FALCONWOOD INC.

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

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

We have an immediate opening for 2 **Cybersecurity Operations Analysts** to support to the Navy Enterprise Resource Planning (ERP) N-ERP. The successful candidate will perform continuous SAP application-level or Network-level cyber security monitoring and reporting using a variety of tools. Successful operation and maintenance of ONAPSIS is required for this position. Other tools are listed below.

Duty Locations: Washington Navy Yard

Desired Skills:

- Able to develop custom scripts and employ program selected cybersecurity monitoring tools to monitor PMW 220 systems for unauthorized accesses or system changes and other unauthorized/malicious activities in an enterprise-level system consisting primarily of Unix and Windows based operating systems, databases, and SAP application software found in three tier information systems. SAP BASIS and/or SAP HANA experience a plus.
- Possess the ability to develop and maintain associated documents to include event escalation and closure processes.
- Must have the skills required to deploy and use platform and application vulnerability scanning tools to detect vulnerabilities, assess risk and recommend mitigation activities.
- Must have the skills necessary to assess DoD RMF based security program implementations, identify weaknesses and recommended and implement corrective actions.
- It is preferred that the candidate possess the skills necessary to perform code reviews manually but may also employ automated tools, such as Fortify, to detect coding flaws.
- It is required that the candidate possess the skills necessary to assess the effectiveness of the implementation of DISA STIGs with regards to platforms and applications.
- Knowledge and use of eMASS desired.
- Must have the ability to communicate effectively in writing and verbally.
- Must be able to work effectively independently and as part of a group.
- Must have knowledge of the tools and techniques to effectively and efficiently perform network and application penetration to assist in the development of plans to execute red/blue team penetration testing as required in support of COTs information systems residing within a cloud environment. Familiarity with common three-tiered information system architectures is required.

Qualifications:

FALCONWOOD INC.

- 3 to 5 years of experience working in a cybersecurity operations environment maintaining the security of enterprise level financial information systems in virtual and/or cloud environments (PaaS).
- The candidate MUST have familiarity with SIEM tools, vulnerability scanning tools, monitoring tools and automated security assessment tools.

• **Event Tracker**	• **MS Powershell**
• **Tripwire**	• **SIEM Dashboard**
• **ACAS Scans**	• **HBSS**

- Will have significant knowledge of and experience with the implementation of NIST, DoD and Navy RMF policies, standards and guidance employed to obtain IATTs, ATO and to successfully perform continuous monitoring of information system controls, associated vulnerabilities and manage associated risks.
- Hands on IT experience (applications development, server build, Active Directory experience) understanding of encryption algorithms.

Must have or be able to obtain and maintain a SECRET security clearance

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.