEVELOPMENT TEAM TO ESTABLISH THE ADVANCED LINE-OF-SITE COMBAT TRAINING SYSTEM]. I initially launched this office IAW REQUIREMENTS ANALYSIS (via the Program Goals

identified in the SOW), and I INSTITUTED DAY-TO-DAY LOGICAL WORK AND INFORMATION FLOWS (PNPs, SOPs). I also CONTINUALLY EVALUATED THESE OPERATIONAL PROCEDURES TO ASSESS THE IMPACT OF SOW OBJECTIVES, NAVY operations, and available resources eventually determining the feasibility of implementing such a new office. My focus as a customer service representative was TO NEGOTIATE A FINAL RESOLUTION TO ALL REQUESTS WHICH REQUIRED DISCUSSING AND EXPLAINING THE SAME TECHNICAL INFORMATION (OFTEN CONTROVERSIAL) TO SEAMAN, NAVY PERSONNEL, ENGINEERS AND OTHER CONTRACTORS. In this capacity I ACTED AS **THE <u>MAIN LIAISON</u> BETWEEN THE USERS OF THE SYSTEMS, THE NAVY CUSTOMER HOLDING THE FUNDING, AND THE ENGINEERS RESPONSIBLE FOR IMPLEMENTING REQUESTED CHANGES VIA SOFTWARE RELEASE FOR THE BEWT/BFTT SYSTEM**. I COMPILED AND PRESENTED BEWT Evaluations after ASSIGNING A PRIORITY LEVEL TO THE INCOMING RESPONSES. I WORKED DIRECTLY WITH NAVAL PERSONNEL TO ASSURE CORRECT PRIORITY ASSIGNMENTS. This assisted in allowing me to emphasize what the users really saw as IMPORTANT TO BE INCORPORATED INTO THE NEXT ENGINEERING RELEASE. I also MONITORED BEWT USER ACTIVITY, GATHERED METRICS, AND COLLECTED USER FEEDBACK ON BEWT OPERATIONS. To assist in gathering data from BEWT Users I not only designed the BEWT Evaluation Form but I also established procedures to ensure all incoming requests and queries from established BEWT Users were recorded, addressed and tracked to closure. I BRIEFED THE ENTIRE TEAM [a wide range of stakeholders including our government customer] during official PMRs) eventually RECEIVING CONSENT TO INCORPORATE SUGGESTED IMPROVEMENTS). The ultimate focus of the BFSO was to coordinate and develop means to enhance synergy amongst those interested in using BEWT.
O Provided technical support and guidance to staff in matters relating to information management (IT) issues that involved a wide range of IT management that spanned the entire organization and/or components of the organization.

• Physically installed BEWT/BFTT training systems on the USS ENTERPRISE and the USS COLE !!!

