**Larry P. Bunch**

224 Doncaster Rd.

Joppatown, MD. 21085

Mobile Phone: 410-688-8391

E-mail: [lpbunch@outlook.com](mailto:lpbunch@outlook.com)

**OBJECTIVE**

To enrich an already rewarding and challenging career with an organization that offers upward mobility and stability. To work somewhere that my contributions to the team and individual accomplishments are recognized. I am looking for an organization where my experience, leadership skills, and knowledge in the disciplines of: cyber intelligence, network defense/security, and information assurance (IA) can all be fused together to provide the greatest impact and success to an organization.

**WORK EXPERIENCE**

**ADEPT Force Group LLC – Senior Cybersecurity Engineer (Site Lead) – Oct 2017 – Present**

Lead Security

My responsibilities include but are not limited to:

* Analyze, assess, evaluate, integrate, improve, implement, test, sustain, and maintain the system cybersecurity posture and capabilities required by the network domain operations compliance requirements
* Provide cybersecurity network domain C&A support and execute activities that include network domain operations requirements for the following networks: Joint Worldwide Intelligence Communications System (JWICS), Secret Internet Protocol Router Network (SIPRNET)
* Develop and prepare the required security control documents or artifacts, and conduct security control assessments, and security test and evaluation required by the respective network authorities and C&A processes such as the Risk Management Framework (RMF)
* Perform all necessary cyber domain activities to ensure the system baselines follow the respective network domain mandated standards, and authorization to connect requirements
* Develop and document security design artifacts and the associated security controls that are meeting the security acceptance criteria and package the accreditation and authorization documents in support of each domain C&A process
* Validate and perform security test evaluations and audits
* Assess security risk, research and recommend countermeasures in accordance with Army and DoD requirements, conduct formal security engineering assessments and security assessments
* Support on-site accreditation testing for networks at CONUS and OCONUS locations

**Netorian LLC – Senior Cybersecurity Engineer (Lead) – Feb 2016 – Oct 2017**

Lead Security Engineer on a new U.S. Army cybersecurity initiative/platform currently in Research and Development that is scheduled to be fielded within the next few years. My responsibilities include but are not limited to:

* Provide technical guidance for directing and monitoring information systems operations. Designs, builds, and implements network systems
* Direct compilation of records and reports concerning network operations and maintenance.  Troubleshoots network performance issues. Analyzes network traffic and provides capacity planning solutions
* Monitor and responds to complex technical control facility hardware and software problems. Interfaces with vendor support service groups to ensure proper escalation during outages or periods of degraded system performance
* Manage the purchase, testing, installation, and support of network communications, including LAN/MAN/WAN systems
* Plan large-scale systems projects through vendor comparison and cost studies
* Perform a variety of systems engineering tasks and activities that are broad in nature and are concerned with major systems design, integration, and implementation, including personnel, hardware, software, budgetary, and support facilities and/or equipment
* Provide quality assurance review and the evaluation of new and existing software products
* Provide input to policy level discussions regarding standards and budget constraints
* Supervise complex operations that involve two or more additional functions such as, but not limited to, network operations, systems security, systems software support, and production support activities

**Covenant Security Solutions C4ISR – Senior Cybersecurity Engineer (Team Lead) – Apr 2015 – Feb 2016**

Information Assurance / Cybersecurity lead engineer my responsibilities include but are not limited to:

* Subject Matter Expert (SME) providing guidance and support government leadership
* Interface with government to resolve contractor / government issues
* Direct, coordinate, and oversees the day to day Certification and accreditation activities of the (PM DCGS-A)
* Create
* Maintain Authority to Operate (ATO) certification packages
* Creating transitioning C&A packages from the old DoD Information Assurance Certification and Accreditation Process (DIACAP) Risk Management Framework (RMF)
* Create and / or review daily, weekly, & monthly reports for both contractor and government leadership
* Ensures that INFOSEC program requirements are implemented and met
* Interfaced between developers, program managers, and deployment site system users. Provide guidance C&A / Information Assurance and support throughout the (systems development life cycle (SDLC)

