

**SP-1**  
**TASK PROPOSAL PART**

**1. Task Proposal**

- 1.1 Task Proposal ID:** 15/SIO-001 **Date received in SPA:** 2015-03-13
- 1.2 Task Title:** Expert - System Security Analyst
- 1.3 Requester / Division / Section:** Simmons,L / SGIS / SIO
- 1.4 Is this a CFE task?** Yes
- 1.5 Task Category:** D
- 1.6 Is this a joint task for MSSPs?** No
- 1.7 Is multiple acceptance required?** No

If 1.6 or 1.7 is yes, indicate the reason:

**2. Project**

- 2.1 Project ID:** SGIS-002 **Project Type:**
- 2.2 Project Title:** Information Security and Infrastructure
- 2.3 Project Manager / Division / Section:** / SGIS / SIO

**3.**

## 4. IAEA Proposed Work Outline

### 4.1 Major task stages with timing:

#### Coordinate Security Efforts

Represent Safeguards while coordinating with the Department of Management (MT) and the IAEA's Central Security Coordinator (CSC) regarding implementation of processes and controls associated with the adoption of international security standards and best practices and leveraging synergies between SG and MT (ongoing during the 24 months)

#### Develop IT Security Policies and Procedures

Create / evolve IT Security policies, procedures, guidelines and standards taking into account Safeguards business needs and industry best practices for IT security. Identify and address gaps in existing policy and procedural documentation.

#### Documentation Compliance

Manage existing repository for all IT security documents, reports and assessments. Design and maintain new taxonomies to enhance accessibility while enforcing defined authorization policies. Ensure information security controls are adequately documented for all systems and processes and are traceable to respective policies.

#### IT Security Validation

Validation of implemented security controls (compliance with defined baselines, standards and processes). Liaison with internal/external auditors to provide evidence of security control compliance when requested.

#### IT Security Incident Response

Participate in or lead incident response investigations. Perform initial/shallow forensic analysis in order to determine severity of suspicious events. Support all phases of incident response activities (i.e., preparation, response, identification, containment, eradication, recovers, lessons learned).

---

#### Reporting

Enhance existing security reports. Design and generate technical reports containing interesting security events and alerts. Design and generate Safeguards management-focused reports containing metrics, activity and resource utilization information used to prioritize allocation of resources.

#### IT Security Support

Provide network security support as needed in the functional areas of :

- . Firewall administration,
- . IDS/IPS maintenance, development (custom signature) and monitoring.
- . Network access control (NAC)
- . ACL reporting
- . Secure VPN

---

**4.2 Support Division(s) / Section(s):** SGIS / SIO

**4.3 End User Division(s) / Section(s):** SG / ALL

4.4 Estimated duration in months: 24

## 5. Safeguards Approval Process

5.1 Suggested MSSPs: USA

5.2 Reason(s):

5.3 To be approved by Committee: SMC

5.4 Committee approval date: 2015-03-17

Comments:

## 6. Acceptance by MSSP(s) - under review

*Date of last update:* 2015-03-13

*Updated by:* KADAVYA

# Job Description for Professional Posts

<b>Position and Grade:</b>	Systems Security Analyst (P4)
<b>Organizational Unit:</b>	IS SGIS Department of Safeguards
<b>Duty Station:</b>	Vienna
<b>Type/Duration of Appointment:</b>	Cost Free Expert/2 Year

## Organizational Setting

The Department of Safeguards is the organizational hub for the implementation of IAEA safeguards. The IAEA implements nuclear verification activities for some 180 States in accordance with their safeguards agreements. The safeguards activities are undertaken within a dynamic and technically challenging environment including advanced nuclear fuel cycle facilities and complemented by the political diversity of the countries.

The Department of Safeguards consists of six Divisions: three Operations Divisions: A, B and C, for the implementation of verification activities around the world; three Technical Divisions: Division of Concepts and Planning, Division of Information Management, and Division of Technical and Scientific Services; as well as two Offices: the Office of Safeguards Analytical Services and the Office of Information and Communication Services.

Within the Department of Safeguards, the Office of Information and Communication Systems (SGIS) is the centre of competence for the specification, development and maintenance of information and communication technology (ICT) systems and for the management of all ICT infrastructure and services to support safeguards. In partnership with other organizational entities, SGIS is responsible for planning and implementing an ICT strategy as well as enforcing ICT standards.

The Infrastructure Section is responsible for providing secure, reliable, and dependable computing, collaboration, database and communications services to the Department of Safeguards. The Infrastructure Section cooperates with other Sections and Divisions in the Department of Safeguards to deliver IT services at a very high standard.

---

## Main Purpose

The Systems Security Analyst will work to strengthen and improve the overall IT security posture of the Department of Safeguards by providing IT security support on security devices and implementing technical controls, providing IT security incident response support, performing IT security vulnerability management, developing IT security procedures and policies, producing IT security reports and coordinating IT security efforts.

