Job Title: Information Security Technical Specialist

Reference Code: 2015-06-03-Information Systems Security Officer (ISSO)

About the Position
Specialty Systems, Inc. has an immediate opening for an Information Systems Security Officer (ISSO)/Information Systems Security Engineer who will be responsible for leading and performing the activities necessary to maintain security and establish functioning external barriers, define/create/maintain the documentation for certification and accreditation of research and development labs and Program of Record systems in accordance with government requirements. The ISSO will assess the impacts on system modifications and technological advances. Additionally, the ISSO will review systems in order to identify potential security weaknesses, recommend improvements to amend vulnerabilities, implement changes and document upgrades. In this position you will work at our customer’s site located a few short miles west of our Toms River, NJ office. You will also work our customer’s Compressed Work Schedule which consists of working four 9 hour days, an 8 hour day for the first week of a cycle followed by four 9 hour days and being off on the second Friday for the second week of a cycle. This results in a 3 day weekend every other week!

About the Company
Specialty Systems, Inc. is an Information Technology and Engineering Services provider serving customers across the Federal Government, NJ State and Local Governments, and private industry markets. Founded in 1978, our mission is to understand our customers’ business problems and leverage emerging technologies to provide solutions that deliver radical and dramatic improvements in operational efficiencies and productivity. We facilitate a stimulating and creative work environment by engaging in ambitious and challenging projects while at the same time recognizing the need to have some fun via our monthly Thirsty Thursday gatherings, season tickets for the Phillies Class A
Lakewood Blue Claws baseball games, annual company picnic and Softball Challenge, and our business casual dress policy.

**Job responsibilities will include:**

- Developing Information Assurance (IA)/Cybersecurity strategies.
- Developing Information Assurance/Cybersecurity plans for the new networks and labs connected the Navy’s Research, Development, Test and Evaluation network.
- Developing Information Assurance/Cybersecurity plans for Navy Programs of Record (PORs)
- Defining connectivity and interface requirements.
- Applying DoD IA and Information Security (IS) policies and standards.
- Assessing system/software risk and vulnerability.
- Supporting IA/Cybersecurity integration.
- Preparing IA/Cybersecurity support documentation.
- Developing DIACAP packages for the certification and accreditation of both new and existing networks/labs/Programs of Record.
- Monitoring the security posture of assigned networks/labs/programs and develop remediation and mitigation plans and tasking to address vulnerabilities.
- Performing remediation of IAVAs, harden servers and workstations.
- Attend systems meetings and IPTs to support the Navy PM for all Cyber Security matters throughout the lifecycle of the system from inception to disposal.
- Performing security related some system administration tasks as required.

**Position Qualification Requirements:**

**Education, Certification, Clearance and Years of Experience:**

- Must have a bachelor of science degree in Computer Science, Electrical Engineering, or a related technical field.
- Must have Security+ CE certification.
- Certified Information Systems Security Professional (CISSP) certification or equivalent is a plus.
- Must have a Secret Clearance and have the ability to obtain a Top Secret Clearance.
- At least 5 years of IA/Cybersecurity experience, including demonstrated knowledge, skills, and abilities to perform the job responsibilities listed above.

**Technical:**

- Must have demonstrated experience applying DoD IA and Information Security (IS) policies and standards.
- Must be fully knowledgeable with Department of Defense IA/Cybersecurity Directives.
- Must have experience performing all of the above listed job responsibilities.
- Must have experience with Retina or ACAS scanning tools.
- Experience with the eMASS certification and accreditation database is preferred.
- Experience with Risk Management Framework (RMF) is a plus.
• Experience as a Validator for Department of Defense systems, programs, or networks is a plus.

This is a full time, salaried position with our complete benefits package which includes paid vacation, holiday, sick/business leave, medical insurance, dental insurance, life insurance, short and long term disability insurance, tuition reimbursement, 401k retirement plan with a competitive corporate matching program, incentive bonus program and much more.

Salary Information
This position has a salary range of between $75,000 and $105,000, based on the candidate’s match to the skill and experience levels required.

Candidates interested in this position should apply online:
https://home2.eease.adp.com/recruit/?id=17540842

EOE/AA Minorities/Women/Disabled/Veteran status/all protected classes/VEVRAA Federal Contractor. If you are a qualified individual with a disability or a disabled veteran and need to request a reasonable accommodation for any stage of the application/interview process, please contact: 732-814-8138

Ability to obtain Department of Defense secret level security clearance is required. Applicants selected will be subject to a U.S. Government security investigation and must meet eligibility requirements for access to classified information. Due to the nature of work performed within our facilities, U.S. citizenship is required.