



## Job Description Print Report

Print Date: 2023-10-20 14:08:06

### Position Review

Position Number	241389	Position Type	CFE/JPO	Subject to Radiation	No	Subject to GD	No
Hyperion Position Number		Fund Type	EBR	Parent Position	009726		
Organization	SGIS-Safeguards Security Group	FTE	1	CCOG 1	1A05B		
Grade	P2	Duty Station	DS - IAEA VIENNA	CCOG 2			
Classified Grade	P2	Position Title	Associate Cyber Security Engineer	Proposed New Title	Associate Cyber Security Engineer		
Master Version	1	Master Status	Approved	Approval Date	06-OCT-23		
Position Version	1	Position Status	Approved	Approval Date	06-OCT-23		

### Job Description Review

#### Organization Settings

The Department of Safeguards carries out the IAEA's duties and responsibilities as the world's nuclear inspectorate, supporting global efforts to stop the spread of nuclear weapons. The primary role of the Department is to develop and implement IAEA safeguards to ensure that there is no diversion of declared nuclear material from peaceful activities and no indications of undeclared nuclear material or activities in a State as a whole.

The Department comprises nuclear safeguards inspectors, responsible for carrying out inspections and verifications of all-safeguards relevant information for nuclear facilities in over 180 States; and technical staff responsible for a wide range of activities including: developing concepts and approaches for implementing safeguards; developing and maintaining safeguards equipment; providing analytical and laboratory services for sample analysis; collecting, evaluating and analysing safeguards-relevant information; providing information and communication technology infrastructure and services; and providing programme coordination support.

The Office of Information and Communication Systems (SGIS) is responsible for the provision of secure Information and Communication Technology (ICT) services that enable the Department of Safeguards to deliver on its mandate. Major services provided by SGIS include provision of information technology project management services; development and maintenance of specialized ICT solutions; operation of resilient ICT infrastructure; provision of customer support services; and protection of safeguards information. In partnership with other organizational entities, SGIS is responsible for planning and implementing ICT strategies as well as promoting ICT standards.

#### Main Purpose

The Associate Cyber Security Engineer (SGIS) is a technical specialist working within the team to assist with IT security measures; an IT forensic enthusiast capable of assisting with forensic analysis; a team member assisting in managing-security related incidents and coordinating service delivery; a project associate, helping to define, plan and execute projects; and a decision support advisor, providing IT security and information security input to managers and colleagues.

<b>Role</b>		
<p>The Associate Cyber Security Engineer (SGIS) is part of the Safeguards Security Group, a team responsible for delivering the information security programmes and operations of the Department of Safeguards. The Associate Cyber Security Engineer (SGIS) interacts with information security experts and IT security practitioners across the Division, the Department of Safeguards, and the Agency. The Associate Cyber Security Engineer (SGIS) works closely with IT and application delivery teams on security topics including incident response and providing subject matter expertise. He/she works with external vendors and product suppliers on new information and technical specifications to evaluate and assess the suitability of their products and keep abreast of technical progress. He/she interacts, when appropriate, with all departmental staff and works closely with management on all aspects of IT security, and particularly on incident follow-up.</p>		
<b>Partnership</b>		
<p>The Associate Cyber Security Engineer (SGIS) works in close collaboration with the IT infrastructure team on matters related to infrastructure security and collaborates closely with business architects and development teams on matters related to application security. He/she works with external vendors and product suppliers on new information and technical specifications to evaluate and assess the suitability of their products and keep abreast of technical progress. The Associate Cyber Security Engineer (SGIS) cooperates in joint Agency-wide IT security projects with the Division of Information Technology (MTIT). He/she interacts, when appropriate, with all departmental staff and works closely with management on all aspects of IT security, and particularly on incident follow-up.</p>		
<b>Functions / Key results Expected</b>		
<ul style="list-style-type: none"> <li>• Contribute to the automation of security activities and the management of security infrastructure through scripting and other technical means to increase their effectiveness and reducing manual effort</li> <li>• Support conducting forensic acquisitions and examinations for a variety of platforms, operating systems and file systems, including Windows, Linux, iOS, and MacOS and analysing the results as well as extracting and preparing indicators of compromise</li> <li>• Contribute to the handling, analysis, and reporting of security incidents both individually and as part of a team</li> <li>• Assist with the implementation of technical defensive security operations and threat hunting using modern tools and techniques</li> <li>• Utilize highly technical means of assessing systems for security and measuring the effectiveness of security controls through testing them and reporting on the results in collaboration with members of the Safeguards Security Group and other security teams in the IAEA.</li> </ul>		
<b>Generic JD Remarks</b>		
<p></p>		
<b>Competencies</b>		
<b>Core Competencies</b>		
<b>Competency</b>	<b>Occupational Role</b>	<b>Definition</b>
Communication	Individual Contributor	Communicates orally and in writing in a clear, concise and impartial manner. Takes time to listen to and understand the perspectives of others and proposes solutions.
Achieving Results	Individual Contributor	Takes initiative in defining realistic outputs and clarifying roles, responsibilities and expected results in the context of the Department/Division's programme. Evaluates his/her results realistically, drawing conclusions from lessons learned.
Teamwork	Individual Contributor	Actively contributes to achieving team results. Supports team decisions.

