IT Specialist IT Specialist IT Specialist, GS-11 (INFOSEC), Civil Service - Dept. of the Army Fort Belvoir, VA Work Experience IT Specialist Department of the Army - Fort Belvoir, VA October 2017 to Present April 28, 2019 to Present. RNEC-NCR, Fort Belvoir, Virginia Job Title: IT Specialist (INFOSEC), GS-2210-11 Job Description: Serves as COMSEC Account Manager for the Command. Responsible for ensuring compliance with established Army regulations, policies and procedures. Supervises the regulatory control of COMSEC accounts, to include the receipt, accountability, and dissemination of COMSEC materials to sub-accounts of the command. Ensures that COMSEC accounts are safeguarded from possible vulnerabilities by developing and implementing the integration of security programs for protecting the command's accounts. October 30, 2017 to April 27, 2019 RRMC IT Specialist (SYSADMIN), GS-2210-11 Job Description: Helpdesk night shift watch supervisor providing Remedy ticket support, IT support, Trusted Agent PKI support and National Gateway Center (NGC) messaging support for the 114th Signal Battalion (BN). Serve as a senior Tier-1 technician within the Network Enterprise Center (NEC) providing installation customers a single point of contact in resolving computer and network related issues. Support changes to customer services including installation and configuration of hardware and software for personal computer (PC) equipment. Document assistance calls in the Information Technology Service Management (ITSM) Remedy system and provide first tier support to customers in multiple areas of information management to include PC, office automation software, general office automation equipment, email, telecommunications, Local Area Network (LAN) services, and specialized applications. Responsibilities include providing Windows 10 Virtual Desktop Infrastructure (VDI), NIPRNET, SIPRNET network environment system administration, service desk and BMC Remedy ticket support. Training System Support Center (TSSC) System Administrator LB&B Associates Inc - Oak Harbor, WA December 2018 to January 2019 Oak Harbor, Washington. Job Title: Training System Support Center (TSSC) System Administrator Job Description: Provide Maritime Communications support for the P-8 Poseidon TSSC at NAS Whidbey Island, Washington. Maintain, administer and provide technical support for operating systems within the respective site IAW with mandated DoD cybersecurity requirements and DoD IA workforce requirements (Appendix G OS Commercial Certification Guidance, SECNAV M-5239.2, and SECNAV M-5239.2 Appendix 4). Provide System Administrator and Information System Technician support in the areas of: Customer Service and Technical Support, Data Administration, Knowledge Management, Network Services, System Administration, and Systems Security Analysis. Maintain and support the following Operating System Software Programs in an operational computer network environment: Data ONTAP, Linux Red Hat, Linux Red Hat Enterprise, Microsoft Exchange Server, Microsoft SQL Server, Microsoft Windows Operating System, Microsoft Windows Server, VMware Server, Brocade v1.11, CISCO v15.0, DIGI v1.9.5, FortiOS 4.0, HP/3Com v2.5, SedNet 1394 (x). Monitor, maintain and install networking equipment including switches, routers and firewalls. Perform hardware and software installation in a client/server environment. Perform routine maintenance, to include diagnostic testing and optimization. Assist Government IA personnel in the configuration and sustainment of the Host Based Security System (HBSS) and the DoD Assured Compliance Assessment Solution (ACAS). Utilize ACAS and HBSS to execute and analyze vulnerability scans upon request by Government IA personnel. Coordinate and implement software backup and antivirus IAW with DoD IA requirements. Perform scheduled IA specific preventive maintenance of computer systems and network components IAW applicable Cyber Security instructions and practices (e.g., DoDI 8570.01-M; CJCSM 6510.01: IA and CND; SECNAV M-5239.1 series 2005 DON IA Program IA Manual; and DoDI 8500.2 series - IA Implementation documentation). RMF Assessor, Contractor Infotree Inc. and KBRWyle Inc September 2018 to October 2018 September 17, 2018-October 7, 2018 Infotree Inc. and KBRWyle Inc., Norfolk, VA Job Title: RMF Assessor Job Description: Perform assessment and authorization tasks, such as supporting CNIC/NAVY process and procedure development. Provide support as a primary liaison with CNIC (Commander Naval Installation Command) for assessment and authorization (A&A) efforts. Conduct cybersecurity analysis in preparation for assessment and authorization, including: technical information security aspects, identifying risks, providing mitigation plan of actions. Analyze system designs, assist with assessment and authorization issues that could prevent a system from receiving authorization. Develop custom mitigation solutions for information system vulnerabilities.

Assessment and Authorization: Identify key stakeholders in the assessment and authorization effort for medical systems and networks and work with them to confirm that the system documentation reflects the current security configuration of the system, in terms of hardware and software components, data flow, interconnections, and ports, protocols, and services. Identify potential risks associated with the configuration of the system and appropriate mitigation strategies. Conduct status meetings and determine next steps in moving systems toward a successful accreditation effort. Work with the cybersecurity team to develop and implement a detailed test plan and review findings from self-assessments to determine readiness for independent assessment. Conduct manual checks of assigned systems during independent testing and report findings in a plan of action and milestones (POA&M) document. Utilize automated tools and eMASS experience and knowledge to capture and report test results. Assist system owners and system administrators in interpreting and applying mitigation strategies. Independent Validation and Verification (IV&V): Conducts in-depth analysis of IV&V and functional/operational test results for accuracy, compliance, and adherence to DoD and Federal cybersecurity technical and operational security requirements. Document residual risks by conducting a thorough review of all the vulnerabilities, architecture, and defense in depth and provides the cybersecurity risk analysis and mitigation determination results for Test Reports. Assist Validators with producing the risk assessment artifacts describing residual risks identified during certification testing. Schedule and conduct eMASS training for CNIC and Program Office personnel. Develop/maintain agency level cybersecurity policy and processes that implement DoD Cybersecurity program. Utilize NIST publications to work strategically on transition of DIACAP to RMF. Provide extensive information assurance support with DISA STIGs/FDCC requirements, defense-in-depth, and other information security and assurance principles and associated supporting technologies. Risk Assessment: Communicate the security posture of systems up the chain of command via CSTAR and eMASS to ensure that accreditation decisions can be made based on a thorough understanding of the risks associated with the particular configuration of systems and networks. Identify strategies for improving the assessment and authorization processes and procedures to meet increasingly tight timelines and budgets.

E-commerce Manager TAOD LLC - Everett, WA December 2014 to December 2017 Job Description: Self-Employment-Develop online business strategy in collaboration with product and marketing managers. Identify products, source products and conduct market research on prices and policies for online product sales. Identify target markets for eCommerce initiatives and develop marketing campaigns to attract more visitors and increase online sales. Work with designer's website developers and content providers, to create or improve the eCommerce site. Ensure that the site is easy to use and navigate, and that it includes all the functions that visitors need to select order and pay for products. Stay up to date with Web technology, introducing additional functionality, such as product videos, to enhance the site; work with payment providers to develop payment mechanisms that are secure and that protect customers' personal details when they pay by debit or credit card. Ensure that any stored customer data is secure against threats from cyber criminals. Maintain a high level of system security to prevent attacks that might disrupt service to customers. Perform site maintenance, check site content and systems regularly to ensure that they are working properly. Update prices and product information, adding new products or removing products that are no longer available. Monitor website performance, such as time for web pages to load, total numbers of site visitors, and visitors by product or page and analyze the website performance statistics information and recommend changes to improve performance. Monitor site metrics to help develop or recommend marketing programs to increase sales. Analyze metrics, such as the number of visitors who just browse, rather than place orders. Identify products that took increased revenue following a promotion, or products where sales declined following a price increase. Also, work with marketing colleagues to create campaigns that improve search engine rankings, increase traffic to the site and strengthen customer loyalty. Information Assurance Engineer (IAE) OBXtek Inc. & Ennoble First - Vienna, VA February 2016 to September 2017 Job Description: Serve as the primary security lead for High, Moderate, and Low impact systems that support Visa, Passport, American Citizen Overseas or Certification Authority for major applications. Provide support for the overall Assessment and Authorization (A&A) life-cycle process in accordance with the Department of State CA/CST System Development Life-Cycle (SDLC) and including the following functional areas.