• Served as Common Criteria Testing Lab's (CCTL) Training Coordinator (Work Group Leader) (perform oversight) (NPLACE, Air Force, 1997-1998, 1999-2002).
 o Conducted gap analysis, analyzed requirements, (implement, maintain, and conduct on-site and remote analyses) designed responding curriculum, identified content, wrote, and implemented the NPLACE Training Plan.
o Authored, developed and coded NPLACE's on-line, Web-based, HTML interactive tutor (i.e., NVLAP Trainer) for learning and understanding our role and interaction with NVLAP (used this HTML interface to provide a new and exciting way for the staff members to grasp the concepts of establishing a CCTL).
o Coded the NVLAP Trainer's on-line quizzes and tests that were automatically graded and provided immediate feedback (such as WebCT) to support mastery learning for the student.
o Developed an MS Access database that tracked and managed all student progress (i.e., tracked student's registration and completion of assigned units, their quiz/test scores, and their overall progress) and course assessment information (i.e., a system that incorporated many administrative features of an LMS).
o Evaluations from students provided feedback on navigation techniques that were incorporated for New Staff Training and suggestions for course content updates. These data provided the foundation for measuring the effectiveness and efficiency of the NPLACE Training Program.
o Provided written advice and guidance to managers (conduct speech/brief) in making specific modifications the NPLACE Training Program.
o The NVLAP Trainer was successful in preparing our staff members in their specific role-based duties (executing appropriate procedures) for an internal audit by NVLAP on their understanding of these concepts.
o Developed the curriculum, created the course content and conducted twenty "live" training sessions courses required for the staff members of NLPACE for Common Criteria Testing Lab Certification: Introduction to the Quality Manual, Writing P&Ps, Work Instructions and Forms, and CEM.
• Served as DIAL's Common Criteria Testing Lab's (CCTL) Training Coordinator (Work Group Leader) (perform oversight) (NPLACE, Air Force, 2002-2003).
o Conducted gap analysis, analyzed requirements, designed responding curriculum, identified content, wrote, and implemented the DIAL Training Plan.
o Incorporated Self-Directed Learning (SDL) to help control costs and to permit the students to control their time, place, duration, and method of learning. This method lends itself to the subject and material and interaction with an instructor was not required. Computer-Based Training (CBT) via the Internet and other written materials were included.
o Conducted many Interactive Classroom Learning sessions to provide our staff with needed interaction with the instructor (myself) because my explanations and experience with the subject matter were vital to understanding the information. Group activities were included to emphasize course content.
o Provided access for students to One-on-One Learning during the initial learning period for our Information Assurance Review/Testing/Evaluation Processes. I was available during all normal business hours to our customer to assist in the initial learning of a complex subject (i.e., P&Ps, Testing/Evaluation Process). I was able to assist our staff in their ability to integrate their learning to their roles defined in the Quality Manual.
o Employed IT Networking as a follow-up to the initial training sessions. I provided an environment to enable our staff members to train together that encouraged the free exchange of ideas, experiences, and successes.
o Made strong recommendations (conduct speech/brief) for our staff to attend Outside Workshops,

Conferences and other training activities sponsored by NIST and NVLAP. The primary focus of attendance was to coordinate and develop means to enhance synergy amongst individuals working in software testing.

o Adopted a combination of learning formats (e.g., SCORM) that delivered learning using a variety of learning methods that were cost- and time-effective. This saved our contract the cost of expensive learning for the classroom and made time management easier (i.e., our staff was able to perform required tasks quicker with more accuracy).

• Contributed as Key IT Training Presenter (conduct speech/brief) in three major Company/Organization Proprietary marketing briefings at EWA CEO and EWA Vice-President level, Nov-Jan, 1998 (i.e., DEA).

o I was the key training presenter in three major Company marketing briefings at EWA CEO and EWA Vice-President Levels, Nov-Jan, 1998. These oral discussions (conduct speech/brief) involved matters related to continued contracting with the Drug Enforcement Agency (DEA). At that time, I also presented my own idea for an artificial intelligent-based training package to train DEA agents using scenarios from actual court testimonies. During these presentations, I showcased all of EWA's capabilities and described in detail the proposed training package. To this day, EWA Corporate level officials, such Doug Armstrong (888 EWA-0002) still comment on my ability to take a fairly complex subject, explain it in acceptable terms to the wide range of audience backgrounds, and field an array of totally unexpected questions and concerns somewhat unrelated to the topic under discussion.

• Identified the curriculum and wrote the Instructor/Lesson Guide for CMD Technology, Inc., SCSI RAID Controller for the Army (1995). The final product was delivered to the customer and met all requirements satisfactorily.

• Created and taught multiple iterations of an intermediate level Domain Engineering course for the Air Force.

• Served as PM (Work Group Leader) (perform oversight) for an IR&D Project I was awarded funding (initial $25K - designed curriculum, developed course, coded content; received additional $33K to present via WWW) via EWA to present this course as CBT.

• Wrote Training Plans, Evaluation Procedures, and Teaching Strategies for two Quality Systems (i.e., ISO 17025) (Quality Control Review).

• Coordinated and supervised training teams in developing technical course materials and identifying teaching strategies.

• Conducted assessments of training programs and documented improvements for upper management.