**Data Network Cooperation Defense Information Systems Agency (DISA) - Information System Security Manager (ISSM) Contractor Team Lead – Apr 2014 – Mar 2015**

As the ISSM / Team lead my responsibilities include but are not limited to:

* Direct, coordinate, and oversees the day to day activities of a team of eight (8) Information System Security Officers (ISSO)
* Responsible for the transitioning of more than 10 accreditations from DIACAP to RMF
* Ensures that INFOSEC program requirements are met
* Ensures accreditation support documentation is developed and maintained within eMASS
* Briefing senior leadership daily
* Create Weekly and monthly reports
* Develop and conduct training for both Government and contracting staff
* Coordination of C&A/IA activities between Tier II & Tier III
* Ensures development of System Security Plans (SSP)
* Responsible for performing those duties normally performed by ISSOs in the event that no ISSO is appointed
* New employee screening
* New contract / proposal writing

**Independent Consultant**

**August 2013 – Mar 2014**

Responsibilities to included: writing business proposals, contract negation, business development, and marketing. Keeping a records of billable and non-billable expenses. In my capacity as an independent consultant. Some of the services that I provided were:

* Conduct risk assessments to identify gaps in the clients’ security posture
* Provide comprehensive face to face review and detailed report of findings
* Recommended mitigation strategies and Courses of Action (CoA) for customer according to industry best practices
* Development or, assist the customer in the development of policies and procedures adhering to the “Defense in Depth” model and “Best Practices”
* Recommend new and emerging technologies and products to customer
* Provide ongoing support for Clients
* Subcontracting services to other companies: to include
  + Instructing information security “Boot camps” To include CISSP and Security+
  + Independent Sales Representative
* Develops or assist in the development of cyber-security/awareness training programs
* Contract negations between the client and myself

**Provideo Management - Defense Information Systems Agency - Principal Security Engineer (Contract Lead) - March 2013 – August 2013**

Responsibilities included:

* Maintain a working knowledge of Department of Defense and NIST Information Assurance (IA) and Computer Network Defense (CND) Policies and Procedures
* Created, Supported, and successfully completed product accreditations
* Communicated complex technical and programmatic information to leadership
* Conducted formal and informal briefing to DISA senior leadership
* Identified IA gaps and recommended mitigation strategies
* Developed Site Security Plans (SSP), Site Responsibility Guide (SRG), and Plan of Action and Milestones (POA&M) adhering to (DIACAP)
* Provided meeting minutes to the PM Program Manager and review Weekly Activity reports (WAR)

**URS/Apptis (DISA) - Principal Security Engineer/ Incident Fusion Cell Senior Analyst**

**March 2012 – 2013**

Fused cyber incidents to include network intrusions, Advanced Persistent Threats, Intrusion Set Attribution, Insider Threats, and Malware Research.

* Collaboration with other task force cells and Subject Matter Experts (SME) within the LE/CI community

Compiled information for incident reports, daily/weekly/monthly reports on the events and incidents

* Provide technical subject matter expertise (SME) for a wide range of security technologies
* Brief Senior Leadership on Advanced Persistent Threats (APT), current vulnerabilities, exploits and malware
* Writing Concept of Operations (CONOPS), Operation Orders (OPORD)’s, policy and procedures for McAfee’s Host Based Security System. (HBSS)

**VortechX LLC (US Army – Communications and Electronics Command (CECOM)) - Sr. Systems Engineer**

**February 2011 - 2012**

Primarily functions as the Information Assurance Security Officer (IASO) working in the US Army Communications & Electronics Command (CECOM) Software Engineering Center (SEC) on the PM DCGS-A program

* Conduct required IAVM scanning and vulnerability assessments
* Monitor IS performance to ensure that processes, security features, and operating system configurations
* Establish audit trails, conduct reviews, and create archives as directed by the IAM.
* Enforce the IS security guidance policies as provided by the IAM and perform IASO duties

**Mantech – Defense Cyber Crime Center/National Investigative Joint Task Force (DC3/NCIJTF) - Sr. Systems Intelligence Analyst - Jan. 2009 - 2011**

Responsibilities include: obtaining and maintaining subject matter expertise on entities of interest in relation to computer and network intrusions.

