FALCONWOOD INC.

About Falconwood, Inc:
Falconwood, Inc. is a small, woman/veteran-owned business providing executive level consultants and programmatic support to Department of Defense (DoD) Information Technology (IT) initiatives and programs.

We provide expert consultation on a diverse range of IT subjects focusing on acquisition strategy, implementation activities, and Cyber Security policy and engineering.

We have an immediate opening for a **Cyber Security Analyst** to provide cyber security support to the Navy Manpower, Personnel, Training, and Education (MPTE) Four Pillars of Capability:

The MPT&E portfolio consists of 55 systems that deliver personnel, pay, training, and recruiting capabilities by delivering enterprise-wide information systems through IT requirements management, enterprise architecture, and resourcing for MPT&E IT networks and systems.

Duty Location:
New Orleans, LA; Orlando, FL; Arlington, VA
**Minimal travel may be required.*

The Cyber Security Analyst:

- Provide Cyber Security guidance and documentation throughout the system development life-cycle
- Support the PM, SCA, ISSM, and ISSE throughout all phases of the security authorization process
- Ensure the completion of cyber related programs, projects, or tasks within estimated timeframes and budget constraints
- Provide Cyber Security guidance at meetings, briefings and design reviews, and during system development in accordance with prevailing Cyber regulations and policies
- Ensure Cyber Security system designs that properly mitigate identified threats and vulnerabilities
- Review and approves test and evaluation activities to validate those threats and vulnerabilities are mitigated
- Perform system security reviews and Certification & Accreditation (C&A)/ Assessment and Authorization (A&A)
- Conduct A&A process for IT systems and networks in accordance with the DoD Risk Management Framework process

FALCONWOOD INC.

- Analyze and reviews the results of network and system vulnerability scans and be able to validate the implementation of IA Controls in accordance with DoD 8500.2
- Assist with development and tracking of the POA&M in eMASS · Supports RMF Checkpoint meetings
- Assist with the System Categorization and Risk Assessment Report, and consults on the SLCM Strategy
- Develop the Security Plan, Security Assessment Plan, Security Assessment Report, and Executive Summaries
- Assess C&A impact based on ACAS and STIG results, and identified the strength of the mitigation or remediation
- Report package status and risks weekly to senior level government leadership

Required Qualifications:

- Minimum SECRET clearance.
- 5+ years of experience in cyber security.
- BS Degree in Cyber Security/Engineering field (e.g. Computer, Electrical, Mechanical, Systems, Security).
- Experience with independently performing validator activities defined in the Navy RMF process guide and applying RMF guidance to Navy or DoD A&A efforts
- Experience with test and evaluation for allocating assigned security controls into assessment objectives and procedures, developing and executing Security Assessment Plans (SAP)
- Experience with using the DoD Assured Compliance Assessment Solution (ACAS) suite of tools and the Enterprise Mission Assurance Support Service (eMASS)
- Experience with vulnerability assessment scanning tools and reporting, intrusion detection technologies, intrusion prevention technologies, and host-based security system (HBSS)
- Knowledge of DoD published Security Technical Information Guidance (STIG) requirements and implementation or compliance process
- Firm understanding of DISA CAL boundaries and experience coordinating with the PPSM team to register ports not registered within the latest DISA’s CAL boundary list
- Firm understanding of sensitive data types and cybersecurity protections associated with that data (e.g. PII, PHI, etc.)
- Working knowledge of eMASS at the ISSE/NQV level

FALCONWOOD INC.

- Possess knowledge of current security threats, techniques, and landscape (threat vectors)
- Experience with information systems security requirements to be implemented during system design
- Experience with business/operations solution architectures (i.e. portals, service management, networks, inventory).
- Skilled in project management and engineering technical management techniques, principles, and practices.
- Proficiency in Microsoft Office applications, particularly Visio, Word, Excel and PowerPoint.
- Ability to think independently with minimal oversight, as well as demonstrate exceptional written and oral communications skills.
- Exemplary customer/client management skills and techniques.

Desired:

- MS Degree in Cyber Security/Engineering field (e.g. Computer, Electrical, Mechanical, Systems, Security).
- 10+ years of cyber security experience.
- IAM/IAT III - Certified Information Systems Security Professional (CISSP) Certification or equivalent
- Navy Qualified Validator (NQV) Level II Certification
- Experience with contingency planning, firewall policy, and ports and protocols, and service management
- Experience with Microsoft Public Azure, Azure Pack and Azure Stack and related Microsoft technologies (Hyper-V, ADR, SCCM, SCOM).
- Familiarity with DON Fleet command structure
- Familiarity with DON network architecture

Please reply directly to this position description with an updated resume and your salary requirements directly to Tiffany Cannon at tcannon@falconwood.biz.

Tiffany A. Cannon
Falconwood, Inc.
Office: 703.888.4328
Email: tcannon@falconwood.biz

FALCONWOOD INC.