RICHARD SEPULVEDA, CISSP, CEH, CNDA, Security+, SAFe 4

6159 Villa Rica Hwy, Dallas, GA, 30157 860-796-1650 **E-mail:** rsepulveda@insecureplanet.com

LinkedIn Profile www.Insecureplanet.com

Senior PKI Solutions Engineer & Cybersecurity Expert

SUMMARY

Experienced in Infosec, PKI engineering, and network administration with an active ***DoD SECRET clearance***. I possess a robust understanding of hardware, software, and encryption technologies, ensuring thorough analysis, implementation, and support across secure environments. My expertise includes encryption software evaluation, project management, and network security consulting. I am committed to upholding the CIA Triad of Confidentiality, Integrity, and Availability in all aspects of security policy implementation.

OBJECTIVE

Provide encryption, network, systems, and security experience, knowledge, and solutions, in a system and network-diverse environment. Protect confidentiality, integrity, and availability of information, and information systems. Advise and engineer secure solutions for business opportunities. Learn, experience, mentor, and share.

EXPERIENCE

08/2023 – Present Insight Global LLC Remote
USAID

Sr PKI Engineer
Responsible for Microsoft PKI Upgrade project incorporating multiple Certificate Authorities and support infrastructure. Involved in migrating infrastructure legacy certificates to the new issued ones based off newly created templates at latest iteration. Collaborated with Entrust technical engagement support migrating to new hardware security modules (HSM's).

- **Project Leadership:** Spearheaded a comprehensive Microsoft PKI upgrade, enhancing security and operational efficiency across the organization.
- **Certificate Migration:** Directed the transition of infrastructure legacy certificates to newly issued ones, creating and utilizing updated server components to ensure compliance with the latest security standards.

- **Hardware Security Module Integration:** Collaborated with Entrust's Professional Services technical team to successfully migrate to advanced hardware security modules (HSMs), strengthening cryptographic key operations and protection.
- **Infrastructure Development:** Played a pivotal role in building and deploying new PKI infrastructure servers, including Certificate Authorities (CAs) and Certificate Distribution Points (CDPs), following best practices for secure and efficient operations.
- **Template Recreation:** Reconstructed all essential certificate templates within the upgraded environment, ensuring seamless integration and functionality.
- **Documentation and SOPs:** Authored comprehensive documentation for PKI and certificate management, encompassing build guides, technical architecture designs, and standard operating procedures (SOPs), facilitating client understanding and system maintenance.
- **Cross-Functional Collaboration:** Worked closely with the Project Management Office (PMO), project teams, and server application administrators to ensure a smooth migration process, minimizing disruptions and enhancing stakeholder engagement.
- **Pilot Testing and Deployment:** Led pilot teams in testing the new infrastructure, identifying and resolving issues prior to full-scale deployment, ensuring system reliability and performance.

12/2022 – 08/2023 Persistent Remote

Principal PKI Architect
Responsible for evaluating new and existing data security solutions, guiding the design and implementation of security solutions and services across business and IT areas using architecture standards, best practices and processes.

- **Security Solutions Evaluation:** Led the assessment of emerging and existing data security technologies, steering the design and deployment of security solutions across business and IT sectors in alignment with architectural standards and industry best practices.
- **PKI and Certificate Management:** Authored comprehensive analysis and requirements documentation for Public Key Infrastructure (PKI) and certificate management systems, enhancing client security postures.
- **Collaboration with IAM Teams:** Partnered with Identity and Access Management (IAM) project teams to comprehend data classification and security needs for various applications, devising optimal implementation strategies.

- **Requirement Translation:** Acted as a key liaison among team leads and clients, effectively translating functional requirements into robust security specifications.
- **Engagement in Security Proposals:** Contributed to multiple security Statements of Work (SOWs), Requests for Proposals (RFPs), and partnership initiatives, driving business development and client acquisition.
- **Development of PKI Solution Packages:** Engineered diverse PKI solution packages tailored for current and prospective sales engagements, broadening the company's service offerings and market reach.