Security Guidance: provide guidance to System Government Task Managers (GTM) and System developers supporting the RMF A&A process using both the National Institute of Standards and Technology (NIST) Special Publication (SP) 800 series and Department of State Foreign Affairs Manual (FAM) guidelines. Assist and advise system GTMs and system developers in the design and development of secure systems architecture as well as industry best practices and information systems technologies available to meet AIS security requirements. Authorization to Operate: Gather required information to support system authorization by organizing technical working groups, conducting fact-finding interviews, attending system demos, assessing system security categorization levels, establishing system security control baselines, and acting as a security advisor to the system's GTM during the security controls implementation phase. Develop and update the following system security documentation which is maintained within the Consular Affairs Certification and Accreditation Management System (CACAMS): Security Categorization Form (SCF), E-Authentication Form (eRA), System Security Plan (SSP), Information System Contingency Plan (ISCP), and Privacy Impact Assessment (PIA). Continuous Monitoring: monitor assigned systems weekly, conduct weekly or monthly meetings with GTMs and developers. Schedule and facilitate boundary meetings, RMF step 1-3 Kick-off meetings, RMF step 6 Kick-off meetings, and attend RMF step 4 Kick-off and POA&M meetings. Plan of Action and Milestones (POA&M): review, monitor, and report system POA&M status to all stakeholders including PM, ISSP GTM, System GTM, System Development Team, and System Operations Teams. Coordinate with appropriate personnel to ensure that POA&Ms are remediated in a timely manner and report closed findings to the POA&M Manager. Assign and track POA&M findings via Remedy Tickets. Configuration Management: analyze, complete and submit Configuration Change Requests (CCRs) by conducting security impact analysis and initiating required actions to maintain security posture and ATO status. Skills: Information System Security Analysis; RMF 1-3 Analysis and support; SSP development and analysis; POA&M analysis; Remedy ticket support; Configuration Change Request (CCR) support and analysis. Information Assurance Specialist, Contractor ManTech International February 2016 to February 2016 February 1, 2016-February 8, 2016 ManTech, Stafford, Virginia Job Title:

Information Assurance Specialist Job Description: Perform work as an ISSO to research, develop, implement, test and review an organization's information security posture to protect information and prevent unauthorized access. Inform users about security measures, explain potential threats, install software, implement security measures and monitor networks. Cyber Security Watch Officer Newberry Group - Columbia, MD November 2015 to December 2015 Job Description: Identify and manage internal and external all-source Military Operations, including both analytical and collection requirements from across the Military Operations community. Report to the Survey Analysis Center Chief and work alone or with DOD civilians and military personnel performing activities in one or more of the following and/or related areas: interface with other offices and agencies to ensure the timely and effective completion of tasks, identify target requirements and task them to the appropriate collection elements and verify that responses meet requirements. Incident Response/Threat Intrusion Analyst BAE Systems Intelligence & Security - McLean, VA August 2015 to November 2015 Job Description: At the MWEOC SOC responsibilities included providing 24/7 incident management support tracking all reported security events/incidents, incident escalation, incident resolution and reporting of events/incidents using proper procedures. Prepared and provided develop ed assessments and reports, documenting weekly trends of incidents, and security events. Coordinated strategic analysis in support of computer security incidents by utilizing McAfee ESM and SEN tickets to help to identify patterns in reported compromises and identify additional threats as part of the same incident. Provided assistance to senior personnel in performing forensic analysis of digital information and physical evidence and provided specialized support by gathering, handling, examining, preparing, entering data, searching, and retrieving, identifying and/or comparing digital and/or physical evidence. Utilized forensic procedures to determine results and observed proper evidence custody and control procedures, documented procedures, security findings and prepared comprehensive written notes and reports. Analyzed network/computer threats and mitigated vulnerabilities while limiting operational impact. At the FEMA MWEOC SOC I applied Federal, DOD, and industry information security requirements, and standards, and working knowledge of best practices, network architectures, current networking technologies, security requirements and features of networks and applications to defend FEMA networks. These activities included: vulnerability assessment, anti-virus administration, DISA STIGs, windows server update services, IDS/IPS configuration/monitoring, E-Mail security, firewalls, TCP/IP packet analysis, log analysis, IT standards; including but not limited to the OSI model, and the methods of exploiting those standards to provide analysis support for incident response and related security issues. Skills: CND, Computer Security, Network Analysis, Network Security, and Incident Response. Cable Technician, Contractor Insight Global July 2015 to August 2015 July 31, 2015-August 2, 2015 Insight Global, Woodinville, Washington Job Title: Cable Technician Job Description: Responsible for cabling the back end of servers, arranging equipment accordingly, racking and stacking servers and switches into cabinets and conducting checks for proper mounting; labeling cables and unboxing packages and putting hardware equipment in the correct location. Continuous Monitoring Analyst L-3 NSS - Alexandria, VA May 2015 to July 2015 Job Description: Provided coordination, IAW O-8530.1, supporting the Trusted Agent with the local Computer Network Defense Service Provider (CNDSP) and Joint Base Pentagon tenants for external assessment activities to evaluate, obtain, maintain lessons learned, and develop after action reports to ensure remediation plans are implemented to strengthen Joint Base Pentagon's security posture. Support the government by developing a communications plan to ensure subscribers communicate with the Trusted Agent when regular external assessments and reports are distributed to the CNDSP to improve network security posture. Develop and maintain an overarching Trusted Agent Mission Portfolio (TAMP) spanning out to, but not limited to a five-year period, including all IV&V, security assessments, continuous monitoring (ConMon), and Red/Blue Team activity, which provides the backbone for all risk management strategic scheduling and resource decisions. Provide collection support for knowledge development during the planning phase to aid in the appropriate allocation of resources across the entire portfolio. Provide planning support for annual assessments, IV&V missions and unique Friendly Network Forces incidents recorded within the TAMP. Identify each SUT as a project and generate a work-breakdown structure, including: mission phases, start, completion, timelines, milestones, inch stones, resources, critical paths and risks. As directed, provide Access Control, Personal Security Control and Awareness and Training security controls audit and assessment Continuous Monitoring (ConMon) support IAW with DOD, DHS, NIST, FISMA standards, policy and regulations (CNSSI-1253, NIST SP 800-137, NIST SP 800-53, NIST SP 800-53A, NIST SP 800-37, and NIST SP 800-39) within the RMF. Skills: CND, Continuous Monitoring, IV&V. Property Investment Manager, Self-Employment Inquire Solutions Inc June 2014 to May 2015 June 17, 2014-May 3, 2015 Inquire Solutions Inc., Lorton, Virginia Job Title: Property Investment Manager Job Description: Self-Employment-Managed property investment accounts, research tax records, real estate websites and community profiles