• Developed the on-line, web-based courses (i.e., NVLAP Trainer, BEWT Main Menu).

• Designed and coded the Graphical User Interface to the BEWT System.

Galaxy Global Corporation	**10/1991 - 3/1992**
Fairmont, WV US	**Hours per week: 40**
Software Engineer	

• Authored the Library Operations Policies and Procedures Manual.
• Organized training for CARDS Program.
• Developed Component Metrics

Halliburton NUS Environmental Corporation	**5/1991 - 9/1991**
Rockville, MD US	**Hours per week: 40**
Scientific Program Analyst	

• Responsible for maintaining NUS' PRA Level 1 PC Workstation Nuclear Utilities Probabilistic Risk Assessment (NUPRA) program by coding enhancement in C++, including problem solving/ resolution and writing user documentation.

Monongalia County Board of Education	**8/1990 - 6/1991**
Morgantown, WV US	**Hours per week: 16**
Substitute Teacher	

• Assisted teachers in incorporating computers and software into their courses, as courseware.
• Performed duties of Substitute Teacher at Secondary Education level.

West Virginia University	**6/1990 - 6/1991**
Morgantown, WV US	**Hours per week: 24**
Graduate Research Assistant	

• Developed, and programmed a student records database for the Human Resources and Education College.

West Virginia University	**6/1989 - 6/1990**
Morgantown, WV US	**Hours per week: 24**
Graduate Teaching Assistant	

• Ran the microcomputer lab (i.e., opening and closing the facility, reserving lab equipment, setting up equipment, monitoring viruses, enforcing policies and procedures, maintaining the network, and keeping hardware/software running).
• Consulted students and faculty
• Taught development workshops and modules required by the state for teacher certification.

Shippensburg University   **8/1988 - 6/1989**
Shippensburg, PA US   **Hours per week: 24**
Instructor of Computer Science
• Instructed undergraduate courses in computer literacy, microcomputer BASIC, and algebra.

Pennsylvania State University   **8/1987 - 6/1988**
Altoona, PA US   **Hours per week: 24**
Instructor of Computer Science
• Instructed undergraduate courses in computer literacy, introductory programming in Watfiv FORTRAN and Pascal, and advanced assembler courses.

West Virginia University   **6/1985 - 8/1987**
Morgantown, WV US   **Hours per week: 24**
Graduate Teaching Assistant
• Instructed undergraduate introductory laboratory courses in IBM Assembler, VAX MACRO Assembler, and PL/I.

United States Department of Energy   **8/1984 - 6/1985**
Morgantown, WV US   **Hours per week: 24**

Computer Programmer
• Provided expertise in application programming for experimental research. Major works included Transmissometer Data Analysis programs and the MIE Scattering Interactive programs.

PROFESSIONAL PUBLICATIONS

• **"An Experienced-Based Optimization of the Goal/Question/Metric Paradigm," University of California's Irvine Research Unit in Software and the University of Southern California's Center for Software Engineering, 30 March 95**.
● **"Assessing the Factors Affecting West Virginia K-12 Teachers' Use and Non-Use of Lesson Plans Published on the Internet," accepted for publication by the Association for the Advancement of Computing in Education and presentation at SITE 2005--Society for Information Technology & Teacher Education International Conference, March 1-5, 2005.**
● **"Assessing the Factors Affecting West Virginia K-12 Teachers' Use and Non-Use of Lesson Plans Published on the Internet," submitted for publication in Computers in the Schools, the Journal of Technology & Teacher Education, and/or the Journal of Research on Computing in Education.**

