GENERAL SECRETARIAT OF THE ORGANIZATION OF AMERICAN STATES

Secretariat for Administration and Finance (SAF)
Department of Information and Technology Services (DOITS)

CALL FOR RESUME

Type of contract: Consultant

Field: Information Security Support

Location: Remote or GS/OAS Headquarters

Remuneration: Final remuneration will be based on skills, experience and workplace location

Start date: August 1st, 2022

Duration: Up to 12 months

Deadline for Application: June 27th, 2022

The Department of Information and Technology Services is responsible for managing all Systems and Technology infrastructure resources and personnel, including all matters related to the plans, policies, procedures and standards governing the utilization of technology resources and management of information technology services of the General Secretariat of the OAS

Candidates will be responsible for technical aspects related to Security Systems implemented at the GS/OAS. The main role is to provide hands-on operational capabilities to the GS/OAS Information Security Architecture. Operations activities include successfully maintaining network security appliances, perimeter security systems and security controls, along with the associated documentation, diagrams and procedures. Additionally, Network Security Engineer is responsible for the installation, configuration, maintenance and upgrade of the Information Security systems.

DUTIES AND ACCOUNTABILITIES

- The areas of concentration encompass the following fields: security penetration research, information security diagnostic review, information security architecture and design, security software evaluation and selection, application security review, risk assessment, data classification, help in the development of security related policies, procedures and standards, Internet security devices and network security.

- Support the CISO in all technical aspects regarding investigations of security breaches, related to information technology infrastructure and information.
- Aid in the enforcement policies pertaining to the use of information resources such as digital information resources, security of wireless systems, remote access to the organization's network, and digital interaction with OAS offices away from headquarters, OAS's missions, partner organizations and local businesses.
- Utilize information security tools in order to prepare reports to evaluate the information security posture of the Organization.
- Monitor OAS information technology infrastructure; identify new threats and vulnerabilities and recommends the use security solutions.
- Help in the development of tools and processes geared to help the areas to evaluate information systems and operations particular of the area to determine contingency requirements and priorities. Provide guidance to identify business practices that are dependent on computer and telecommunications systems and that in the event of an incident may severely affect the primary functions of the organization.
- Testing and Evaluation of new products and technologies. Prepare various technical reports.
- Perform other related duties as assigned.
- Define security controls aligned with Software Development Lifecycle
- Oversee adherence to information security policies and procedures.
- Within the delegated authority, is responsible for the support of GS/OAS information security Architecture, including servers, software and associated hardware.
- Develop procedures and strategies for information security administration and maintenance; create and maintain comprehensive documentation for all implemented security solutions.
- Research and recommend information security solutions to meet organizational growing requirements. Recommend new technology products and configurations to address specific customer requirements.
- Acquire and maintain knowledge of OAS systems and standards, security policies, support policies, and methods.
- Provide feedback on the effectiveness of the implemented security products by preparing reports as needed; make recommendations for acquisition of information security products; provide justification for equipment and services.
- Attend team meetings held with senior technical staff to coordinate work and solve emerging problems and situations.
- When assigned project manager responsibility, has the overall responsibility for the project to manage the project taking into account integration across all areas and is responsible for:
    - Developing the project plan; estimating and directing project resources; monitoring and managing the project schedule, the project budget and the project risk; dealing with operational issues.
    - Engaging and maintaining communication with stakeholders; organizing project committee meetings, ensuring minutes are taken; reporting to the CISO and other high level officials involved in the project on the strategic issues; communicating project status to project sponsor, all team members, and other relevant stakeholders and involved parties.
    - Preparing Project status reports and project change request; maintaining project documentation.
    - Negotiating and resolving issues as they arise across areas of the project and where they impact on the other activities, systems and projects.
    - Managing project team members and looking after the interest of the project team.
    - Ensure that the project meets requirements and objectives.

REQUIREMENTS

Essential:

- **Education**:
  - Bachelor's Degree in Computer Science, Computer Engineer or similar.
- **Language requirements:**
  - Excellent oral, writing and communication skills in English and Spanish.

- **Professional experience:**
  - 5+ years of progressively responsible experience implementing and administrating information security solutions.
  - 5+ years of progressively responsible experience implementing and administrating network devices and services, computers hardware and software, computer network installation, maintenance and support; network architecture and topologies.
  - Training and experience in planning, designing, installing and maintaining information security solutions.
  - Experience with TCP/IP based networking environments, including knowledge of and experience with the use of standard TCP/IP model.
  - Experience with open source information security solutions.
  - Experience administering CISCO, Palo Alto security solutions.
  - Experience with Web Application Firewall solutions.
  - Experience working with Microsoft Azure and M365 Security/Compliance Services including ID and Access management, Threat Protection, Cloud Security, Microsoft Defender, Intune, Information Protection and Governance, Risk Management and Compliance Management.
  - Experience installing and configuring computer systems in a networked environment, applying diagnostic techniques.
  - Broad understanding of computer networking technology, system analysis and design techniques, project management and information systems development. Thorough knowledge of network operating systems and protocols, Linux and Windows environments, and network manager applications.

Desirable:

- Advanced University Degree (Master's) in Information Security.
- Certification in one or more of the following technologies preferred: Microsoft Security Technologies, Cloud Security, OCSP, GIAC Certifications, CISSP, CCSP Network Security, Incident Response.
- Knowledge of SIEM platforms.
- Experience working with Risk Management and compliance.

SUBMISSION OF APPLICATIONS:

Interested candidates should send their CV and cover letter (no more than 250 words) with the subject "Information Security Support" to DOITS-CV@oas.org no later than June 27th, 2022.

No phone inquiries accepted. Only shortlisted candidates will be contacted.