to locate real estate investment opportunities. I visited real estate properties to assess property viability for purchase as real estate investment property; Managed Rental properties, tenants, leases and coordinate with vendors and contractors to initiate repairs and maintain property. I worked with bank loan officers and realtors to apply for real estate investment loans for acquiring real estate investment properties. Contacted and worked with real estate management companies to establish rental contracts and real estate property management agreements. Managed agreements and contracts with construction contractors and subcontractors to repair and restore acquired real estate properties for resale or use as rental investment property. I also, coordinated the response to all issues reported by contracted real estate property management companies. Worked with accountants to provide all required records and receipts for tax and account management and attended real estate investor forums about real estate investment techniques and strategies. Security Control Assessor (SCA) CACI, NGA Campus East - Springfield, VA July 2012 to June 2014 Job Description: Provided program independent IA system security controls assessment; coordinated security controls and continuous monitoring assessment testing activities with all system A&A stakeholders. Conducted continuous monitoring assessments to discover vulnerabilities, malware, rogue devices, and ensure that system security controls are maintained and continue to be implemented correctly. Responsibilities included providing analysis of security controls and continuous monitoring assessment results to provide recommendations of corrective actions to reduce or eliminate system vulnerabilities for the Certification Authority (CA); also, conducting security controls assessment testing to accomplish the evaluation of the management, operation and technical security controls in information systems (IS) through inspection and formal testing. Provided analysis of security control assessment results and recommended corrective actions to reduce or eliminate system vulnerabilities to the CA. Performed Retina and SRR scans on assigned systems in a virtual machine software test environment, in support of Certification to Field (CtF) accreditation activities. Utilized Microsoft Office (Excel and Word), FileZilla, Retina, SSH, SRR, Remote Desktop and the Data Transfer Agent (DTA) applications, tools and services to perform Retina pre-scans and post-scans on assigned systems. Compared and analyzed POA&Ms, verified system fixes and patches with system administrators and Information System Security Engineer Representatives (ISSE Rep.) in a Windows XP, Windows Server 2008, Windows Server 2003, and Windows 7, Red Hat Linux, and UNIX software test environments. Upon completion of testing, verification and validation; responsibilities included the preparation of Security Certification Test Reports (SCTRs) and security certification memos that were submitted to the Certification Authority (CA) for approval of assigned systems for Certification to Field (CtF) designation. Monitored and updated the Verification and Validation Group Online Tools (VOLT) portal for Request for Service (RFS) security status and upon completion of assigned testing, updated a CERT MEMO tracker. Monitored XACTA SPIDs to track and verify the status of program ATOs, OATTs and ATCs. Monitored and assessed the security impact resulting from the installation of MEMOGRAM and TECHGRAM updates for NGA Deployed Systems (NDS) and SECGRAM and OPSGRAM updates for Integrated Exploitation Capability (IEC) systems. Prepared monthly and as-needed Simplified EZ, SECGRAM, MEMOGRAM and security certification memorandum documentation to record the security impact of minor software changes, application software updates, security patches and COTS updates on segment systems, in accordance with (IAW) governing security publications consisting of: ICD-503, DCID 6/3, DODIIS C&A guide, DJSIG, JDCSISSS, and standard operating procedures (SOP). Also, I participated in OCIO/CSIA meetings, Verification and Validation (V&V) Resource Allocation Meetings and Independent Verification &Validation meetings as assigned. Skills: Information System Security Analysis; Information System Security Testing and Evaluation; XACTA, SRR, RETINA; SCTR, and POA&M generation and analysis. Security Engineer, Contractor Telos June 2012 to July 2012 June 4, 2012-July 10, 2012 Telos, Defense Manpower Data Center, Alexandria, Virginia Job Title: Security Engineer Job Description: Provided the Information Assurance Manager (IAM) and system users with support for the proper configuration and use of information systems and provide oversight for all security-related requirements. Responsibilities included: assisting with the design or redesign of information systems, ensuring information system compliance with DOD configuration guidelines and the preparation of Certification and Accreditation documentation; monitoring all aspects of security to ensure it is maintained at acceptable levels including performing security audits, ensuring conformity of password policies and other security countermeasures and implementing other Information Assurance (IA) safeguards IAW DoD requirements. Tracked information system's IAVA compliance and assisted with or performed other IA tasks as required by the Information Assurance Manager. Additional tasks included assisting with the in-processing of new contractor hires by collecting vetting-related artifacts/documentation such as, Standard Form 85R, DLAH Form 1728, training certificates, proof of citizenship, etc. Property Investment Manager, Self-Employment Inquire Solutions Inc November 2011 to June 2012 November 24, 2011-June 3, 2012 Inquire Solutions Inc., Lorton, Virginia Job Title: Property Investment Manager Job Description: Self-Employment-Managed property investment accounts, research tax records, real estate websites and community profiles to locate real estate investment opportunities. I visited real estate properties to assess property viability for purchase as real estate investment property; Managed Rental properties, tenants, leases and coordinate with vendors and contractors to initiate repairs and maintain property. I worked with bank loan officers and realtors to apply for real estate investment loans for acquiring real estate investment properties. Contacted and worked with real estate management companies to establish rental contracts and real estate property management agreements. Managed agreements and contracts with construction contractors and subcontractors to repair and restore acquired real estate properties for resale or use as rental investment property. I also, coordinated the response to all issues reported by contracted real estate property management companies. Worked with accountants to provide all required records and receipts for tax and account management and attended real estate investor forums about real estate investment techniques and strategies. IT Specialist (GS Naval Surface Warfare Center - Dahlgren, VA August 2011 to November 2011 Q), Sensors Division (Q40), Sensor technology Branch (Q41); Dahlgren, Virginia Job Title: IT Specialist (GS-11) Job Description: Responsibilities included the development, use and application of information technology (IT) to accomplish work supporting sensor systems analysis, sensor systems safety, laboratory testing, mission assurance, and critical infrastructure analysis. Provided support for a wide range of Windows-based applications and specialized software and hardware applications related to engineering and scientific work, including the adaptation of software and hardware applications to meet specific mission needs. Responsible for conceiving, devising, implementing, testing, managing and maintaining information system structures to facilitate data backup, data storage and data analysis in a highly secure environment. Also, I provided support planning, designing, implementing, configuring, managing and troubleshooting stand-alone computers, networks, servers, and client systems. Installed and configured computers, servers, routers and supported the fabrication and routing of cables. Provided help desk support to users in a Windows 2000/2003/XP operating system