Internal / External Job Posting

Job Number: 005520
Closing Date: Open Until Filled
Resumes received in our office after the closing date will not be considered.

Position Title:	**Cyber Security Engineer/Senior Cyber Security Engineer**
Salary Band:	L/M
Range:	DOE (Salary will be determined based on experience, qualifications and attributes.)
Work Location & Schedule:	Anchorage This is a regular exempt level position that works an urban 40-hour week or compressed work week 9/80 schedule. Relocation benefits may apply.
Number of Positions:	One (1)
Recruiting Contact:	Tracey L. Mueller, Employee Relations Manager E-Mail: alyeska_jobs@alyeska-pipeline.com Apply on-line @ www.alyeska-pipe.com
Minimum Qualifications:	(Applicant must meet or exceed these minimum job requirements to apply for this position.) ▪ Bachelor's degree or equivalent preferably in a relevant field ▪ Three (3) years of experience involving cyber security technical field related to IT and/or Control systems security ▪ Advanced knowledge of Cyber Security and Information Technology systems ▪ Advanced written and verbal communication skills, able to influence across departments, agencies and stakeholders *Note: Additional related exempt level experience above the minimum may be substituted for the education requirement.*
Preferences:	• 10 years of experience in cyber/information security with at least one certification such as CISSP, DISA, CISM, CISA, GIAC, Information Assurance Management. • U.S. Government Clearance level of SECRET or higher or ability to obtain clearance • Demonstrated history of continuing information security education and awareness of current information security threats to enterprises • Expertise with Process Control Network (PCN) architecture, functions, network protocols& related security issues • Expertise with computer and network security incident response and investigative procedures • Familiarity with controls environments and security • Established relationships with federal law enforcement and/or intelligence communities • Familiarity with telecommunications protocols and related security issues • Member of InfraGard • Ability to communicate security related concepts to a broad range of technical and non-technical staff in an intelligent, articulate, and persuasive manner. • Information Assurance concepts • Information security standards and regulations, including but not limited to: • NIST SP800 series • NERC/CIP • HIPAA • SOX • Firewall and DMZ architecture • Secure remote access technologies • Network segmentation and zones of trust • Data classification and handling

	• Familiarity with Unix, Linux, Solaris, Oracle
Accountabilities and Specific Requirements:	**Under the direction of the Cyber Security & Infrastructure Manager, the Cyber Security Engineer is accountable for the following:** ▪ Recognition of the critical nature of TAPS ▪ Responsible for facilitation, planning, analysis and design functions related to cyber security infrastructure and cohesive, integrated information security risk & vulnerability management program to include IT & Control systems infrastructure and architecture ▪ Regularly interfaces with federal law enforcement agencies to enhance coordination, information sharing, & law enforcement ▪ Facilitate collaboration across IT, Controls, and operations teams to ensure integrity, availability, reliability and performance of cyber protection measures ▪ Reviews, recommends, and updates existing policies, procedures & standards to maintain alignment with corporate business goals, technical requirements, information security industry standards and best practices & emerging threat research & developments ▪ Monitors & audits to ensure compliance with cyber security regulations and guidelines ▪ Implements process, policy and a cohesive, integrated information security risk and vulnerability management program for the organization, including IT and controls environments ▪ Components of the cyber security risk and vulnerability management program include but are not limited to: Maintain and develop log monitoring, analysis, and alerting for anomalous events that could indicate evidence of a compromise or policy violation ▪ Implementing business oriented information security model in the enterprise and process control environments while giving substantial consideration to critical infrastructure issues and requirements ▪ The role and model will reflect an overall information assurance approach and incorporate authenticity, utility, and possession ▪ Provides cyber security assurance and point of integration between IT systems and Controls environment ▪ Ensure the confidentiality, integrity, and availability of data residing on or transmitted to/from/through
Knowledge & Skills:	▪ Analysis & Problem Solving ▪ Regulations ▪ Interpersonal Communication ▪ Law / Investigations ▪ Project Management ▪ Business Management ▪ Information Technology/Management ▪ External Relations/Internal Relations ▪ Operations Control ▪ Security
Contributor Level	Individual Contributor – Professional

Internal / External Job Posting

Job Number: 005520
Closing Date: Open Until Filled
Resumes received in our office after the closing date will not be considered.

Pre-Employment Drug Screen Testing	Alyeska Pipeline Service Company (APSC) requires pre-employment drug testing utilizing hair test collections for all positions. The preferred collection site is from the head (approximately 1/2 inch of hair length necessary). Head hair testing provides an approximate 90 day window of detection that checks for drug use. In addition, for Department of Transportation covered positions, APSC will also utilize urinalysis testing. Any positive drug test makes you ineligible for APSC employment.
Employment Verification using E-Verify	Federal Law requires all employers to verify identity and employment eligibility of all persons hired to work in the United States. Alyeska Pipeline Service Company participates in E-Verify. E-Verify is an Internet-based system that compares information from an employee's Form I-9, Employment Eligibility Verification, to data from U.S Department of Homeland Security and Social Security Administration records to confirm employment eligibility. http://www.dhs.gov/e-verify
TWIC	This position may include travel to Alyeska's Valdez Marine Terminal (VMT), a regulated facility, and the employee hired to work on the VMT or to provide emergency support or other approved work for the VMT will be required to have a Transportation Worker Identification Credential (TWIC). For more information about this Federal credential access the Web site listed below. The successful candidate will be required to obtaining a TWIC prior to their hire date. http://www.tsa.gov

ALYESKA PIPELINE SERVICE COMPANY IS AN EQUAL OPPORTUNITY EMPLOYER THAT VALUES WORKPLACE DIVERSITY.

Alyeska Pipeline is a drug-free and alcohol-free workplace.
Apply on-line at www.alyeska-pipe.com