06/2022 – 12/2022 Insight Global LLC Remote
CarMax

PKI Engineer
Served as the Project SME for the inaugural integration of Axiad Cloud PKI with Venafi-supported PKI systems, facilitating the seamless transition from Microsoft's internal PKI environment.

- **Engineered and Configured Migration Processes**: Led the engineering, installation, configuration, and testing phases, collaborating closely with Axiad's engineering team to ensure seamless migration.
- **Coordinated Server Farm Migrations**: Oversaw the migration and configuration processes for U.S.-based CarMax server farms, working with support teams to deploy, test, and validate each iteration.
- **Developed New Certificate Templates**: Designed and implemented new certificate templates within the Axiad environment to replace legacy Microsoft PKI templates, enhancing security and compatibility.
- **Migrated SSL Certificates**: Led the migration of thousands of SSL certificates to the new Axiad Cloud PKI infrastructure, ensuring continuity and security of services.
- **Authored Technical Documentation**: Created detailed engineering documents covering installation, configuration, migration, and testing procedures to support ongoing operations and future projects.

09/2021 – 05/2022 Insight Global LLC Remote
Santander Bank NA

PKI Engineer
As the Subject Matter Expert (SME) for Santander Bank N.A., I led the establishment of two new Public Key Infrastructure (PKI) systems, integrating Keyfactor for comprehensive certificate management. This initiative encompassed the engineering, installation, configuration, testing, documentation, and support of various PKI components, including Subordinate Certificate Authorities (CAs), Certificate Revocation List (CRL) Web Distribution, Online Certificate Status Protocol (OCSP), Network Device Enrollment Service (NDES), Certificate Enrollment Services (CES),

Keyfactor Command, Keyfactor Orchestrators, and associated database servers.

Key Responsibilities and Achievements:

- **Lead Engineer for Microsoft PKI Implementation:** Spearheaded the planning and execution of installing and configuring two new Microsoft PKI infrastructures, ensuring robust security and compliance with industry standards.
- **Deployment of Subordinate Certificate Authorities:** Successfully installed, configured, tested, validated, and documented Subordinate CAs, enhancing the bank's hierarchical trust model and certificate issuance capabilities.
- **CRL and OCSP Configuration:** Implemented and validated CRL Web Distribution and OCSP services to manage certificate revocation and real-time status checking, thereby strengthening the bank's security posture.
- **NDES and CES Implementation:** Set up and tested NDES and CES to facilitate certificate enrollment for network devices, streamlining secure communications across the organization's infrastructure.
- **Integration of Keyfactor Solutions:** Played a pivotal role in configuring Keyfactor Command, Orchestrators, and database servers within the new PKI infrastructure, enabling automated certificate lifecycle management and operational efficiency.

08/2016 – 09/2021 Insight Global LLC Remote
Perspecta - Navy Contract

PKI Engineer

As an engineer on a Navy contract, I led the deployment of the Next Generation Enterprise Network (NGEN) Public Key Infrastructure (PKI) Upgrade Project for the Navy Marine Corps Intranet (NMCI) network. This initiative aimed to enhance the Department of Defense's (DoD) multi-tier PKI by integrating Active Directory and adhering to Agile project management methodologies, while strictly following DoD, Defense Information Systems Agency (DISA), and Defense Information Assurance Certification and Accreditation Process (DIACAP) guidelines.

Key Contributions:

- **NGEN Centrify Upgrade Project Leadership:** Spearheaded the NGEN Centrify Upgrade Project across multiple domains, ensuring seamless integration and improved security protocols.
- **Microsoft PKI Modernization:** Played a pivotal role in upgrading the legacy Microsoft PKI to a more advanced system, enhancing the network's security and efficiency.
- **Comprehensive Documentation:** Authored and revised over 20 installation, configuration, testing, and validation documents, providing clear guidelines for current and future implementations.
- **Axway Validation Authority Enhancement:** Supported and ensured the timely upgrade of the Axway Validation Authority and Desktop Validator, meeting all designated provisioning timelines to maintain system integrity.