BUZZ WORDS

• Battle Force Tactical Training (BFTT) Electronic Warfare Trainer (BEWT), Battle Force Tactical Training (BFTT), C++, Capability Maturity Model (CMM), Common Criteria Testing Laboratories (CCTL), Comprehensive Approach to Reusable Defense Software (CARDS), Computer-Assisted Instruction (CAI), Computer-based Instruction (CBI), Configuration management (CM), DADAP, Database, Domain Engineering (Domain Scoping, Domain Analysis, Domain Design, Domain Management, Domain Implementation), DOT files, Electronic Warfare (EW), Factory Acceptance Test (FAT), Feature Oriented Domain Analysis (FODA), Goal/Question/Metric (G/Q/M), HP-Unix, Hyper Text Mark-up Language (HTML), IEEE Standards, Independent Verification and Validation (IV&V), Instructional Design, Information Assurance Review (IAR) Plans and Procedures (P&P), Interactive Computer Education, Interactive Disassembler (IDA), Internet, ISO-9000, KPAs, Learning Content Management Systems (LCMS), Learning Management Systems (LMS), Library Administration, Local Area Network (LAN), Management, Metrics, Mil-STDs, Motorola Processor (MPC860), National Information Assurance Partnership (NIAP), National Institute of Standards and Technology (NIST), National Voluntary Laboratory Accreditation Program (NVLAP), Network administration, NSA, Nuclear Utilities Probabilistic Risk Assessment (NUPRA), Object Oriented Design (OOD), ODM, Personal Management Tracking System (PERMATS), PowerPC, Proposal Writing, Qualified Product List (QPL), Quality Manual/System, Reuse, Risk Assessment/Management/Mitigation, Site Acceptance Test (SAT), Software Engineering, Software Metrics, Software Optimization and Reuse Technology (SORT), Software Reliability Engineering, Standard Generalized Markup Language (SGML), Synthesis, Technical Writing, Testing, Training, Webertise, Windows (95, 98, NT), World Wide Web (WWW), and Verification and Validation (V&V).

COMPUTER EXPERIENCE

Operating Systems:
• DOS, HP-UX 10.x, Linux, Sun Solaris, Unix, VAX VMS, Windows (95, 98, Me, NT, XP).
Databases:
• Adabase, d Base II, Empress Informix, Microsoft Access, Microsoft SQL Server, Oracle, Pervasive, and Sybase.
Languages:
• Ada, Apple BASIC, C, C++, COBOL, dBase III, FORTRAN 77, GKS, GPSS, GW-BASIC, HTML, HyperCard, HyperTalk, IBM 360/370 Assembler, IBM BASIC/BASICA, Java, JCL, MACRO-11 Assembler, Microsoft QuickBASIC, Modula 2, Pascal, Perl, PL/I, Smalltalk, Terripan LOGO, Turbo Pascal, VAX BASIC, VAX Command Language, VAX MACRO Assembler, Visual Basic, and Watfiv FORTRAN IV & V.
Software:

- Adobe Acrobat Professional, Apple Scan, AT&T Frame-Creation System (VideoTex), Bank Street Writer, BioStat, BITNET, CompuServ, Corel DRAW, Cricket Graph, DataDrill, The Interactive Disassembler (IDA), Dynamic Object Oriented Requirements System (DOORS), EpiStat, Excel, First Choice, FrameMaker, Franklin Planner, Hyper Scan, LaserWrite (Interactive Videodisc), Lotus 123, LotusNotes, LView Pro, MacDraw II, MacDraw, MacWrite, McCabe IQ Suite, Microsoft Access, Microsoft Excel, Microsoft PowerPoint, Microsoft Project, Microsoft SharePoint, Microsoft Visio, Microsoft Word, MyStat, Norton Utilities, PageMaker, Paint, PC Tools, PILOT, ProComm, Prodigy, Q-Modem, Rationale RequisitePro, Ready Set Go, SASS, ShadeTree, Silver Platter ERIC, SmartDraw, StatView, Super Paint, SuperTrace Plus, SyBase (APT Workbench), Webster's New World Writer, West Virginia Microcomputer Educational Network, WordPerfect, Writing Assistant, WS_FTP32, and WWW Browsers (Netscape, IE).

Hardware:
- VAX/VMS, UNIVAC IBM 360/370, CRAY Super Computer, LSI-11, LSI-1123, PRO 350/360, Berkley UNIX, Wylbur, CMS IBM 360/370, TI-99/4A, MS-DOS, OS/2, IBM PC, IBM PS2 (and IBM compatibles), Macintosh Plus, Macintosh SE, Apple DOS, Apple ProDOS, Apple.

