

Here is another opportunity that just opened at ManTech for a contract at Nellis AFB, NV (see below and attached). Please feel free to share with your employment networks. Interested candidates should apply online using this link:

<http://jobs.brassring.com/tgwebhost/jobdetails.aspx?partnerid=10696&siteid=45&jobid=1322650>

They may also send their resumes directly to: [Emily.Eskelsen@mantech.com](mailto:Emily.Eskelsen@mantech.com)

A current TS/SCI clearance is required.

### Security Control Assessor (SCA) I

Current Position	Recommended New Position #
107	184
108	185
109	186
110	187
111	188
117	189
131	190

The SCA is responsible for conducting a comprehensive assessment of the management, operational, and technical security controls employed within or inherited by an IS to determine the overall effectiveness of the controls (i.e., the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system). SCAs also provide an assessment of the severity of weaknesses or deficiencies discovered in the IS and its environment of operation and recommend corrective actions to address identified vulnerabilities. Responsibilities will cover Collateral, Sensitive Compartment Information (SCI) and Special Access Program (SAP) activities within the customer's area of responsibility.

**Duties may include:** (may be modified with concurrence of the Contracting Officer and the Contract Program Manager)

- Perform oversight of the development, implementation and evaluation of information system security program policy; special emphasis placed upon integration of existing SAP network infrastructure
- Perform assessment of information systems, based upon the Risk Management Framework (RMF) or the JAFAN 6/3 process
- Advise the Authorizing Official (AO) and/or Delegated Authorizing Official (DAO) on any assessment and authorization issues
- Advise the Authorizing Official (AO), Delegated Authorizing Official (DAO) and Program Security Officer (PSO) on assessment methodologies and processes

- Evaluate Authorization packages and make recommendation to the AO and/or DAO for authorization
- Evaluate Information system threats and vulnerabilities to determine whether additional safeguards are required
- Advise the ISO and PSO concerning the impact levels for Confidentiality, Integrity, and Availability for the information on a system
- Evaluate threats and vulnerabilities to information systems to ascertain the need for additional safeguards
- Review and approve the information system Security Assessment Plan, which is comprised of the SSP, the SCTM, and the Security Control Assessment Procedures
- Ensure security assessments are completed for each IS
- At the conclusion of each security assessment activity, prepare the final Security Assessment Report (SAR) containing the results and findings from the assessment
- Initiate a POA&M with identified weaknesses and suspense dates for each IS based on findings and recommendations from the SAR
- Evaluate security assessment documentation and provide written recommendations for security authorization to the AO
- Develop recommendation for authorization and submit the security authorization package to the AO
- Assess proposed changes to information systems, their environment of operation, and mission needs that could affect system authorization
- Ensure approved procedures are in place for clearing, purging, declassifying, and releasing information system memory, media, and output
- Assist in team and PSO compliance inspections
- Assist the PSO's with security incidents that relate to cybersecurity and ensure that the proper and corrective measures have been taken
- Assess changes within the information system boundary that could affect the authorization of the boundary
- Ensure that Information systems requirements are addressed during all phases of the system life cycle

**Experience:**

- 7 – 9 years related experience
- Minimum of four (4) years experience in SAP and Collateral Information Systems (IS) Security and the implementation of regulations identified in the description of duties.

**Education:**

- Bachelors degree in a related discipline or equivalent experience (4 years)

**Certifications:**

- Must meet position and certification requirements outlined in DoD Directive 8570.01-M for Information Assurance Technician Level 3.

**Security Clearance:**

- Current Top Secret Clearance with SCI Eligibility
- Eligibility for access to Special Access Program Information
- Willingness to submit to a Counterintelligence polygraph

**Other Requirements:**

- Must be familiar with security policy/manuals and the appropriate DCIDs/JAFANs and other guiding policy documents.
- Must have the ability to work in a dynamic environment and effectively interact with numerous DOD, military/civilian personnel and industry partners
- Working knowledge of Microsoft Office (Word, PowerPoint, and Excel)
- Possess a high degree of originality, creativity, initiative requiring minimal supervision
- Willingness to travel within the organizational geographic Area of Responsibility (AOR) (note - could be extensive, and will include both air and ground transportation)
- Must be able to lift 50 lbs