12/2015 - 7/2016 Diversant LLC Atlanta, GA
The Home Depot Corporate

PKI Security Engineer
As a resolute engineer, I have provided comprehensive support for a multifaceted enterprise infrastructure, focusing on internal and external Public Key Infrastructure (PKI) systems, including RSA Certificate Authority (CA), Entrust, Symantec, Venafi Certificate Management, Active Directory, and Thales Security Modules. My role was pivotal in a large-scale enterprise migration to SHA-256 encryption, where I served as the Subject Matter Expert (SME) for current and forthcoming security encryption projects. I streamlined Service Level Agreements (SLAs) and optimized work processes to enhance accountability, efficiency, reporting, and auditing. Additionally, I managed SSL certificate renewal tracking for over 20,000 endpoints.

Key Achievements:

- **Enhanced SSL Certificate Management:** Revamped the in-house tracking and reporting system to effectively manage the lifecycle of SSL certificates, including issuance, renewal, reissuance, and revocation. This initiative-taking approach significantly reduced the risk of certificate-related outages, aligning with best practices in certificate lifecycle management.

- **Coordinated Large-Scale Certificate Renewals:** Led after-hours renewal operations for servers across 2,250 store locations, collaborating with cross-functional teams to ensure seamless deployment, testing, and validation. As part of this work certificate issuance/renewals automation was achieved utilizing Venafi Certificate Management policies, workflows and the incorporation of API's. This initiative ensured uninterrupted service and compliance with security standards.
- **Evaluated Emerging Security Technologies:** Conducted Proof of Concept (POC) evaluations for recent technologies related to certificate authorities and internal alternatives, ensuring the organization's infrastructure remained at the forefront of security advancements. This initiative-taking evaluation is crucial for maintaining robust security postures.

- **Led Symantec Security Enhancements:** Spearheaded the upgrade project for Symantec Security Event Managers (SSEMs), enhancing the secure transmission of confidential data and reinforcing the organization's data protection measures. Upgrading security infrastructure components is essential for safeguarding sensitive information.

12/2013 – 12/2015 State of South Carolina Columbia, SC
Department of Technology Office

Information Data Architect \ Encryption Engineer

As a contractor for the State of South Carolina Budget and Control Board, I led the design and implementation of comprehensive security solutions across multiple state agencies. My responsibilities encompassed deploying Symantec Drive Encryption, CyberArk Privileged Access Management, AirWatch Mobile Device Management, and Nessus Security Center.

Key Achievements:

- **Symantec Drive Encryption Deployment:** Spearheaded an enterprise-level, centrally managed deployment of Symantec Drive Encryption (formerly PGP) across various internal and external state agencies. Oversaw all phases, including evaluation, proof of concept, testing, pilot, deployment, and post-deployment support. Authored support documents, test plans, standard operating procedures, and architectural diagrams to ensure seamless implementation.

- **CyberArk Privileged Access Management:** Installed, configured, and deployed CyberArk Enterprise Password Vault (EPV) as part of a comprehensive project to enhance sensitive information management and privileged access management. This initiative improved security and compliance by managing over 20,000 privileged accounts across a heterogeneous data center environment.

- **Symantec to McAfee Drive Encryption Migration:** Led the migration project from Symantec to McAfee Drive Encryption, ensuring data integrity and minimal disruption to operations. Implemented best practices for endpoint encryption to protect data at rest and in transit.

- **Nessus Security Center Deployment:** Supported the Nessus Vulnerability Assessment project by configuring scanning criteria, policies, reporting, and deployment methodologies. This deployment enhanced the organization's ability to identify and remediate vulnerabilities across the network.

- **Documentation and Standard Operating Procedures:** Authored various support documents, test plans, desktop/helpdesk standard operating procedures, and architectural diagrams to facilitate smooth deployment and ongoing support of security solutions. This documentation ensured consistency and compliance with organizational policies.

- **Cross-Agency Collaboration:** Coordinated with multiple internal and external state agencies to ensure the successful deployment and integration of security solutions, enhancing the overall security posture of the state's IT infrastructure. This collaborative approach ensured that security measures were uniformly applied across all agencies.

