Patrick Caruso

720 Elvira Ave, Redondo Beach, CA 90277 • 781-534-3361 • patcaru@icloud.com • **Active DoD TS/SSBI**

Objectives

- Leverage over a decade of experience in cybersecurity, systems engineering, and leadership within DoD and SCI environments to conduct comprehensive criminal and civil investigations.
- Utilize a strong foundation in risk mitigation, cross-agency collaboration, and security protocol implementation to address critical national security threats, including terrorism, human trafficking, drug smuggling, and financial crimes.
- In pursuit of CISSP Certification to drive risk management and the strategic deployment of scalable security controls.
  - Projected test date of December 2nd, 2025

EDUCATION

SALVE REGINA UNIVERSITY

Master of Arts received May 2013, GPA: 3.7 June 2011 – May 2013

- Degree in Administration of Justice and Homeland Security with a concentration in Cyber-Security and Intelligence
- Researched subject matter consisting of computer networking concepts, high-tech crime, industrial espionage, homegrown and international terrorism, counter-terrorism, intelligence, counter-intelligence, cyber-crime (best practices in safeguarding against), hacktivism, online extortion, basic cyber-forensics, logical reasoning and analytic techniques (methodologies and avoiding analytic pitfalls)

Bachelor of Arts received May 2011, GPA: 3.1 Sept 2007 – May 2011

- Degree in Administration of Justice with a minor in Sociology
- Enrolled in courses pertaining to civil and criminal law, torts, the Constitution, and Homeland Security
- Additional coursework in Psychology, Philosophy, and Economics

EMPLOYMENT

NORTHROP GRUMMAN

Manager Systems Engineering 2 November 2022 – Present

- Lead a team of 13 senior systems engineers, driving technical excellence in cybersecurity initiatives while fostering career development, performance optimization, and conflict resolution, with a focus on collaborative and security-driven solutions in high-stakes environments.
- Direct the design and implementation of cybersecurity requirements and controls for space systems, demonstrating the ability to navigate and mitigate risks in complex technological environments
- Champion the standardization of cybersecurity practices across program architectures, ensuring scalable and consistent security strategies, pivotal for maintaining robust security postures within large corporate infrastructures
- Employ agile frameworks for the efficient allocation, tracking, and execution of program requirements, highlighting adaptability and a proactive stance towards organizational security challenges
- Spearhead architecture reviews and formulate baseline security controls, utilizing knowledge in security architecture and risk analysis to enact significant security enhancements and compliance across diverse systems
- Led a 3-month TDY in Australia for a critical installation of computer networking equipment, serving as the project's primary cybersecurity expert
  - Ensure stringent customer requirements were met, overseeing cybersecurity protocols and conducting validation tests
  - Directly engage with on-site personnel, enhancing customer trust and satisfaction through expert guidance and communication
  - Navigated complex, cross-cultural challenges to deliver high-stakes cybersecurity solutions, demonstrating adaptability and excellence

Senior Principle Cyber Systems Engineer May 2020 – November 2022

- Championed secure protocol adoption by the enterprise
- Adjudicated RMF Requirements traceability using DOORs and JIRA Confluence
- Vetted SW with CVE analysis for program/customer approval
- Developed security integration and testing plans for various applications and operating systems (CTP Compliance Events)
- Performed HBSS/EVSS vulnerability and compliance scans, review, and mitigation adjudication
- Developed and adjudicated work instructions for various Systems Security Engineering processes: PPSM, STIG, SW Approval
- Established body of evidence (BOE) plans for adjudication within the SCTM
- Draft and publish technical documentation for CDRL and non-CDRL customer deliveries

