

To apply for one of these career opportunities, or for more information, please contact:

resumes@govsg.com

Mid IA Vulnerability Management Lead

- Assess and implement identified corrections (e.g., system patches and fixes) associated with technical vulnerabilities as part of the Information Assurance Vulnerability Management (IAVM) program, consistent with DoD Directive 8500.1, and DoD Directive O-8530.1.
- Maintain configuration control of hardware, systems, and application software.
- Identify and properly react to security anomalies or integrity loopholes such as system weaknesses or vulnerabilities.
- Install and administer user identification or authentication mechanisms.

Job Title: 8570.1M Information Assurance (IA) Workforce Management

Clearance: Able to obtain DOD Secret Clearance.

Job Description

The ideal candidate must be able to demonstrate a broad range of skills necessary to manage the IA Workforce

Tasks will include a full range of IA Workforce activities including:

- Creating and maintaining the overall Plan of Action and Milestones (POA&M) for the DoD client, ensuring that DoD 8570 requirements are met for IA training and certification.
- Develop and coordinate training plans for all IA personnel.
- Disseminate appropriate IA workforce information to designated team members.
- Assist customers in updating training records.
- Participate in IA meetings as necessary.
- Identify and recommend IA Workforce training classes and opportunities.
- Track appropriate metrics to monitor the effectiveness of the IA workforce management program.
- Coordinate with the Contracts Division that contract language reflects training and certification requirements.
- Prepare status reports to brief management.

- Additional tasks may include data collection, drafting technical white papers, briefings, research, and hands on technical support as required.

Required Skills

- Ability to work independently with team members, client representatives, and with limited supervision.
- Minimum of 3 years of experience in the Federal, DoD, and/or Intelligence Community.
- Experience with DoD 8570 requirements.
- 3+ years of experience with IA workforce issues including POA&Ms, reporting, training and metrics.
- Must hold or be able to obtain and maintain a security clearance.

Job Title: Mid FISMA Lead

Clearance: Able to obtain DOD Secret Clearance.

Job Description

The ideal candidate must be able to demonstrate a broad range of Federal Information Security Management Act (FISMA) security and privacy skills, ensuring Federal compliance with all FISMA controls.

Tasks will include a full range of FISMA activities including:

- Updating FISMA data utilizing existing tools to develop an accurate listing of FISMA compliance metrics
- Identification of deficiencies and the tracking of deficiencies through a Plan of Action and Milestone (POAM).
- Working with all business units to ensure all relevant controls are in place.
- Ensuring that appropriate documentation and test evidence is captured and appropriately stored and maintained.
- Utilizing appropriate tracking tools to monitor ATOs, Contingency Plans, Continuity of Operations Plans (COOP Plans).
- Interacting with DOD clients to understand their security policies and ensure that projects appropriately comply with their requirements
- Track appropriate metrics to monitor the effectiveness of the IA program in the areas of C&A and FISMA.

- Additional tasks may include data collection, drafting technical white papers, briefings, research, and hands on technical support as required.

Required Skills

- Ability to work independently with team members, client representatives, and with limited supervision.
- CISSP, CISM, CISA or CIPP.
- Minimum of 3 years of experience in the Federal, DoD, and/or Intelligence Community.
- Experience with FISMA and FISMA controls.
- 3+ years of experience documenting security plans, procedures, policies, standards, risk assessments, contingency plans, and POA&Ms.

Must hold or be able to obtain and maintain a security clearance.

Mid Platform IT Lead:

Derived from DoDD 8500.1, Paragraph E2.1.16.4, Platform IT::

1. REFERS TO computer resources, both hardware and software, that are physically part of, dedicated to, or essential in real time to the mission performance of special-purpose systems. PIT does not include general purpose systems.

2. MAY:

- a. Reside aboard or on a platform
- b. Be stand-alone
- c. Have an interconnection to other Platform IT (known as a “Platform IT-to-Platform IT Interconnection”)
- d. Have a Platform IT Interconnection (see DoDI 8500.1) to other IT that is not Platform IT (e.g., a general-use ship’s network, such as ISNS, or a non-Platform IT system)