9/2013 - 12/2013 General Dynamics Alexandria, VA
US Patent & Trademark Office

PKI-Encryption Engineer
As a Public Key Infrastructure (PKI) Engineer at the United States Patent and Trademark Office (USPTO), I played a pivotal role in supporting the Federal Bridge Certification Authority (FBCA) PKI infrastructure across both extensive campus environments and remote locations. My responsibilities encompassed the development and implementation of internal and external network strategies to enhance user authentication, identity management, web access, and VPN security.

Key Responsibilities:

- **Internal PKI Environment Management:** Provided engineering support for the internal Entrust PKI environment, which included managing clustered Certification Authorities (CAs), Directory Controllers (DCs), F5 Validation Authority for Online Certificate Status Protocol (OCSP), both clustered and standalone Hardware Security Modules (HSMs), and Identity Management (IDM) systems.

- **External PKI Environment Maintenance:** Maintained the external Entrust PKI environment, overseeing components such as CAs, DCs, Active Directory Lightweight Directory Services (AD-LDS), Digital Certificate Management (DCM) web interfaces, and application servers running Entrust Administration Services (AS). Additionally, I supported the TruePass Authentication Section, which facilitated secure access to the Electronic Filing System (EFS) and Private PAIR (Patent Application Information Retrieval) systems.

- **Smart Card Management System Oversight:** Was responsible for the Homeland Security Presidential Directive 12 (HSPD-12) compliant Card Management System (CMS), ensuring the issuance and maintenance of Personal Identity Verification (PIV) smart cards.

- **Support for Identity Management and Security Tools:** Provided support for various security tools and systems, including Probaris IDM, biometric scanners, Active Identity solutions, secure email communications, digital signatures, and associated databases.

7/2001 – 8/2012 Computer Sciences Corporation East Hartford, CT

PKI-Encryption Engineer/ Security Administrator
As a Lead Public Key Infrastructure (PKI) Engineer, I have spearheaded enterprise-level security initiatives across multiple clients, focusing on drafting security standards, managing encryption testing, and deploying comprehensive PKI solutions.
Enterprise Security Leadership

- **Development of Security Standards**: Authored and implemented enterprise security standards and system configuration guidelines, ensuring robust and consistent security postures across diverse organizational environments.

- **Encryption Strategy Management**: Led the processes for security encryption testing, evaluation, and deployment strategies, overseeing multiple encryption projects to successful completion.

Client Engagements and Achievements

- **CSC**:
  - *Training and Development*: Directed training programs for 400 helpdesk and desktop support technicians, enhancing their proficiency in supporting various PKI and desktop encryption security applications at Tier 1 and Tier 2 levels. Additionally, implemented training for subordinate engineers and administrators to support Tier 3 level operations.
  - *PKI Infrastructure Management*: Installed and maintained the corporate PKI infrastructure, including patches, version upgrades, application changes, log management, and security assessment systems. Developed customized PKI desktop installation client packages compatible with various operating system versions and tailored installers for international locations in Asia and EMEA.
- **United Technologies (UTC)**:
  - *PKI Migration Project*: Played a pivotal role in UTC's large-scale PKI migration project. Executed the cloning of UTC's production environment, including Entrust 5.0 Certification Authority (CA), subordinate CAs, Syntegra X500, staging LDAP servers, Entrust 7.1 CA, and iPlanet LDAP servers. Coordinated with vendor and client staff to achieve successful completion within designated timelines.
  - *New PKI Environment Deployment*: Established a new PKI environment post-migration, comprising Entrust CA, messaging server, compliance servers, and webmail appliance servers. Configured PKI policies based on UTC, CSC, and Entrust role models, and customized the messaging server to automate traffic handling through UTC mail hubs.
  - *Compliance and Monitoring*: Provided engineering support for encrypted email scanning compliance servers and management consoles used for content scanning to meet government ITAR restrictions and compliance requirements. Configured SNMP trap reporting servers to monitor status and facilitate after-hours monitoring and required actions.
- **Pratt & Whitney**:
  - *Security Integration*: Collaborated with the security team to define roles, policies, and support methodologies for file, folder, mail, and SAP-based encryption methodologies.
  - *Encryption Deployment*: Served as the principal engineer for all Check Point Full Disk Encryption (FDE) and Check Point Media Encryption (CME) server-based deployments. Directed and implemented configuration, customization, and support of server and desktop encryption clients, including upgrades, patches, and troubleshooting. Provided Level 3 support for all Check Point encryption applications.
- **Rocketdyne**:
  - *LDAP Integration*: Contributed significantly to engineering and migrating Rocketdyne's LDAP exchange system to