RAYTHEON

ISSM - Information Systems Security Manager November 2018 – May 2020

- Managed a team of 8 direct reports; providing guidance, support and direction in order to satisfy program requirements and maintain NIST compliance
- Interfaced with both the program and the customer in order to satisfy milestones requiring Information Assurance prerequisites
- Trained my direct reports and others on weekly auditing requirements such as: Assured File Transfer (AFT) processes & tools, Splunk, Lumension (Device Control), investigative methodologies and identifying & reporting security anomalies
- Developed keen insight on a wide array of Special Test Equipment to include the sanitization, implementation and disposition of such equipment
- Cultivated an environment that fosters best practices and a security posture consistent with expectations identified and mandated by the DAAPM v.2.1
- Independently traveled offsite to customer and sub-contractor locations to aid in standing up and maintaining information systems for accreditation under RMF

Senior Information Assurance Cyber Specialist July 2017 – November 2018

- Assisted in identifying solutions to complex compliance and security problems by using effective written, speaking, analytical, project management, organizational, and customer service skills
- Performed Assessment and Authorization activities such as documentation preparation, system configuration/validation, and certification testing
- Performed security sustainment activities such as hardware/software change management, account management, media protection and assured file transfers
- Experience with various information system security assessment/hardening tools like DISA STIGs and SCAP benchmarks
- Conducted technical and nontechnical reviews and audits of multiple classified information systems
- Worked in DoD environment ensuring RMF/DAAPM requirements and compliance
- Conducted self-inspection and audit trail review

Senior Systems Engineer @ DISA Headquarters February 2017 – July 2017

- Installed new (while maintaining current) servers and configured hardware, peripherals, services and settings in accordance with best practices for Windows 10 systems and Windows 2008 servers
- Performed daily system monitoring, verifying the integrity and availability of all hardware, server resources and systems while reviewing system and application logs
- Performed daily backup operations, ensuring all required file systems and system data are successfully backed up to the appropriate media and sent for offsite storage, following NIST best practices.
- Implemented and documented research methods while recommending innovative approaches in order to repair and recover from hardware or software failures
- Applied OS/Application patches and upgrades on a routine cadence Non-Export Controlled – See Sheet 1

Computer Systems Technologist August 2015 – February 2017

- Provided system administration support in a classified engineering environment for Linux/Unix (Red Hat, Solaris, HP-UX) and Windows Servers, Windows 2007/Win2k8, storage arrays (network appliance) and disaster/recovery backup systems
- Actively maintained an estimation of 40 of the company's computer systems on 3 separate networks while managing user account and data administration in accordance with each network's security requirements
- Proficient at comprehensively explaining complex technical concepts to clients and non-technical staff
- Timely and efficiently responded to computer system anomalies while implementing keen intuition
- Performed all aspects of asset management including the certification, sanitization and disposition of classified assets
- Performed data backups and assist with data recovery while following Veritas NetBackup Administration guidelines
- Function with an excellent client service record
- Ensure and maintain NISPOM compliance

DENLY GARDENS

Acting Manager / IT Support Sept 2008 – August 2015

- Integrated front of house and back of house operations by deploying, maintaining and troubleshooting a PoS system; enhancing efficiency and fiscal organization
- Stood up and maintained a set of a series of point of sale equipment with a smart register while integrating them over a secure LAN
- Implemented physical and administrative hardening techniques to ensure that the integrity, confidentiality and availability of the networked PoS system remains secure
- Performed daily monitoring and routine backups of all sales logs generated and audited the use of voided transactions to prevent misuse and theft
- Perform routine updates to the PoS clients in order to ensure that security vulnerabilities are patched
- Led a server team of 7 staff members and instructed on processes for the use and maintenance of the hardware and software of the PoS system
- Ensure that best practices are in place with respect to WiFi access, staff training, secure safes and protected PoS systems

SKILLS AND INTERESTS

- *CompTIA Security+ CE, Splunk Power User, 6Sgima* Certified
- Proficient in Database research, Splunk, Microsoft Office, Active Directory, VMware, Group Policy, Lumension (Ivanti) and network navigation & monitoring
- Knowledgeable with Mac OS, HP-UX, Solaris, Red Hat and Windows
- Fundamental understanding of TCP/IP concepts
- Enjoy physical fitness, keeping up to date with technological trends, gastronomy, rock climbing, traveling, and learning about unfamiliar cultures