* Research current and emerging threats, recognize links and relationships between threat entities, and identify indications of future activities.
* Provide detailed analysis in the form of: Briefs, Special Reports, and Alerts and other intelligence products
* Collaboration with other task force cells and Subject Matter Experts (SME) within the LE/CI community

**Maryland Army National Guard - Information Systems Operator S-6 Section Chief - Nov. 1992 – Mar. 2008**  
Computer Network Specialist (Network Administrator) Responsible for the configuration of network hardware/software, network performance. Responsible for equipment inventory, creating evaluation reports and the counselingof 20+ soldiers

* Determine requirements, manage and coordinate the activities of personnel via Training Plans and Operation orders. Develop and administer on-site training programs
* Analyze telecommunications and information management and security needs
* Direct the installation, operation and maintenance of specified battlefield information services.

**(Note:** From 1992 to 1997 my job title was MOS 11B20 - Infantry Squad Leader)

**e-Management Inc. Department of Energy (DOE) - Cyber Security Engineer - December 2006 - January 2008**   
Served as a technical lead of Computer Network Operations (CNO) responsible to architect, deploy, and administer Cyber Security related solutions. Oversee implementation and management of Intrusion Detection Systems other cyber security related systems. Served as a liaison between DOE cyber-security and LE/CI.

* Assist in the development of policies in support of certification and accreditation (C&A) program
* Collects and translates information security requirements into system security documentation
* Created customized SNORT rules and IDS, Firewall, and Sys Log file analysis
* Developed and provided Cyber-Security/Awareness training to DOE field sites.

**Jacob & Sundstrom Inc. (ARL/HPCCERT) Senior Network Security Analyst - February 2001 - November 2006**   
Senior Network Security Analyst supporting the DoD with intrusion detection and network security services. Responsibilities included: monitor and protecting several large DoD networks by performs real-time and retrospective analysis using deep knowledge of networking, UNIX, Windows, and intrusion detection systems to determine if an intrusion has taken placeCompiling information and preparing computer security incident reports and preparing daily/weekly/monthly reports on the events and incidents detected in the course of network monitoring.

**Education / Training**

* Associate Degree, 8/2003 – 6/2006 - Strayer University | White Marsh, MD
* US Army Primary Leadership Development Course (PLDC) - 5/1994
* 74B - Information Systems Operator-Analyst | State: GA 8/1998 – 11/1998
* i2 Analyst Notebook Level 1
* Tactical Message System (TMS) Course - 8/2004
* AN/TYC-24(V)\* Tactical Message System Planners’ Course - /2004
* Network Encryption System – System Administrator – 02/1999

**Certifications**

* CISSP - Certified: 12/20/2010 (Member Id: 377627)
* Certified Ethical Hacker (CEH) Certified: 04/28/ 2006 (Member Id: ECC914302)
* SANS GIAC Certified Incident Handler – GCIH (Gold) Certified: 01/31/2003 (Member Id: 394)

**Professional Memberships / Affiliations**

* Armed Forces Communications and Electronics Association (AFCEA)
* Information Systems Security Association (ISSA)
* International Information Systems Security Certification Consortium (ISC)2
* Signal Corps Regimental Affiliation

**Honors/ Volunteer Activities**

* Meritorious Service Medal
* “Key Note” Speaker at the *2014 Cybersecurity Innovation Forum & Expo*
* Head Coach of the 12U Joppatown Seahawks (*2013 Champions of the Upper Chesapeake Youth Football League*)