software environment and a Windows Server 2003 software operations environment. Documented maintenance activities, system configuration, implemented and performed security audits of networks and computer systems. Responsibilities included preparing reports with recommendations for the study of information system methodology and possible information system alternative solutions; developed and presented short and long-range IT plans for small computer networks (5-40 computers) and stand-alone workstations. Provided system analysis and system administration support for application software, operating systems, network services, data management, and encryption services. Developed and implemented security policies and procedures in accordance with JAFAN 6/3 requirements and local security policy. Developed specifications for the acquisition of computer hardware, software and services; reviewed the adequacy of contractor proposals; and/or acted as a Contracting Officer's Representative (COR). Developed and prepared projects, studies, and evaluations which involved analytical work concerning the integration of information systems, computer programming, and computer equipment used in sensor systems, testing and laboratory environments. MDA FSET ITT Communications Division - Washington, DC June 2011 to June 2011 Job Description: Provided support for the day to day operation, maintenance, and interoperability of the MDA prototype computer system and software components in direct support of the collection, monitoring, fusion analysis, display, and dissemination of maritime related information to intelligence analysts and decision makers. These duties included, but were not limited to, periodic maintenance, to include installation and configuration of software patches, operator training, and troubleshooting identified system problems. The Maritime Domain Awareness Fleet Systems Engineer (MDA FSET) is the primary point of contact for MDA operators for all issues related to system operations and performance. Information System Security Engineer (ISSE) DigiFlight Inc - Springfield, VA September 2010 to April 2011 Job Description: Provided technical support to identify information protection needs, define system security requirements, design system security architecture, develop detailed security designs, implement system security plans, and assess information protection effectiveness at government, defense and contractor facilities. Systems supported: Windows Server 2008, Windows 7, Windows XP, Linux, UNIX, BSD operating systems; thin clients, thick clients, servers, switches and various telecommunication devices. Tools and services used: MS Office Excel, Retina, SRR scripts, DTA, Gold Disk, XACTA IA Engine, Remote Desktop, SECURE CRT, DUMPSEC, MMC security Snap-in, and Remedy. Conducted system security scans on UNIX, LINUX, and Windows operating systems utilizing SRR, Retina and Gold Disk scripts and manual checklists to identify vulnerabilities matched with DISA and CYBERCOM STIGs, IAVMs, IAVAs, IAVBs, and IAVTs. With scan results created POA&Ms for inclusion in system security authorization agreements in support of the Certification & Accreditation process in a large scale virtual machine engineering development environment. Coordinated with information assurance officers, certification engineers, information system security representatives, software engineers and systems engineers to achieve OATT, ATC and ATO approval for new systems implemented in IT architecture and IT entity virtual machine environments. Skills: Information System security analysis; Retina, Gold Disk, SRR; STIG analysis, POA&M

generation and analysis. Information System Security Representative (ISSR) DigiFlight Inc - Reston, VA February 2010 to September 2010 Job Description: Implemented automated information system security, and operational compliance with documented security measures and controls in defense, contractor and government facilities. I provided certification and accreditation (C&A) support by populating system security authorization agreements (SSAA) in the XACTA information assurance engine database to complete security plans (SPID) to meet C&A requirements for deployed systems. Coordinated with information assurance officers (IAO), information system security representative lead (ISSR), and system engineers (SE) and government personnel to resolve security issues for the completion of C&A packages for deployed systems. Submitted security plans to the information assurance officer (IAO) for submission to the designated approving authority (DAA) for approval to operate (ATO) authorization for the release of approved deployed systems to CONUS and overseas locations. Coordinated with systems engineers to analyze and upload POA&Ms to append to SSAAs and managed artifacts located in assigned XACTA SPIDs; provided continuity planning tool (CPT) support through updating information technology disaster recovery (ITDR) plans; attended meetings with operations personnel for discussing the planning, organization and practicality of disaster recovery plans and disaster recovery training scenarios. Coordinated and setup weekly C&A VTC meetings with overseas personnel to plan the coordination of the release and distribution and or removal of deployed systems and peripheral components and monitored secure chat rooms to provide on call C&A support for deploying systems worldwide in support of crisis response. Coordinated with logistics personnel to update, correct and manage an asset management database and to identify missing and incorrect system tracking data. Identified and reported discrepancies between data contained in XACTA SPIDs and asset management database entries; worked with C&A team IAOs, the C&A team ISSR team lead and logistics personnel to resolve any missing, incorrect and/or incomplete asset management and related XACTA data. Coordinated with Security Installations (SI) personnel to identify and locate physical security documents to input into XACTA SPIDs in support of the C&A process for deployed systems. I also submitted and tracked Remedy trouble tickets to resolve system problems, account problems, application problems and database problems for XACTA, CPT, ITDR, asset management systems and administrative systems, and assisted with the coordination, planning and scheduling of all daily and weekly C&A meetings. Skills: Information System Security Analysis; XACTA IA Engine C&A processing. Property Investment Manager, Self-Employment Inquire Solutions Inc September 2009 to January 2010 September 4, 2009-January 31, 2010 Inquire Solutions Inc., Lorton, Virginia Job Title: Property Investment Manager Job Description: Self-Employment-Managed property investment accounts, research tax records, real estate websites and community profiles to locate real estate investment opportunities. I visited real estate properties to assess property viability for purchase as real estate investment property; Managed Rental properties, tenants, leases and coordinate with vendors and contractors to initiate repairs and maintain property. I worked with bank loan officers and realtors to apply for real estate investment loans for acquiring real estate investment properties. Contacted and worked with real estate management companies to establish rental contracts and real estate property management agreements. Managed agreements and contracts with construction contractors and subcontractors to repair and restore acquired real estate properties for resale or use as rental investment property. I also, coordinated the response to all issues reported by contracted real estate property management companies. Worked with accountants to provide all required records and receipts for tax and account management and attended real estate investor forums about real estate investment techniques and strategies. Information Security Administration IntePros Federal - Arlington, VA July 2009 to September 2009 Job Description: Documented information systems within the Joint Staff (JS) Integration Lab environment to support certification and accreditation (C&A) for the test lab. The JSIL is the final test bed before new software/hardware is installed on the Joint Staff production systems. Created documentation to support the test effort, applied IAVA patches and hot fixes, monitored