AFFILIATIONS
- ISACA Member, 2013-Present
- National Defense Industrial Association (NDIA) Member, 2008-Present
- American Society for Quality (ASQ) Member, 2006-Present
- Project Management Institute (PMI) Member, 2005-Present
- Phi Delta Kappa (PDK), Member, 2004-2010
- American Chemical Society (ACS) Member, 1981-1985

JOB RELATED TRAINING
- **DISA DoD PKI and NSS PKI Registration Authority (LRA/RA/KRA) Training 11/03-04/2020**
- DISA Risk Management Executive RMF Course for Implementers & Assessors 09/12-16/2016 and 02/03-07/2020.
- DISA Security Readiness Review (SRR) Walk-through for Traditional 01/11-15/2016
- DISA Security Readiness Review (SRR) Walk-through for Applications 12/14-18/2015
- DISA Security Readiness Review (SRR) Walk-through for ACAS 04/29-05/01/2015
- DISA FSO DoD IA Boot Camp 01/14-17/2013
- DISA FSO Security Readiness Review (SRR) Walk-through for UNIX 06/25-29/2012 PASSED!
- DISA FSO Security Readiness Review (SRR) Walk-through for WINDOWS 07/16-20/2012 Missed by 2 points.
- HOUSE PROPOSAL WRITER'S TRAINING 9/18/2010
- ICM INTEGRATED CONFIGURATION MANAGEMENT (CMMI®) 10/26/2009
- BM0049 ORGANIZATIONAL CONFLICT OF INTEREST - OCI AWARENESS 7/22/2009
- SERVICE ORIENTED ARCHITECTURE (SOA)-BASED OPERATIONS CENTER (SBOC) INTERNAL RESE 12/15/2008
- PM FORUM - THE SAIC PMP CREDENTIAL TRAINING PROGRAM 12/10/2008
- ITIL3 ITIL FOUNDATIONS V3.0 TRAINING 11/11/2008
- IESTT SYSTEM & SOFTWARE ESTIMATION TECHNIQUES (CMMI®) 10/22/2008
- IESTI INTRODUCTION TO SYSTEM & SOFTWARE ESTIMATION (CMMI®) 10/21/2008
- OPF/D ORGANIZATIONAL PROCESS FOCUS & DEFINITION (CMMI®) 8/14/2008
- IRDMO INTEGRATED REQUIREMENTS DEVELOPMENT & MANAGEMENT OVERVIEW (CMMI®) 7/30/2008
- CMMIOM SAIC CMMI® OVERVIEW FOR MANAGERS 7/8/2008
- H-18 DEFECT PREVENTION / ROOT CAUSE ANALYSIS & RESOLUTION 1/29/2008
- PDH146 IN-PROCESS REVIEW (IPR) OVERVIEW 10/30/2007
- ICM INTEGRATED CONFIGURATION MANAGEMENT (CMMI®) 9/20/2007
- H-3 PROCESS PERFORMANCE & PRODUCT QUALITY MEASUREMENTS (CMMI® LEVEL 4 METRICS) 9/6/2007
- PDH138 USING MEASUREMENT TO TRANSLATE BUSINESS VISION INTO OPERATIONAL SOFTWARE STRATEG 8/22/2007
- H-20 STATISTICAL MANAGEMENT OF A PROCESS 7/25/2007
- H-6 PROCESS AUDITS OVERVIEW 7/17/2007
- ET1115 10 SOFTWARE PROCESS IMPROVEMENT TRAPS TO AVOID 7/11/2007
- H-17 SNSG COMMON APPROACH IMPLEMENTATION FOR CMMI® 7/11/2007
- H-14 SNSG QUALITY SYSTEM (PROCESS FRAMEWORK) 7/10/2007
- H-16 FORMAL DECISION MAKING 7/2/2007
- FTP14 FTP TRAINING QUANTITATIVE MANAGEMENT 6/4/2007
- SC0073 RECOGNIZING CONFLICTS OF INTEREST [ETH221-A70EN] 6/4/2007
- ET1110 "SYS 502: DEVELOPING INTEGRATED, EXECUTABLE ARCHITECTURES" 6/2/2007
- ET1098 APPLICATION KNOWLEDGE CAPTURE: A METHOD FOR PREVENTING THE LOSS OF CRITICAL IT K 5/15/2007
- ET1097 BEST PRACTICES INTEGRATION: ITIL + SIX SIGMA 5/8/2007
- CMMI® Version 1.2 and Beyond (PDF) 5/7/2007
- 61AUD QUALITY AUDIT TRAINING 5/7/2007
- ET1091 RIGHT-SIZING PROCESSES AND MAXIMIZING PRODUCTIVITY 3/28/2007
- ET1086 BALDRIGE CRITERIA FOR PERFORMANCE EXCELLENCE CHANGES 2007 3/5/2007
- PDH126 CMMI® - CONFIGURATION MANAGEMENT INSIGHTS 2/14/2007
- IT0067 INTRODUCTION TO ENGINEERINGEDGE(TM) 1/10/2007