Planning and Organizing	Individual Contributor	Plans and organizes his/her own work in support of achieving the team or Section?s priorities. Takes into account potential changes and proposes contingency plans.	
<b>Functional Competencies</b>			
<b>Competency</b>	<b>Occupational Role</b>	<b>Definition</b>	
Client orientation	Associate	Establishes effective relationships with clients to understand and meet or exceed their needs. Finds ways to ensure client satisfaction.	
Commitment to continuous process improvement	Associate	Identifies opportunities for process, system and structural improvement as well as improving current practices, increasing effectiveness and achieving efficiency gains. Actively supports the application of sound quality management standards and process improvement.	
Technical/scientific credibility	Associate	Acquires and applies new skills to remain up to date in his/her area of expertise. Reliably applies knowledge of basic technical/scientific methods and concepts.	
<b>Expertise</b>			
<b>Expertise</b>	<b>Description</b>		<b>Asset</b>
Information Technology IT Security	Exposure to IT security incident response, forensics, vulnerability assessment, software assessments, and other IT security areas.		N
Information Technology Information Security and Risk Management	Knowledge of how to manage information security risk through the application of technical, procedural, detective, and other types of controls, monitoring their progress, and assessing their maturity levels.		N
Information Technology Network Security	Understand internetworking, the associated protocols, the application layers of stacks, and the ability to analyze network traffic and activity data for issues and anomalies.		N
Information Technology Software Engineering	Ability to automate work using code and create tools to contribute to the team and its work.		N
Information Technology Systems Administration	Specify, implement, and manage security systems.		N
<b>Position Specific FC</b>			
<b>Position Specific FC</b>	<b>Occupational Role</b>	<b>Definition</b>	
<b>Position Specific Expertise</b>			
<b>Position Specific Expertise</b>	<b>Description</b>		<b>Asset</b>
<b>Languages</b>			
<b>Languages</b>	<b>Asset Languages</b>		
English	Arabic Chinese French Russian Spanish		

Qualification	
Qualification Title	Description
Bachelor's Degree	University degree in management, social sciences, science and technology, international relations or other relevant field.
Experience	
<ul style="list-style-type: none"> <li>• Demonstrable experience with scripting languages and/or software development.</li> <li>• Knowledge of reverse engineering software to determine its capabilities and functions.</li> <li>• Experience with attack frameworks such as Cobalt Strike or cyber security concepts related to attack and defence.</li> <li>• Good familiarity with Windows operating systems and security features including active directory, group policy and authentication methods as well as networked operating system functions and features.</li> <li>• Knowledge of data reporting and visualization, trend analysis, and using data to support decisions or measure effectiveness.</li> <li>• Experience with Linux and Unix-like operating systems and associated network services.</li> </ul>	