WSUS to support the continual monitoring of the JS accredited systems. Incident Handler Northrop Grumman Information Systems - Arlington, VA March 2009 to July 2009 Job Description: Reviewed and tracked detected incidents to identify new exploits, threats, mitigation strategies, and enforced incident reporting standards. Reviewed reported incidents and identified correlation with other activity through database queries and through network traffic analysis. Exchanged information and ideas; coordinate incident reports, traffic analysis, law enforcement data, and intelligence data to correlate activity, and coordinate with DOD organizations to analyze new activity and determine whether the activity is an additional incident. Maintain briefings and brief the senior leadership when requested or as necessary. Developed defensive measures to protect additional DOD assets from being compromised or to detect further compromises and reported other potential compromises to the responsible CERT. Documented pertinent information, including method of attack as well as mitigation strategies at the local and the enterprise level. Skills: DISA CENTAUR scanning and analysis, Joint CERT database ticket tracking and reporting. Computer Security Representative 4 Northrop Grumman Information Assurance Innovation Center - Millersville, MD January 2009 to March 2009 Millersville, Maryland Job Title: Computer Security Representative 4 Job Description: Applied current computer science technologies and Information Assurance requirements to review, design, develop, evaluate and integrate computer/communication systems and networks to maintain system security posture. Decomposed system specifications to determine security/IA requirements and define Certification/ Security Test & Evaluation requirements. Conducted test analysis for vulnerabilities and associated risks; coordinate with program management and customers to mitigate risk and ensure compliance with DoD/Fed IA requirements. Developed system security/IA plans under guidance in DIACAP, FISMA, NISCAP, NIST 800-53A, NIST SP 800-37 and JAFAN 6/3. System Data Technician, Contractor Solers Inc August 2008 to January 2009 August 1, 2008-January 2, 2009 Solers Inc., Chantilly, Virginia Job Title: System Data Technician Job Description: Monitored daily software and network operations in a distributed environment to provide first level software support, network support and problem resolution identification in a government facility. Duties included providing support monitoring and working with users on fault isolation and problem resolution as well as system analysis and reporting in a 24-hour shift work environment. Skills: LINUX operations. Information System Technician (IT) Office of Naval Intelligence, Directorate 4, Div - Suitland, MD May 2007 to August 2008 421, ONI INTELCOMM worldwide support; Suitland MD Job Title: Information System Technician (IT) Job Description: Provided worldwide technical logistic support to Navy and Marine Corps SPINTCOMMs, coordinated with the ONI Registry, ONI SSO Office, DCS, and the USPS to manage the shipment of DMS, COMSEC, and intelligence communication systems components to worldwide SPINTCOMM locations. Supported the installation or removal of intelligence communication systems and maintained, managed and monitored worldwide SPINTCOMM equipment inventories as well as performing DRMO and TASO duties for the ONI-421 Office and DMS Lab spaces. Skills: CompTIA Security + certification, TASO, property/asset management and logistic support for Navy SCI telecommunications and USN/USMC SPINTCOMM facilities. Information Systems Technician (IT) ISAF HQ - Kabul, AF December 2006 to April 2007 Job Description: Alternate Crypto Custodian for NATO in Afghanistan. Maintained and managed all NATO sub receipt holders CMS accounts for 1800 crypto line items and NATO COMSEC key management throughout the Afghanistan AOR. Managed EKMS key receipt and distribution and transferred digital keys from STE phones to CYZ-10 DTD for further distribution. Issued COMSEC key tape canisters and COMSEC key pads; maintained CMS record, and security clearance record databases. Loaded crypto variables, configured and provided tech support for fifty STU-IIB secure telephones, secure cell phones and TCE-621 cryptographic equipment at ISAF HQ. Established new crypto circuits, conducted monthly CMS destruction and traveled throughout the Afghanistan area of operations in helicopters, armored/unarmored coalition convoys to provide EKMS support to NATO elements. I also provided on-call COMSEC support to all NATO elements in the Afghanistan AOR. Skills: NATO CMS Custodian, EKMS experience, COMSEC circuit implementation. Information Systems Technician (IT) Combined Security Transition Command-Afghanistan - Kabul, AF May 2006 to December 2006 Kabul, Afghanistan Job Title: Information Systems Technician (IT) Job Description: Information Management Officer (IMO); completed the installation of JWICS, SIPRNET, CENTRIX and NIPRNET network components, workstations, peripheral devices and VOIP phones and provided ADP support, installing, reconditioning, updating and configuring computers for CSTC-A DOIM, CJ-6 at Camp Eggers, Kabul, Afghanistan. Supported the installation, verification, maintenance and provided tech support for the PKI system throughout Camp Eggers in accordance with DOD requirements; conducted nightly physical security checks, network/software applications trouble-shooting, added users to MS Outlook security groups, performed weekly and monthly database backups; coordinated with the IT help desk and system users to resolve network, computer and software Remedy tickets. As directed by CJ6 DOIM, I provided coordinated support with vendors and customers for the ordering, receipt, distribution and installation of new computers, peripheral equipment, network equipment and software products. Also, on a weekly basis, I provided technical support for Staff Information Work Space (IWS) conferences and management support for the Camp Eggers contract office by managing Afghan contractors who performed printer/photo-copy maintenance. I investigated facilities outages and worked with contractor personnel to trouble-shoot, repair and maintain electrical, plumbing and HVAC systems in buildings at Camp Eggers. In the DOIM office, I provided telecommunications technician support through the maintenance, configuration and distribution of IRIDIUM satellite phones, Thuraya satellite phones, GSM cellular telephones; and system configuration support for SIPRNET, CENTRIX and NIPRNET laptop computers for field operations, field personnel and new personnel. I also provided administrative support by interviewing personnel and preparing affidavits for missing government cellular telephones. As directed, I conducted research to identify customer requirements for the installation of the CENTRIX network with CENTRIX workstations and provided on-call COMSEC STE KOV-14 support and technical support to Staff Officers through-out Camp Eggers. In support of the Camp Eggers Knowledge Management Office I provided Information System technical support for Inspector General Teams, and I provided on-call system and applications trouble-shooting on computers and audio-visual equipment support for conferences, briefings and events through-out Camp Eggers. I provided security escort support as assigned on a daily watch rotation or on call assignment in support of field communication site visits, convoy security operations, and convoy operations to provide protection for Provincial Reconstruction Teams (PRT) throughout the Afghanistan AOR. Skills: Navy Individual Augmenter Combat Skills Training (NIACT), DOIM Information Management Officer, IWS conference support, PKI implementation/support, STE COMSEC support and convoy security operations. Cryptologic Technician Communications (CTO)

