**Joel E. Astore**

16206 Fantasia Dr

Tampa, FL 33624

Mobile: 850-503-6974, Email: joel.astore@gmail.com

**Personal Profile**

Over fifteen years of professional experience supporting the Air Force, Army, Navy, and Marine Corps provides various avenues of knowledge, processes, and software suites building a strong foundation for further growth in the field. Supporting ATOs across branches and classification levels has enabled a well-versed understanding of varying Plans of Action & Milestones (POA&M) platform approaches, each with the same goal of supporting Risk Management and Assessment.

**SECURITY CLEARANCE:** Top Secret (2019) SCI (2019)

**EDUCATION**

***Bachelors of Science in Network Security*** May 2014

ECPI University (Virginia Beach, VA)

***Masters of Science in Information Assurance*** June 2016

Strayer University (Virginia Beach, VA)

**PROFESSIONAL CERTIFICATIONS**

* CompTIA Security+

**PROFESSIONAL EXPERIENCE**

*Computer Network Defense Analyst*  Jul 2022 – Current

Technical Solutions and Maintenance, Inc (MacDill AFB, FL)

* Support J6 incident response team to include monitoring, tracking, and creating incident response Remedy tickets utilizing the Cyber Kill Chain methodology.
* Support incident response for all SOCOM network devices to include Windows, Linux, Microsoft, and networking devices.
* Collect critical data points supporting the incident based on expertise in incident response life cycle.
* Monitor and analyze activity utilizing Splunk
* Develop, implement, and review rules within HBSS/ESS modules (ENS, DLP, RSD) to support the incident response effort
* Work as a team to ensure constant incident response support through consistent communication across the group to include new threats and suspicious activities.

*Cybersecurity Engineer*  Apr 2022 – Jul 2022

Paragon/Amyx (Remote, FL)

* Develop, tailor, assign, test, and review NIST 800-53 controls for system platforms resulting in direct security risk impact to the platform
* Manage POAM within eMASS including adding, closing, and editing current entries
* Ingest and associate ATO supporting artifacts to include scan results, checklists, and documentation
* Develop plan of mitigation along with determination of controls that require immediate closure
* Support SecDevOps processes and functions for newly developing software supporting system
* Direct developer team in efforts to build RMF package supporting ATO for environment ensuring all resources available to successfully acquire ATO
* Create and review environment policy documents to support ATO efforts and requirements following accepted process to ensure the newly developed policy is distributed to parties integrating changes
* Work with team of engineers to support various accreditation boundaries in varying stages of accreditation

*Wing AP ISSO / ISSO Team Lead*  Aug 2019 – Apr 2022

Jacobs (Eglin AFB, FL)

* Operate within multiple SAP environments following JSIG requirements
* Provide ISSM level support for 53rd Wing AP office as well as all directly reporting groups and squadrons
* Briefed Wing Commander, supporting Squadron Commanders, and ACC regarding Information Security topics to include status of high threats mitigations, risk of non-compliance, requirements/impacts related to proposed changes, and various other IA focused topics
* Review, refine, and audit all SAP ATO packages managed and submitted through the 53WG/AP office
* Provide guidance and support to ISSOs supporting ATO packages across all RMF life cycle steps
* Develop RMF package templates that incorporate STIG correlation into the control documentation
* Manage all Jacobs’ ISSOs within the 53rd Wing reporting to the AP Wing Office to include time keeping and training
* Support TACLANEs of various levels to include availability, keying, batteries
* Process CAF documentation for 53WG

*Information Assurance/Cybersecurity Analyst* Oct 2018 – Jun 2019

DSA (Charlottesville, VA)

* Developed and maintained ATOs for various network levels
* Continued support of NIPR, SIPR, and JWICS networks to ensure compliance with ATO package
* Create, modify, and implement documentation in accordance with RMF standards for government ISR programs

*Information Assurance/Cybersecurity Analyst* Sep 2014 – Oct 2018

Leidos (Bridgewater, VA/OCONUS Locations)

* ISSO of Leidos VBW Secure Network.
* Design and modify security programs and processes over multiple government Intelligence, Surveillance, Target Acquisition, and Reconnaissance programs
* Create, modify, and implement documentation in accordance with RMF standards for government ISR programs
* OCONUS Information Assurance Lead providing guidance to ensure a positive Information Assurance/Cyber Security posture for two government programs in hostile zones
* Manage privileged and standard user accounts for government programs, confirmation of compliance with account requirements, as well as utilizing JPAS
* Support Information Assurance projects from initial concept to implementation for ISR programs including full support of continuous monitoring and change management process
* Audit multiple environments on a regular basis to assure baseline configuration compliance utilizing STIGViewer, ACAS, Nessus, Nmap, Veeam, and other various supporting software
* Utilize WSUS, Security Center, and Nessus to ensure security risk remains aligned with accepted risk
* Work with team members to make certain programs progress forward as technology and attack approaches change leveraging resources such as DISA, Cisco, RedHat, and Microsoft.
* Support inter-department efforts to provide efficient and effective asset functionality while maintaining little to no risk.