integrate with Pratt & Whitney's, facilitating standard organizational email encryption across different networks.

- **Hamilton Sundstrand**:
  - *Email Encryption Project*: Played a vital role in a large-scale email encryption project with Boeing, enabling the sharing of public certificates for seamless email communications within the continental United States.
  - *Training and Support*: Initiated training programs for Windsor Locks desktop support teams, equipping them with the latest encryption technologies and techniques to support various encryption desktop application versions. Provided direct support for Symantec Critical Systems Protection suite, securing and blocking various proxy points for servers within the organization.
- **Sikorsky**:
  - *Smart Card Encryption Deployment*: Represented the security team in smart card encryption deployment project meetings. Collaborated with Stratford security and desktop teams on various encryption projects, providing mentorship to enhance product support capabilities.
- **Carrier and Otis**:
  - *Onsite Training*: Established onsite training programs for Farmington desktop support technicians, focusing on PKI and Check Point FDE and CME clients, enhancing their ability to support encryption technologies effectively.

7/2007 - 7/2012	US Naval Space & Warfare System Command	Groton, CT.

US Navy Reserves- Computer Network Defense Engineer

- Assisted in preparation of US Navy vessels for annual information security IAVA certifications.
- Contributed to creating training material, PowerPoints, etc. for various units infosec training requirements as tasked.
- Administered, patched, and implemented IAVA to Naval Submarine Support Command.
- Stood-up Hercules/Citadel servers to download all pertinent security patches and IAVA material from US Navy REDCOM center.
- Provided over 400 hours of information security training to more than 200 sailors from various ships and subs and four aircraft squadrons based in Norfolk and San Diego.
- Performed information assurance vulnerability assessments on more than 12 ships.
- Fly Away Team member performed pentests and vulnerability assessments, password cracking, reporting, assisted crew with vulnerability mitigation, to complete mission scanning both NIPR (Unclassified) and SIPR (Classified) Navy networks on target ships.

4/1998- 6/2001	Navy Technical Training Center- Corry Station	Pensacola, FL.

Electronic Warfare Instructor/ Information Systems Administrator

- Administered, maintained, troubleshot, upgraded, configured, installed, and repaired all pertinent Base wide network needs for 600 users complying with Novell and NT 4.0 hierarchy.
- Implemented Information System Security and Antivirus resolution.
- Upgraded and built custom PC configurations following Navy Base Network guidelines and standards.
- Assisted in the installation of 5 network classrooms consisting of approximately 104 workstations to be used for training in both highly classified and unclassified areas.
- Upgraded Navy Base Standard Training Activity Support System computers to present NT 4.0 version status, using Ghosting software for efficiency and speed, applying all Oracle upgrades and patches allowing secure firewall penetration utilizing Alta Vista Tunnel protocols.
- Lead technician for Base upgrade project of 600 users from Novell based Lotus CCMail email client to present MS Exchange Server 5.5/Outlook 2000 client, training and working with Upgrade Team Members.
- Resolved various helpdesk IT issues from printer configuration to network troubleshooting in base offices and student labs.
- Trained 20 Cryptologic Maintenance Technicians to support aforesaid Helpdesk(Navy Instructor Certified).
- Recommended preventive, mitigating, and compensating controls to ensure the appropriate level of protection and adherence to the goals of the overall information security strategy.
- Assisted in the development of access-controls, separation of duties, and roles.
- Conducted technical risk evaluation of hardware, software, and installed systems and networks.
- Assisted with testing installed systems to ensure protection strategies are properly implemented and working as intended.
- Assisted in incident response and recommend corrective actions.
- Implemented Security training with base personnel covering potential network environment threat vectors.
- Participated in forensic recovery and analysis of base assets.