Office of Naval Intelligence, ONI-4, ONI-421 SPINTCOMM Division - Suitland, MD June 2004 to April 2006 Suitland, Maryland Job Title: Cryptologic Technician Communications (CTO) Job Description: Provided worldwide technical/logistic support to Navy and Marine Corps SPINTCOMM's. Maintained, managed, and monitored worldwide SPINTCOMM equipment inventory property records. Managed the shipment of DMS, COMSEC, and intelligence communication system components to worldwide SPINTCOMM locations in support of the installation of intelligence communication systems; provided support for the analysis and distribution of field engineering notices (FEN) for the Defense Message System. I worked as an ADP representative providing property management and technical support for the installation and removal of computer systems and related components in the ONI-421 DMS Lab, and ONI-421 office spaces. Prepared and processed DD-1149 property documents conducted DRMO procedures for the removal and distribution of obsolete/damaged equipment and maintained DRMO records; maintained and operated the ONI-421 DMS Lab CAW workstation and provided support for updating the CRL. Provided support for the resolution of financial lost property audits and lost equipment inquiries. Also, I worked with the ONI property office to record the installation and removal of computers, network devices, peripheral devices, monitors, printers, telecommunications equipment and video/TV equipment. Prepared security documents and coordinated with the ONI SSO and the ONI registry for the world-wide distribution and receipt of cryptographic items and classified hard drives via the Defense Courier Service (DCS). Provided general technical support, trouble-ticket resolution for ONI-421 systems and facilities problems, and maintained world-wide SPINTCOMM property distribution records, and I performed TASO and supply clerk duties for the ONI-421 office and DMS lab. Skills: DMS Administrator, ADP representative, TASO, CAW CA/ISSO. Cryptologic Technician Communications (CTO) USS Carl Vinson, CVN-70, Operations Department, OT Div., SSES - Naval Station Bremerton, WA January 2003 to April 2004 Naval Station Bremerton, Washington Job Title: Cryptologic Technician Communications (CTO) Job Description: Provided Special Intelligence messaging support, managed, maintained and operated thirteen Special Intelligence Communications circuits, including SCI digital communications, SCI voice (satellite and HF), SCI-ADNS, TACINTEL, ANDVT, AMHS, NOW terminal circuits, OPINTEL Broadcast, SR SPRAC, LR SPRAC and HFSPRAC. Provided technical and CMS support for SCI video teleconferences, maintained cryptographic equipment, including: KWR-46, KG-84C, NES, STU-III, and KYV-5, KY-58, KIV-7 and KG-194 crypto equipment; and conducted COMSEC operations, including receipt of OTAT's, re-keying and reloading of CRYPTO equipment, COMSEC key management, and CMS destruction. Monitored, checked and updated LADS in support of DSSCS messaging; conducted trouble-shooting, system configuration, and system administration on Windows NT systems, DOS systems and UNIX systems. Configured CISCO routers and provided technical control with, ping, telnet, black and red patch panels, patch cords and oscilloscopes on CISCO routers, SATCOMM circuits, fleet broadcast, and NOW circuits to restore degraded communications and resolve crypto problems. Managed strike group SCI communications network connectivity and provided technical support to restore SCI communications with escorting guided missile cruisers (CG) and guided missile destroyers (DDG) during periods of degraded communications. Produced and maintained communication logs, communication administrative records, CMS destruction records and provided support for EKMS inspections. Formatted, routed and processed Special Intelligence (SI) messages for world-wide distribution and conducted new operator training for cryptographic equipment operations and CMS destruction procedures. Skills: SCI-ADNS Operator, CMS user, CRITIC message processing and Special Intelligence communications (BE-3s, STRUMs, KLs and Intelligence Summaries). Cryptologic Technician Communications (CTO) USS Paul F. Foster DD-964, Operations Department, OT Div., SSES - Naval Station Everett, WA June 2001 to January 2003 Naval Station Everett, Washington Job Title: Cryptologic Technician Communications (CTO) Job Description: Provided Special Intelligence messaging support, managed, maintained and operated Special Intelligence communications circuits, including SCI digital communications, SCI voice (satellite and HF), SCI-ADNS, TACINTEL, AMHS, ANDVT, SI-SATCOMM TTY, LR SPRAC, SR SPRAC, HF SPRAC, NOW terminal circuits, SNDI and the OPINTEL Broadcast. Maintained cryptographic equipment, including: KWR-46, KG-84C, NES, STU-III, KYV-5, KY-58, KG-194 and conducted COMSEC operations, including receipt of OTAT's, re-keying and reloading of CRYPTO equipment, COMSEC key management and CMS destruction. Conducted trouble-shooting, system configuration and system administration for Windows NT systems, DOS systems and UNIX systems; configured CISCO routers and provided technical control with ping, telnet, black/red patch panels, patch cords, and oscilloscopes on SATCOMM circuits, fleet broadcast, and NOW circuits to restore degraded communication circuits and resolve crypto problems. Managed SCI communications network connectivity provided technical support to restore communications with the NOC during periods of degraded communications and transmitted COMSPOT messages as required. Produced and maintained communication logs, communication administrative records, CMS destruction records and provided support for EKMS inspections; processed, formatted and routed Special Intelligence messages for world-wide distribution via SCI-Networks, TACINTEL and AMHS. Provided training for new operators in Special Intelligence communications, CMS operations and CMS destruction procedures. Provided support for VBSS teams, GCCS-M track updates and national intelligence tracking database updates by visually identifying foreign warships and vessels of interest. Maintained and operated SRBOC as CHAFF round loader and stood security watches as topside security with the M-14 rifle, POOW with the M-9 pistol and pier security with the M-870 shotgun. Skills: SCI-ADNS Operator/Administrator, CMS user, CRITIC message processing and Special Intelligence communications (BE-3s, STRUMs, KLs and Intelligence Summaries). Cryptologic Technician Communications (CTO) USS Kearsarge LHD-3, Operations Department, OT Div., SSES - Norfolk, VA June 1998 to April 2001 Naval Operations Base Norfolk, Virginia Job Title: Cryptologic Technician Communications (CTO) Job Description: Provided Special Intelligence messaging support, managed, maintained and operated Special Intelligence communications circuits, including, SCI digital communications, SCI voice (satellite and HF), SCI-ADNS, TACINTEL, AMHS, ANDVT, SNDI, HF TTY, NOW terminal circuits, SI-SATCOMM TTY, STICS/TRIBUTARY, SR SPRAC and the OPINTEL broadcast. Maintained cryptographic equipment, including: KWR-46, KG-84C, NES, STU-III, KYV-5, KY-58, KG-194 and conducted COMSEC operations, including receipt of OTAT's, re-keying and reloading of Crypto equipment with AN/CYZ-10, KOI-18, and KYK-13 devices, performed CMS destruction and maintained CMS records. Conducted trouble-shooting, system configuration, system administration and technical control with black and red patch panels, patch cords, crypto equipment, oscilloscopes, and telnet on SATCOMM circuits, DOS systems, Windows NT systems, UNIX systems, and CISCO routers to restore degraded communication circuits and resolve crypto problems. Managed SCI communications network connectivity provided technical support to restore communications with the NOC during periods of degraded communications and transmitted COMSPOT messages as required. Produced and maintained communication logs, communication administrative records, CMS destruction records and provided support for EKMS inspections. Processed, formatted and routed Special Intelligence (SI) messages for world-wide distribution via SCI-Networks, TACINTEL and AMHS. Updated and referenced LADS, DOI-101 and DOI-102 publications as required and conducted training for new operators in Special Intelligence communications, CMS operations and CMS destruction procedures. Provided technical support to restore degraded communications with TLCF/NOC and performed UNIX software updates, tape backups, restoral from tape and testing support for TACINTEL II+. Also, assisted SPAWAR with the installation and testing of SCI-ADNS in the USS Kearsarge SSES and operated SRBOC as a CHAFF round loader. Skills: TACINTEL operator, CMS user, CRITIC message processing, Special