- FTP02 FTP TRAINING QUALITY ASSURANCE 11/13/2006
- FTP01 FTP TRAINING PROCESS OVERVIEW 10/24/2006
- FTP04T FTP TRAINING PEER REVIEWS T-T-T 10/5/2006
- PDH114 SEAY BU LMS OVERVIEW 9/21/2006
- FTP01T FTP TRAINING PROCESS OVERVIEW T-T-T 9/12/2006
- FTPEE FTP TRAINING - INTRO TO ENGINEERING EDGE 9/7/2006
- PF0806 PROJECT MANAGEMENT FORUM - SE CORE OVERVIEW 8/22/2006
- Summary_Of_CMMI_V1.2_Changes (PDF) 8/18/06
- SCAMPI_V1.2_Changes (PDF) 8/18/06
- CMMI_V1.2_Upgrade_Training (PDF) 8/18/06
- CMMI_V1.2_Upgrade_Training (PDF) 8/18/06
- CMMI_V1.2_Model_Changes (PDF) 8/18/06
- CMMI_V1.1_Sunset (PDF) 8/18/06
- IMP INTEGRATED MEASUREMENT FOR PRACTITIONERS (CMMI®) 5/23/2006
- QA1005 QUALITY ASSURANCE AND PERFORMANCE-BASED ACQUISITIONS 5/10/2006
- ST SOFTWARE TEST PROCESS (CMMI®) 5/4/2006
- IPRP INTEGRATED PEER REVIEW PROCESS (CMMI®) 3/30/2006
- BU1017 RISK MANAGEMENT AND SG-20 3/23/2006
- BD1001 BUSINESS DEVELOPMENT - INTRODUCTION TO PROPOSALS 2/28/2006
- ICMO INTEGRATED CONFIGURATION MANAGEMENT OVERVIEW (CMMI®) 2/23/2006
- BU1006 BOE DEVELOPMENT OVERVIEW 2/21/2006
- ICM INTEGRATED CONFIGURATION MANAGEMENT (CMMI®) 2/14/2006
- IMMTS INTEGRATED MEASUREMENTS FOR MANAGERS & TECHNICAL STAFF (CMMI®) 2/9/2006
- DD2004 AN INTRODUCTION TO DATADRILL PROJECT LIFECYCLE MANAGEMENT 2/8/2006
- CAG SAIC COMMON APPROACH GUIDANCE FOR CMMI® 2/1/2006
- 7Q1054 AGILE ESTIMATE AND PLANNING 1/26/2006
- BU1011 PROJECT CLOSEOUT 1/17/2006
- BU1041 CLIENT ASSESSMENT OVERVIEW 12/22/2005
- BU1009 PROJECT STARTUP 12/7/2005
- SREM2O SW RQMTS ENGR & MGMT (V2) OVERVIEW 11/30/2005
- BU1005 PROJECT MANAGEMENT PROCESS AND PROCEDURES OVERVIEW AND TAILORING 11/29/2005
- TTF115 TECHNICAL TRAINING FORUM 11/22/2005
- TF1105 TECH FORUM: MEASUREMENT OF REQUIREMENTS INSTABILITY 11/17/2005
- BU1031 DATA MANAGEMENT PROCEDURES OVERVIEW 11/10/2005
- BU1029 QUALITY ASSURANCE PROCEDURES OVERVIEW 11/8/2005
- TF0905 TECH FORUM: KNOWLEDGE ENGINEERING 9/5/2005
- BU1006 BOE DEVELOPMENT OVERVIEW 8/19/2005
