**Justin J. Hensley**

(540) 690-4121 | justinhens@gmail.com

Manassas, Virginia

**Citizenship:** United States

**Secret Security Clearance:** Current until April, 2024.

**SUMMARY OF QUALIFICATIONS**

* Experienced Information Technology and Cybersecurity leader with proven ability to make well informed, difficult decisions in stressful situations which support the overall objectives and vision for the system/program office.
* Mentored and guided a diverse, often geographically dispersed, group of personnel in order to meet project goals and deadlines.
* Over 19 years of experience in providing successful Information Technology and Cybersecurity support to customers and developing solutions to meet customer requirements.
* Supported FEMA systems as an ISSM for the past 2 years within wide-ranging operational environments, and the previous 4 years as the ISSM for a Marine Corps program office working with Mission Critical, Tactical IT systems on the SIPRNet.
* Deployed in support of OEF 12-1 as the Communications Chief for 1st EOD Company, where I was the touch point for all Very Small Aperture Terminal (VSAT) requirements, with 52 separate systems deployed throughout the Area of Operations.
* Familiarity with the use both the VSAT and Support Wide Area Network (SWAN) in an operational/tactical environment.
* 8570 compliant with Marine Corps cybersecurity course work; technicians and managers courses.
* Managed the authorizations of all assigned systems within the Marine Corps Certification and Accreditation Support Tool (MCCAST), Xacta, and Cyber Security Assessment and Management (CSAM). Familiarity with Enterprise Mission Assurance Support Service (eMASS).
* Familiarity with Splunk, Axonius, STIGs and SCAP, and Tenable Nessus Security Center.
* Familiarity with the SDLC processes/lifecycle; both waterfall and agile.
* Core Competencies Include:

Process Improvement Leadership & Personnel Development

Information Security ConMon Activities

Statutory / Regulatory Compliance IT Services Management

FISMA Compliance Assessment and Authorization Process

WORK Experience

**Cybersecurity Lead/Information Systems Security Manager** November 2020 – Present

Purple Jay, LLC., 21882 Brickshire Cir., Ashburn, VA 20148

* Developed and assessed the FEMA Common Control Catalog, working with the Policy and Governance division to address numerous GAO Audit findings and NFRs.
* Administered the Common Control Working Group, managing new DHS/FEMA requirements associated to new GRC tool deployment and the adoption of the NIST 800-53, Revision 5 control set.
* Provided multiple trainings to the entire FEMA cybersecurity workforce; Implementation Statement Standardization training, POA&M Process training, and Control Scoping and Tailoring training.
* Worked hand in hand with the Cybersecurity Policy, Planning, and Training (CPPT) division to update/develop role-based training for System Owners and Information System Security Officers (ISSOs).
* Monitored and ensured compliance with annual FISMA requirements
* Reviewed and provided feedback to system personnel on Contingency Planning activities.
* Train and mentor the ISSO workforce on the requirements associated to the Software Engineering Lifecycle and Risk Management Framework.
* Currently working with the Security Operations Center to integrate NOSC/SOC SaaS solutions into the common control offerings and with the FEMA Cloud Environments to rationalize their offerings for applications onboarding into their environments.

**Software Transition Cybersecurity Lead** September 2020 – January 2021

TriStar Engineering Inc., 1801S. Liberty Dr., Bloomington, IN 47401

* Serving as the liaison between the TriStar software development unit (SDU), Lockheed Martin, and the Marine Corps program office as the cybersecurity lead for the software transition. Providing recommendations and guidance to TriStar staff in all aspects of cybersecurity and information security (IS), to include but not limited to, best practices for incorporating cybersecurity into the software development cycle and systems engineering processes, as well as providing process improvement opportunities.
* These process improvements have taken shape through the creation of a risk management process for the software development unit in conjunction with a CMMI inventory.
* Worked through the Managing Performance and Measurement (MPM) section of the CMMI inventory and creating an MPM plan for the SDU.

**Information System Security Manager** September 2016 – September 2020

Program Manager (PM) Air Command and Control Sensor Netting (AC2SN), Marine Corps Systems Command

* Served as the Information System Security Manager (ISSM) for the Cybersecurity team providing recommendations and guidance to the Program Manager Air Command and Control Sensor Netting staff in all aspects of cybersecurity and information security (IS), to include but not limited to, best practices for incorporating cybersecurity into the acquisition life cycle and systems engineering processes, as well as providing process improvement opportunities.
* In conjunction with managing the assessment and authorization requirements, successfully supervises the FISMA compliance for all the systems within the portfolio throughout the system life cycle.
* Responsible for the successful assessment and authorization for all Programs of Record (PoR) within the Air Command and Control Sensor Netting portfolio and ensuring that cybersecurity / information security is incorporated into the acquisition life cycle at the earliest opportunity in order to reduce cost and schedule inhibitors.
* Assessed, mitigated, and tracked vulnerabilities on the IT Security POA&M for each assigned system in alignment with their Information Assurance Vulnerability Management (IAVM) Plan and requirements outlined in their respective Authority to Operate (ATO) granted by the Marine Corps Authorizing Official (AO).
* Responsible for ensuring baseline DoD cybersecurity controls are applied to systems in accordance with the DoD 8510.01 as well as all other directives and regulations governing the management of a successful cybersecurity program.
* Subject matter expert providing technical guidance for cybersecurity planning, evaluation of Information Assurance (IA) and IA enabled products, development of cybersecurity documentation, and the tracking of all IA products for the Program Manager Air Command and Control Sensor Netting.
* Supervised the development of cybersecurity documentation in accordance with all Marine Corps, DoN, and DoD directives such as the Information Systems Continuous Monitoring Plan.
* Helped redefine the cybersecurity processes and deliverables that the program office used to communicate cybersecurity posture of each system to the SCA, AO, and other outside entities

***Networking Chief*** October 2010 – August 2016

United States Marine Corps, disparate locations

higher Education

***DeVry University, Online*** 2011 – 2014

* Technical Management, GPA: 4.0

**MARINE CORPS SPECIALTY SCHOOLS**

***Cybersecurity Managers Course*** 2016

***Cybersecurity Technician Course*** 2016

***Very Small Aperature Terminal (VSAT) Course*** 2013

***Advanced Satellite Operators Course*** 2013

***Tactical Data Network Operators Course*** 2004

***Data Network Specialist Course*** 2003

***Other Specialty Schools***

* ISACA Certified Information Security Manager (CISM) (May, 2021)
* ISC2 Certified Information Systems Security Professional (May, 2022)
* CompTia Security + CE (September, 2020)
* CompTia Network + (2010)
* Cisco Certified Network Associate (CCNA) (2008 and 2011)
* Equal Opportunity Representative Course (2014)