Intelligence Communications (BE-3s, STRUMs, KLs and Intelligence Summaries). Cryptologic Technician Communications (CTO) NAF Misawa Airbase, Honshu, Misawa - JP May 1996 to May 1998 Job Description: SPINTCOMM Special Intelligence Communications watch-stander managed; operated the Aboveboard Special Intelligence communication system and secure SD-1910 data communications/terminal equipment (DCE/DTE) for message transmission and message downloading on a rotating shift watch schedule. Transmitted, sorted, routed, corrected and processed Special Intelligence (DOI-103, DSSCS) and GENSER (JANAP-128) record message traffic. Performed system updates, system trouble-shooting, ran the BUSTER program to check disks, messages and files for hidden classified data; monitored secure satellite circuits in support of EP-3E ARIES II VQ-1 fleet air reconnaissance missions. Managed and updated Special Intelligence read boards for VQ-1 pre-mission briefs, VQ-1 post mission briefs and daily intelligence briefings. Maintained KG-84C, KG-84A, KYV-5, KY-58, KY-57 and STU-III cryptographic equipment and conducted daily, weekly, and monthly CMS re-keying with OTAR operations, KOI-18 devices, KYK-13 devices and KSD-64 CIKs. Maintained CMS records, communication records and conducted daily, weekly, monthly and yearly CMS destruction. Also, updated DOI-101 and DOI-102 message router indicator databases, monitored SCIF security systems, verified personnel security clearances and provided Special Intelligence messaging support to Naval Security Group personnel. Skills: Cryptologic Technician Communications (CTO), Aboveboard Special Intelligence Communications Operator, CRITIC message processing, GENSER message processing, CMS user, Special Intelligence Communications (STRUMs, KLs and Intelligence Summaries) Education George Mason University April 2009 to Present High School Diploma Lake Washington High School September 1992 to June 1995 Military Service Branch: Navy Service Country: United States Rank: N/A November 1995 to August 2008 Cryptologic Technician Communications (CTO) and Information Systems Technician (IT) Provided telecommunications support and Information processing support using computer terminals, observing all applicable security measures. Provided administrative support, which included maintaining files and updating communications publications via automated methods. Completed system vulnerability tests, and software patch assessments in IT lab environment. Controlled and operated communications systems and networks including satellite systems, network servers, patch panels, modems, routers, multiplexers and communication security devices. Assured signal quality and signal path integrity using test equipment such as protocol analyzers, distortion test sets, spectrum oscilloscopes and signal analysis equipment. Working environments included: secure compartments that house computers and communications devices onboard ships and secure office environments. Operated and managed various computerized information processing systems and communications circuit control equipment as part of a communications watch team or independently. Provided general IT and Telecom support. Designed, installed, operated and maintained IT systems technology, including local and wide area networks, microcomputer systems and associated peripheral devices. Performed the functions of a computer system analyst. Operated and coordinated telecommunication system operations including automated networks, data links and data circuits. Transmitted, received, operated, monitored, controlled and processed all forms of telecommunications through various transmission media including global networks. Applied diagnostic, corrective and recovery techniques for integrated information systems. Maintained all necessary communications logs, files and publications, and provided telecommunications/computer-related training and assistance to a wide variety of personnel. Military experience; November 1, 1995-August 11, 2008 -USN active duty (12 years, 9 months and 11 days) -Rank: E-5 -Naval Information Technology (October 1, 2006-August 11, 2008) -Naval Cryptology, Special Intelligence communications (April 26, 1996-September 30, 2006) -Seaman trainee, (November 1, 1995-April 25, 1996) o Command history: Unit/command Rank Rating Occupation ONI E-5 IT2 INTELCOMM world-wide support technician ISAF HQ E-5 IT2 NATO CMS custodian CSTC-A CJ6 E-5 CTO2 IMO/KMO support technician Fort Jackson, SC E-5 CTO2 90NI trainee ONI E-5 CTO2 SUITLANT SPINTCOMM support technician NOB Norfolk E-5 CTO2 2782 C school trainee CVN-70 E-5 CTO2 Special Intelligence communications operator DD-964 E-5 CTO2 Special Intelligence communications operator NTTC Corry Station E-4 CTO3 2735 C School trainee LHD-3 E-4 CTO3 Special Intelligence communications operator NTTC Corry Station E-4 CTO3 TACINTEL C school trainee VQ-1 E-4 CTO3 Special Intelligence communications operator NTTC Corry Station E-3 CTOSN CTO A school trainee RTC Great Lakes E-1 ------ Basic military recruit trainee o Overseas duty, campaigns and sea deployments -Operation Enduring Freedom-Afghanistan; APR 06-MAY 07 -USS Carl Vinson, CVN-70; Western Pacific deployment, JAN 03-OCT 03 -USS Paul F. Foster, DD-964; Western Pacific deployment, JUN 02-DEC 02 -USS Kearsarge, LHD-3; Mediterranean deployment, Kosovo Campaign, APR 99-OCT 99 -VQ-1 Det. Misawa; Misawa, Honshu, Japan, MAY 96-MAY 98 Commendations: Joint Service Achievement Medal, NATO Medal, NATO Afghanistan Medal, Kosovo Campaign Medal, Afghanistan Campaign Medal, Global War on Terrorism Expeditionary Medal, Global War on Terrorism Service Medal, Good Conduct Medal, National Defense Service Medal, Command Meritorious Unit Commendation, Navy/Marine Corps Overseas Service Ribbon, Sea Service Deployment Ribbon. Three letters of commendation, June 1998 from the VQ-1 OIC, April 2006 from the ONI, and September 2006 from CSTC-A. Branch: United States Navy Rank: N/A Commendations: Joint Service Achievement Medal, NATO Medal, NATO Afghanistan Medal, Kosovo Campaign Medal, Afghanistan Campaign Medal, Global War on Terrorism Expeditionary Medal, Global War on Terrorism Service Medal, Good Conduct Medal, National Defense Service Medal, Command Meritorious Unit Commendation, Navy/Marine Corps Overseas Service Ribbon, Sea Service Deployment Ribbon. Three letters of commendation, June 1998 from the VQ-1 OIC, April 2006 from the ONI, and September 2006 from CSTC-A. Certifications/Licenses Certified Authorization Professional (CAP) The Certified Authorization Professional (CAP) course is designed for the information security practitioner who supports system security commensurate with an organization's mission and risk tolerance, while meeting legal and regulatory requirements. The CAP certification course conceptually mirrors the NIST system authorization process in compliance with the Office of Management and Budget (OMB) Circular A-130, Appendix III. Led by an (ISC) authorized instructor, the CAP training seminar provides a comprehensive review of information systems security concepts and industry best practices, covering the seven domains of the CAP CBK: Risk Management Framework (RMF), Categorization of Information Systems, Selection of Security Controls, Security Control Implementation, Security Control Assessment, Information System Authorization, and Monitoring of Security Controls. The CAP certification is an objective measure of the knowledge, skills, and abilities required for personnel involved in the process of authorizing and maintaining information systems. Specifically, this credential applies to those responsible for formalizing processes used to assess risk and establish security requirements and documentation; which ensure that information systems possess security commensurate with the level of exposure to potential risk and damage to assets or individuals. CompTIA Security+ CE International, vendor-neutral DoDD 8570 IAT Level II certification, that proves competency in system security, cryptography, network infrastructure, access control and organizational security. Additional Information SPECIALTIES Information Assurance/Information Security/Communications Security (18 years) Cryptography (12 years) Cryptologic/C4I System operations (11 years, 4 months) Defense Messaging (11 years) Information