*Network Security Consultant*  Dec 2011 – 2014

Hewlett Packard (Norfolk, VA)

* Oversee build process and upgrade/patch maintenance of over 10,000 Navy and Marine Corp Intranet (NMCI) servers to ensure security in accordance with Department of Defense (DoD) standards
* Utilize ePO, SEP, and SSIM to monitor, detect and counterattack threats to the NMCI network
* Provide Tier 4 support to NMCI wide classified and unclassified workstations/users
* Oversee, delegate, and troubleshoot ticket queue for Information Assurance (IA) Applications team
* Develop, verify, and maintain operational guidelines for NMCI systems
* Provide detection and removal of non-DoD approved software along with spam filtering
* Provide detection, deterrence, containment, and recovery operations for attempted and successful network attacks to guarantee integrity, availability, and confidentiality of NMCI information and assets
* Perform daily administration and maintenance on NMCI classified and unclassified wide area network

*Senior Security Technical Consultant* May 2011 - Dec 2011

Symantec CORP (Norfolk, VA)

* Managed 10,000 plus servers and over 350,000 workstations to ensure no viruses or malware were affecting the NMCI networks
* Oversaw the Symantec Endpoint Protection Manager (SEPM) on NMCI systems
* Utilized SSIM to administer rules and policies on NMCI systems
* Overhauled Symantec solution monitoring and remediation guidelines into a streamlined daily checklist allowing a timelier response to issues detected on all Symantec products found on NMCI networks
* Provided complete protection and compliance for NMCI servers, stopped attacks, and utilized real-time visibility while using the SCSP software
* Prioritized threats by means of maintaining SSIM to allow for logging, management, retention, and analysis of events

**United States Air Force** June 2004 - Feb 2011

*Communications Security (COMSEC) Accountant* - Langley AFB Feb 2010 - Feb 2011

* Managed two COMSEC accounts and supported two networks with support to Head Quarters Air Combat Command, 1 Fighter Wing, 480 Intelligence Wing
* Supervised Emissions Security (EMSEC) certification database overhaul including inspections
* Managed Computer Security (COMPUSEC) program; providing IA visual aids and training 403 IA Officers
* Managed and inspected 80 Secure Voice Responsible Officer (SVRO) accounts preventing COMSEC incidents and compromises
* Issued 300 keys monthly, supporting 20 base agencies, the Global War on Terrorism, Operation Iraqi Freedom, and Operation Endearing Freedom
* Conducted IA assessments on 50 units identifying deficiencies as well as providing instruction to correct

*Network Security Technician* - Spangdahlem AB Germany Feb 2006 - Feb 2010

* Information Assurance Officer for 52nd Communications Squadron
* Administered base Blue Coat proxy server policies to prevent abuse and misuse, safeguarding against attacks and intrusions
* Administered Symantec Mail Gateway on Microsoft Exchange Servers safeguarding users against malicious external attacks
* Utilized Vulnerability Management System tool (VMS) eEye Retina Network Security Scanner bi-monthly to detect vulnerabilities on workstations
* Utilized DISA's VMS Gold Disk utility weekly to detect vulnerabilities on 120 network servers
* Performed daily administration and maintenance tasks on unclassified and classified wide area network
* Ensured peripherals, workstations, servers, communication devices and associated operating systems were secure, on-line and available for user access 24 hours a day
* Established and verified operational procedures for Air Force network servers
* Implemented and managed classified Symantec Antivirus server which protected 26 servers and 400 workstations from malicious tampering and virus infestation
* Configured new tape library leading to backup and recovery capabilities of over 24TB of data
* Assisted in $1.5M United States Air Forces in Europe (USAFE) Smart Client pilot, posturing A6 for go/no-go decision on full Air Force Smart Client implementation

*Certificate Authority* - Langley AFB Dec 2004 - Feb 2006

* Prepared Defense Message System (DMS) encryption cards for command-wide distribution to Air Combat Command (ACC) utilizing Certification Authority Workstations (CAW)
* Received, processed, and coordinated shipment of ACC requests for encryption cards supporting classified and unclassified official messages while strictly adhering to National Security Agency (NSA) policies
* Maintained accountability of data records issuing and revoking Fortezza cards essential to NSA oversight of the DMS program