4/1996- 4/1998	Atlantic Fleet Weapons Training Facility	Roosevelt Roads Naval Station, PR.

Electronic Warfare Range Operator/ Information Security Officer/ Technician

- Conducted training and operations for US and NATO navies, above, below, in the air and on of Vieques Island of electronic systems and weapons release simulating actual combat environments.
- Implemented remote radiating of controlled emissions simulating hundreds of enemy fire control/missile and friendly radars for

training requirements so foresaid units could identify and report efficiently and speedily these correlations. Reports were then analyzed and evaluated for accuracy for final grading of participating units.
- As Information Security Officer was on fly-away team transiting between Puerto Rico, Vieques, St Croix, and St Thomas Islands. During these missions' facilities Information Systems would be regularly scanned for possible security compromises, viruses, illegal software, improper use of computers, password control, network vulnerabilities, etc.
- Networking team member in the upgrading and relocation of 16 HP TAC-3 UNIX system fiber optic network including splicing 80 strands and rerouting. This network was highly classified due to its use in Caribbean Anti-Narcotic missions being fed raw data from P-3's, U-2's, ship and land-based units and facilities.

4/1993 -4/1996	Fleet Information Warfare Center	Naval Amphibious Base, Coronado, CA.

JMCIS-UNIX Administrator/IT Support/Electronic Warfare Technician

- Worked with Navy Research and Development (NRAD) installing Joint Maritime Command Information System (JMCIS) a HP-TAC-3 UNIX based network which encompasses various external systems to communicate effectively via classified satellites, sea, land, and air based units bringing intelligence gathering, communications, and instantaneous targeting data together for the fleet.
- As part of Admirals Staff was flown to Japan to participate in Operation Foal Eagle on USS Duluth, responsible for the JMCIS gear in Command Information Center, working closely with intelligence gathering Cryptologic Technicians.
- As a ULQ-13 Van Operator/Technician was responsible for transiting to various land sites including Fallon, Nevada, where electronic warfare was conducted against Navy air units including Top Gun. Responsible for programming radar simulations and radar/communication jamming of aforesaid units.
- Supported Raytheon complete upgrading of (6) Vans including a complete refit of all remotely controlled computer transmitting networks. Also worked on 440V AC high voltage TWT type signal generators, troubleshooting, maintaining, and repairing equipment.

EDUCATION

Certification Path

Zscaler Zero Trust Architect - 5/2023
Zscaler Sales Professional - 4/2023
Zscaler Sales Engineer- 4/2023
Certified SAFe 4 Practitioner (Agile) - 11/2019
Certified Information Systems Security Professional- CISSP 11/2008

Security+ CompTIA - 02/2017
Certified Ethical Hacker- CEH 03/30/2011
Certified Network Defense Architect- CNDA 05/15/2011
Computer Network Defense in Depth Baseline Assessment 9/2008 SPAWAR Atlantic Fleet Naval Base, Norfolk VA.
Entrust Security Manager Administration Comprehensive 9/2005 Kanata, Ottawa, CAN.
Security Certified Network Professional - SCNP Hardening the Infrastructure 10/2004
Linux + CompTIA 7/2004
Security Certified Network Professional - SCNP Network Defense Countermeasures 5/2004
Security Certified Network Architect - SCNA Advanced Security Implementation 4/2004
Security + CompTIA 2/2004
MCSE 2000 Core and Electives -University of West Florida US-FL-Pensacola - 4/2001

Bachelor's Path

5/2009 Capella University
Information Security NSA Accreditation, Enterprise Architecture, *Project Management.*

2/2004 New Horizons Bloomfield CT
Security Track- SCNA, SCNP, Security+, Linux+, CompTIA

6/1998 Navy Instructor Training US-FL-Pensacola

Learning Theory, Interpersonal Communications, Principles of Speech, Instructional Media, Curriculum Design, and Instructional Strategy.