Technology support /Automated Data Processing: (13 years, 6 months) Telecommunications (11 years) Physical Security (12 years) Information Technology Asset Management (4 years) E-commerce (1 year) Property management (1 year) CYBER SECURITY, INFORMATION ASSURANCE AND INFORMATION SECURITY EXPERIENCE Security Controls Authorization (A&A, C&A, IV&V): 01/2009-03/2009; 02/2010-09/2010; 07/2012-06/2014; 02/2016-09/2017 (4 years, 4 months) Information Sys. Security Engineering: 09/2010-04/2011; 06/2012-06/2014, 02/2016-10/2017 (4 years, 2 months) Virtual machine (Cloud) software test environment: 02/2010-04/2011; 07/2012-06/2014 (3 years, 2 months) Computer Security: 08/2011-11/2011 (3 months) Computer Network Defense: 03/2000-04/2004, 03/2009-09/2009; 05/2015-12/2015 (5 years) InfoSec/PERSEC/Physical Security (TASO): 06/2005-12/2006 and 05/2007-08/2008 (2 years, 9 months) Network Security: 03/2000-04/2004 (4 years, 1 month) Cryptology: 04/1996-08/2008 (12 years, 4 months) Information Security Jobs/Roles Experience: Information Technology Specialist (Current), TSSC System Administrator 12/28/2018, RMF Assessor 10/07/2018, Information Assurance Engineer 09/30/17, Information Assurance Specialist 02/08/2016, Incident Response/Threat Intrusion Analyst 11/22/2015, Continuous Monitoring Analyst 07/10/205, Security Control Assessor 06/17/2014, Security Engineer 06/30/2012, Information Technology Specialist 11/23/2011, Information System Security Engineer 09/18/2011, Information System Security Representative 09/17/2011, Security Administration 09/03/2009, Incident Handler 07/13/2009, Computer Security Representative 03/27/2009, Terminal Area Security Officer 08/01/2008, Communications Security Material System Custodian 04/30/2007, Information Management Officer 12/09/2006, Certification Authority Workstation Certificate Authority/Information System Security Officer 04/20/2006, Terminal Area Security Officer 04/20/2006, Sensitive Compartmented Information-Networks Operator 04/30/2004, Tactical Intelligence Operator 04/30/2004, Special Intelligence Communications Watch-stander 05/01/1998. Information Security Systems, Tools, Applications, and Ticket Tracking Experience: McAfee ESM, Retina, Gold Disk, SRR, DUMPSEC, Secure CRT, CENTAUR, XACTA, DTA, CACAMs, BUSTER, MMC Security-snap in, remote desktop, Remedy, VOLT, Joint CERT database, CPT, WSUS, ITDR database. Information Security Control Programs, Reports and Documents Experience: FAM, RMF, DIACAP, NISCAP, C&A, A&A, RMF, ICD-503, DODIIS C&A guide, DJSIG, JDCSISSS; CNSSI-1253, NIST SP 800-137, NIST SP 800-53, NIST SP 800-53A, NIST SP 800-37, NIST SP 800-39, DCID 6/3 and JAFAN 6/3; SSP, TAMP, CtF, SCTR, RFS, SPID, MEMOGRAM, TECHGRAM, OPSGRAM, SECGRAM, Simplified EZ, STIG, POA&M, SSAA, OATT, ATC, ATO, IAVM, IAVA, IAVB, IAVT, FEN, CCR, SCF, eRA, ISCP, PIA, Standard Form 85R, and DLAH Form 1728. COMMUNICATIONS SECURITY EXPERIENCE Communications Security Material System (CMS); Electronic Keying Material System (EKMS): ISAF HQ NATO CRYPTO Cell Alt. CMS Custodian: 12/2006-04/2007 CMS user: 04/1996-05/2008 Certification Authority Workstation (CAW) and Public Key Infrastructure (PKI): Trusted Agent, Security Token Issuance Documents: 10/30/2017-Present Common Access Card Personal Identification Number Reset System (CPR) Operator: 10/30/2017-Present PKI implementation and support: 06/2006-11/2006 Certification Authority (CA) for CAW: 06/2005-06/2006 United States Government Type 1 Cryptographic Equipment Operational support: Broadcast Security: KWR-46 Secure Data: KG-194, KG-84C, KG-84A, KIV-7 Secure Telephone: STU-III, STU-IIB, STE Secure Voice: KYV-5, KY-58, KY-57; ANDVT Network Encryption: NES 4001A, TCE-621 Crypto Fill Device/ security token: KSD-64A, FORTEZZA card, KOV-14, KSD-64A, KOI-18, KYK-13, CYZ-10 PHYSICAL SECURITY EXPERIENCE ONI POOW, security screening, military protocol and access control: 06/2004-04/2006 and 05/2007-08/2008 Convoy security, OEF-A armed escort duty, M-16A2 rifle: 05/2006-04/2007 POOW, shipboard quarterdeck security watch, M-9 pistol: 06/1998-01/2003 Pier Security, access control and security watch, M-870 shotgun: 06/1998-04/2004 Topside Rover, shipboard-topside security watch, M-14 rifle: 06/2001-01/2003 SPINTCOMM Watch-stander, monitored SCIF security systems, verified personnel security clearances: 05/1996-05/1998 DEFENSE MESSAGING EXPERIENCE CRITICOMM, COI-101, COI-104 CRITIC messages: 04/1996-06/2005 DSSCS Special Intelligence, DOI-103 full format and abbreviated format record messages: 04/1996-04/2004 General Service (GENSER), JANAP-128/ACP-127 full format record messages: 05/1998-04/2004; 11/2017-Present DOI-101 and DOI-102 DAG and PLA database support: 05/1996-06/2000 ACP-128, Message and Telecommunications Operations:

04/1996-04/2008, 11/2017-Present. Legacy Address Directory Service (LADS) support: 06/2000-06/2005 DOD ADP/ IT SUPPORT JWICS, SIPRNET, and NIPRNET: 06/1998-08/2008, 01/2009-09/2009, 11/2017-Present CENTRIX: 06/2006-12/2006 CRYPTOLOGIC/C4I SYSTEMS EXPERIENCE National Gateway Center-R, SYSADMIN and Message Operator support: 11/2017-Present Defense Message System (DMS) Administrator, logistics and field engineering notice support: 06/2004-04/2006 SCI-Networks (SCI-ADNS) SI message operator: 03/2000-04/2004 Automated Message Handling System (AMHS) SI Communications Operator: 06/1998-04/2004 Tactical Intelligence Exchange System (TACINTEL) SI Communications Operator: 06/1998-04/2004 ABOVEBOARD SI Communications Operator: 05/1996-05/1998 Critical Intelligence Communications (CRITICOMM) Message Processing Operator: 02/1996-06/2005 Special Intelligence Communications (SPINTCOMM) Watch-stander/support: 05/1996-05/1998; 06/2004-07/2008 Automatic Digital Network (AUTODIN): Message Processing Operator: 02/1996-06/2005 and 05/1996-04/2004 Joint Special Imagery Processing System Navy (JSIPS-N), IT and CMS support: 06/1998-05/2004 Global Command and Control System-Maritime (GCCS-M), Intelligence, IT and CMS support: 06/1998-05/2004. SOFTWARE OPERATIONS EXPERIENCE Windows 10: 11/2017-Present LINUX: 08/2008-01/2009 Windows NT: 03/2000-04/2004 UNIX: 06/1998-04/2004 DOS: 05/1996-05/1998 COMPUTER NETWORKING OPERATIONS EXPERIENCE CISCO 4500M router: 03/2000-04/2004 Blue Ridge Networks Borderguard 1000: 03/2000-04/2004 TELECOMMUNICATION OPERATIONS EXPERIENCE Video teleconference and collaboration systems: SCI-VTC: 06/1998-04/2001, 02/2003-04/2004 TANDBERG VTC: 02/2003-04/2004 Polycom VTC: 02/2010-09/2010 Information Work Space (IWS): 06/2006-12/2006 Satellite Communications (SATCOMM): Fleet Broadcast: 06/1998-04/2004 Demand Assigned Multiple Access (DAMA): 06/1998-04/2004 Special Intelligence SATCOMM teletypewriter: 06/1998-12/2003 Sensitive Compartmented Information UHF SATCOMM: 05/1996-04/2004 Sensitive Compartmented Information SHF SATCOMM: 06/1998-04/2004 Scalable Transportable Intelligence Communication System/TRIB: 06/1998-12/1999 International Marine Satellite (INMARSAT): 06/1998-04/2004 and

12/2006-04/2007 IRIDIUM: 06/2006-11/2006 Fleet Satellite Communications (FLTSATCOM): 06/1998-04/2004 Ultra-High Frequency Follow-On (UFO): 06/1998-04/2004 Defense Satellite Communication System III (DSCS III): 06/1998-04/2004 Radio and teletypewriter systems: High Frequency Voice: 06/1998-04/2004 High Frequency teletypewriter: 06/1998-12/2003 Navy Order Wire (NOW): 06/1998-04/2004 Sensitive Compartmented Information VHF LOS: 05/1996-04/2004 Sensitive Compartmented Information UHF LOS: 05/1996-04/2004 Secure telephone, secure data device, and secure-dialup: STU-IIB, STU-III, and STE: 05/1996-04/2008 Motorola secure cell phone: 12/2006-04/2007 AT&T SD-1910: 05/1996-05/1998 Secure Newsdealer Dial in (SNDI): 06/1998-01/2003 Satellite Phones and Cellular Phones: IRIDIUM satellite phones: 05/2006-12/2006 Thuraya satellite phones: 05/2006-12/2006 GSM cellular phones: 05/2006-12/2006 NAVY PRIMARY OCCUPATIONS Information Systems Technician (IT): 10/01/2006-08/11/2008 Cryptologic Technician Communications (CTO): 04/26/1996-09/30/2006 Seaman (SN): 11/01/1995-04/25/1996 NEC DESIGNATIONS 9720: Comm. and Intel Specialists, 0000 CTO: Cryptologic Technician Communications, 9185: TACINTEL, 2782: Defense Message System Administrator, 90NI: Naval Individual Augmentee Combat Training Skills.

Name: Peter Perry

Email: james07@example.com

Phone: +1-495-440-5969x5326