- BU1018 CAUSAL ANALYSIS AND RESOLUTION 8/18/2005
- CMMI-1 GENERIC SCAMPI APPRAISAL TEAM TRAINING 8/9/2005
- CMMI® SEI INTRODUCTION TO THE CMMI 8/2/2005
- BU1021 DECISION ANALYSIS AND RESOLUTION 7/26/2005
- BU1024 ARCHITECTURE CONCEPTS OVERVIEW (SE-AO) 7/25/2005
- PF630 PROJECT MANAGEMENT FORUM: PMR TEMPLATE FOLLOW-UP 6/30/2005
- TF0605 TECHNICAL FORUM: ARCHITECTURE SOLUTIONS PART 2 6/23/2005
- PF622 PROJECT MANAGEMENT FORUM: PMR TEMPLATE 6/22/2005
- BU1031 DATA MANAGEMENT PROCEDURES OVERVIEW 6/9/2005
- BU1030 CONFIGURATION MANAGEMENT PROCEDURES OVERVIEW 6/8/2005
- BU1029 QUALITY ASSURANCE PROCEDURES OVERVIEW 6/7/2005
- BU1010 PROJECT EXECUTION AND CONTROL 5/26/2005
- BU1038 DOMAIN ENGINEERING PROCEDURE (SE-DE) 4/26/2005
- RM0405 INTRODUCTION TO RISK MANAGEMENT FOR ORLANDO INCOSE 4/22/2005
- OSW419 PDH: SOFTWARE ENGINEERING PROCEUDRES OVERVIEW 4/19/2005
- HS0405 HEALTH SEMINAR: CONFLICT RESOLUTION WORKSHOP 4/13/2005
- OQA412 QUALITY ASSURANCE 4/12/2005
- BU1009 PROJECT STARTUP 4/5/2005
- ET1001 BOTTOM-LINE MANAGEMENT TRAINING 4/2/2005
- CMMIOS SAIC CMMI® OVERVIEW FOR STAFF 3/30/2005
- GEN330 PDH: TS BU PEER REVIEWS 3/30/2005
- OSY329 PDH: SYSTEM ENGINEERING PROCESS OVERVIEW 3/29/2005
- IQA INTEGRATED QUALITY ASSURANCE (CMMI®) 3/23/2005
- PR0033 INTEGRATED QUALITY ASSURANCE OVERVIEW (CMMI®) 3/23/2005
- OQA310 CONFIGURATION MANAGEMENT 3/10/2005
- BU1029 QUALITY ASSURANCE PROCEDURES OVERVIEW 3/8/2005
- OSY215 DRA TOOLS 2/25/2005
- OSW225 CASUAL ANALYSIS AND RESOLUTION 2/22/2005
- OSY205 PDH: TECHNICAL FORUM 2/18/2005
- OSW215 PDH: SOFTWARE ENGINEERING PROCEUDRES OVERVIEW 2/15/2005
- GPT GOVERNMENT PROPERTY GUIDELINES TRAINING 2/9/2005
- OPI219 T&SS BU METICS AND QPM APPROACH 1/28/2005
- HP-UX 10.x System Administration for HP 9000 Systems, 1997
- Motivating Employees - The Solution to the Puzzle, 1995
- Risk-Focused Prevention Programs -- Grant Writing Seminar, 1995
- Rural Area Mini-Grant Program, 1995