## **Role**

The Systems Security Analyst is an IT security expert and will provide advice and guidance on a broad range of IT security topics which include intrusion detection and prevention, IT forensics, auditing and remediation, access controls, penetration testing, risk assessments, policy compliance and procedural development. In addition to providing expert advice in these areas, the Systems Security Analyst will be an implementor of IT security solutions drawing on hands-on practical experience in the areas mentioned above.

## **Partnerships**

The Systems Security Analyst collaborates extensively with other members of the security team, networking team, systems team, data integration team, software development team, project managers and the business architects, providing technical expertise to achieve secure, operational and sustainable solutions. He/she works with external vendors and product suppliers on new information and technical specifications to evaluate and assess the suitability and effectiveness of their products. The Systems Security Analyst collaborates with the Department's Central Security Coordinator regarding IT security policy, compliance, auditing and procedures.

## **Functions / Key Results Expected**

- Work to improve the automatic detection and classification of security events in the ITC systems of the IAEA through the development of tools, processes, procedures, and automation measures.
- Identify and create crucial security alerts based on multi-event correlation and anomalies by writing correlation rules in the Security Incident and Event Management systems as well as custom scripts and reports.
- Enhancing existing security reporting
- Administer, maintain, monitor, audit and document firewall, IDS, IPS, NAC, LAN & WAN, and VPN systems
- Regular program of vulnerability assessment and management and developing metrics to report on the effectiveness of the program
- Assist with threat and risk assessment and prioritizing resources towards remediating the highest risks
- Create automatic and regular attestation reports on access controls
- Participate in incident response investigations and improve the overall security through clear reporting of the results
- Validating security controls

---

## **Knowledge, Skills and Abilities**

- - Expert knowledge of and in-depth technical skills in all aspects of IT security, including firewall systems, intrusion detection/prevention systems, encryption, public key infrastructure, virtual private networks and access control

**RESTRICTED**

- Scripting and/or development experience sufficient to create automated tools and reports to increase the performance of security event handling and to produce useful information for incident handlers in languages such as Perl, UNIX shells, Python, and tools related to the Microsoft .NET stack
- Experience with the installation, management and development of an enterprise security event management system such as ArcSight, with expertise in creating correlation rules
- Demonstrated experience with IT security assessments and vulnerability management especially as such experience applies toward developing a regular, measurable program of improvement
- A broad and thorough knowledge of penetration testing and vulnerability assessment tools and techniques
- Fully immersed in TCP/IP networking technologies and especially the security aspects related to such networks and systems such as packet analysis for both deep inspection and trends.
- Excellent analytical skills: Ability to analyse complex security requirements and propose solutions, and analyse event data such as logs and signatures and draw appropriate conclusions
- Thorough knowledge of and practical experience with security incident response and management processes
- Strong planning and organizing skills to set clearly defined objectives, plan activities in a timely manner and monitor performance against deadlines and milestones
- Learning attitude: Exhibits quick learning skills for new systems and requirements
- Additional skills that would be very beneficial include: application security assessments; threat modelling; network anomaly detection; malware kill chain analysis and malware signature detection
- Strong interpersonal skills: Ability to work in a pro-active manner in a multicultural environment with sensitivity and respect for diversity

---

**Education, Experience and Language Skills**

- Advanced University (or equivalent) degree (Masters) in information technology or computer science
- At least seven years of relevant working experience in one of the fields mentioned above, including at least four years in networking
- Excellent technical knowledge and experience in communications and network architecture and design
- Practical and demonstrated experience in conducting forensic acquisitions and examinations for a variety of platforms, operating systems and file systems, including Windows (FAT & NTFS), Macintosh (HFS+), Linux (EXT2/3); and hands-on experience in forensic tools
- Excellent skills in capturing and analysing network traffic for both incident investigation and issue resolution

**RESTRICTED**

- Managing security incidents, analysis and reporting
- Formulating, developing and implementing IT security policies and procedures
- Scripting and development skills in relevant languages such as Python and C#
- Practical, recent experience with wide area networking, local area networking, Cisco networking products, Juniper Netscreen products and the Microsoft Windows and UNIX operating systems
- Thorough knowledge and hands on experience in products such as Cisco networking equipment, Checkpoint firewalls, intrusion detection systems
- Experience in evaluating third party products, conducting technical feasibility studies and assessing the suitability of products desirable
- Excellent written and oral ability in English as well as presentation skills
- Knowledge of and practical experience with IT service quality standard (ITIL) processes desirable.
- Knowledge of the ISO 27000 series standards for Information Security Management.
- Fluency in written and spoken English essential. Working knowledge of other IAEA official languages (Arabic, Chinese, French, Russian or Spanish) as well as German desirable

<b>Internal Human Resources use only:</b>	
Effective Date:	
Occupational Group(s):	
Post Number:	