11/1997 New Hampshire College US-Puerto Rico-Roosevelt Roads Naval Station

Computer Concepts, Introduction to Marketing, Human Relations Admin

7/1992 Navy Campus US-CA San Diego
Technical Drafting, Natural Sciences, Management Information Systems, Social Sciences/History, Western Civilization.

10/1991 San Diego City College US-CA-San Diego

Microcomputer Applications, Technical Illustration/Airbrush Rendering.

5/1991 Naval Technical Training Center US-FL-Pensacola

Electronic Technology (Solid State/Digital, Soldering, AC/DC Circuits, Introduction to Microcomputers, Electronic Test Equipment).
Electronic Technology (Systems Maintenance, Circuit Theory, Applied Mathematics, Digital Electronics, Troubleshooting).

Basic Electronic Lab, AC/DC, Digital Principles, Computer Systems, Control Systems, Communications, Troubleshooting/Maintenance.

CLEARANCE 2017- Present DoD SECRET (Active)

AFFILIATIONS 11/2008 – Present International Information Systems Security Certification Consortium(ISC)2 Member

SKILLS

Skill Name

Unix - Linux System Administration RHEL

Venafi Certificate Management

IP Packet Analysis – Wireshark/Ethereal, tcpdump
Intrusion Detection - Snort
Penetration Testing - Nessus/Nmap

Entrust Desktop Solutions
Entrust Entelligence Security Provider
Entrust Certificate Authority
Entrust Messaging Server
Entrust WebMail
Entrust Compliance Server
Entrust Truepass
Pointsec Mobile Security
RSA SecureID
Checkpoint Full Disk Encryption
Checkpoint Media Encryption
Symantec Critical System Protect
Symantec PGP WDE Encryption
Microsoft CA, ADCS
Vericept 360
Vericept Protect
Perl, HTML

DHCP, MySQL, Postfix, SSH Administration

Microsoft Project Manager
Visio
Adobe Photoshop
Gimp

Citrix Metaframe Administration

HP-UX Unix

Active Directory Administration
McAfee ePO
McAfee Drive Encryption
MS Server 2003+
MS Exchange

Fiberoptics Installer/Splicer
Airwatch MDM

S/MIME/ PGP Administration
eEyeRetina
Backtrack/Metasploit
SecureID Administration
TrueCrypt
PIV Smartcards
CyberArk PAM
CyberArk SIM
Centrify
Cisco Endpoint Security
Cisco Networking Components
Axway Validation Authority
Axway Desktop Validator

ADDITIONAL INFORMATION

AWARDS:

- Letter of Commendation for Navy Base MS Exchange/Outlook upgrade project.
- Letter of Commendation for Navy Marine Corp Relief Drive Volunteer Excellence,
- Letter of Commendation for American Multi-Heritage Committee Volunteer.
- Awarded (3) Letter of Commendation for outstanding training to the fleet.
- Volunteer Roosevelt Roads Elementary Schools Science Club Administrator- working with US Fish and Wildlife Biologists saving endangered Green Sea Turtles.
- Received Letter of Commendation for superb Electronic Warfare training to the Navy (Top Gun).
- Letter of Commendation for researching and building (4) Russian T-49 mock mobile gun units to be used for search and destroy mission training in the Pacific.
- Volunteer and coordinated Adopt-A-School program in San Diego.

NAVY MEDALS & RIBBONS:

Navy and Marine Corps Achievement Medal (4)
Navy Battle "E" Ribbon
Navy Good Conduct Medal (3)
Naval Reserve Meritorious Service Medal

National Defense Service Medal
Global War on Terror Service Medal
Military Outstanding Volunteer Service Medal
Navy Sea Service Deployment Ribbon (2)
Naval Reserve Sea Service Ribbon
Cold War Medal

INTERESTS:

Information Security, Cyber Warfare, Military History, Computers, Graphics, Chess, Model Building, Antiques, Collectibles, Cars, Zymurgy, Science Fiction, Boating, Martial Arts, Archery.