REFERENCES

Mr. Arnold Enfusse

Chief, DODIN Command Cyber Readiness Inspection Branch (JD31)
(Retired)
DODIN Defensive Cyber Operation Assessment Division (JD3)
DODIN Readiness and Security Inspections (DRSI)
Joint Force Headquarters DoD Information Network (JFHQ-DODIN)

Phone Number: Personal Cell: 717 360-3859
Email Address: N/A

Mr. James T. Lynch

Chief, Ecosystem Accreditation Section (SEL721) (Retired)
SE/ECO/CyLOB
DISA Mechanicsburg

Phone Number: N/A
Email Address: Personal: jtlynch2@hotmail.com

Mr. Nicholas L DePatto

DODIN Command Cyber Readiness Inspection Branch (JD31)
DODIN Defensive Cyber Operation Assessment Division (JD3)
DODIN Readiness and Security Inspections (DRSI)
Joint Force Headquarters DoD Information Network (JFHQ-DODIN)

Phone Number: 717 267-9249
Email Address: Nicholas.L.DePatto2.civ@mail.mil

Mr. Richard M. Klein

PKI Auditor
Defensive Cyber Operations Access Control Inspection Branch (RS32)
DoDIN Readiness & Security Inspections (DRSI)

Phone Number: 301 225-6230
Email Address: Richard.M.Klein8.civ@mail.mil

Mrs. Donna K. Gutshall

Plans and Operations Branch (JD12)
DODIN Defensive Cyber Operations (DCO)
Analysis & Reporting Division (JD1)
JFHQ-DODIN Readiness and Security Inspections (DRSI)

Phone Number: 717 b267-9635
Email Address: Donna.K.Gutshall.civ.mail.mil

Mr. Timothy Hershey

PKI Auditor
Defensive Cyber Operations Access Control Inspection Branch (RS32)
DoDIN Readiness & Security Inspections (DRSI)

Phone Number: 717 267-9561
Email Address: Timithy.R.Hershey.civ@mail.mil

Mr. George Connors

DISA REB

Phone Number: 717 267-9391
Email Address:

Mr. Robert Shipp

USARMY USAMC (USA)

Phone Number: 717 267-4115
Email Address: Robert.E.Shipp2.civ@mail.mil

Mr. Patrick Theeke

TASC PM
L-3 Communications, Inc
Program Manager / L-3 Chief

Phone Number: Cell: 304 376-9294
Email Address: theekep@gmail.com

Ms. Anita Carlos

Director of Quality Assurance

Phone Number: N/A
Email Address: ANITA.K.HENDERSON-CARLOS@saic.com

ADDITIONAL INFORMATION

AWARDS
- **Selected for the 2019 Cyber Technical Innovators Program ($5000) 8/10/2018.**
- **DEFENSE INFORMATION SYSTEMS AGENCY OUTSTANDING TEAM Award [to FS4 (ESD Net Assurance Implementation Planning Team)] 4th Quarter 2012.**
- **First Place Winner of the 2006 IPG Process Improvement Award ($1000), 3/15/2006.**
- **Competitive Outstanding Research Award $250, West Virginia University PDK Chapter, 12/8/2004.**
- **Outstanding Doctoral Dissertation Award $500, Phi Delta Kappa International, 11/11/2004.**

DISSERTATION
- Assessing the Factors Affecting West Virginia PreK-12 Teachers' Use and Non-Use of Lesson Plans Published on the Internet, 2004

ACCOMPLISHMENTS
- Contributed as key training presenter in three major Company Proprietary marketing briefings at EWA CEO and EWA Vice-President level, Nov-Jan, 1998.
- Played major role as a member of the EWA-Fairmont team in developing and winning four contracts from the West Virginia High Technology Consortium/Foundation. Ensured proposal writing process and contributed as a writer addressing key challenges concerning documentation updates, Workshop scheduling, the Training Plan, and the Metrics Report.

Abbreviated "targeted" (computer scientist, program management, software engineering, process engineering, technical editor, quality assurance, metrics analyst, testing engineer, training & education) resume available upon request.