Internal/External Job Posting

Job Number: 005580
Closing Date: December 5, 2018
Resumes received in our office after the closing date will not be considered.

Position Title:	Cyber Security Engineering Lead
Salary Band:	M
Range:	DOE (Salary will be determined based on experience, qualifications and attributes.)
Work Location & Schedule:	Anchorage This is a regular exempt Anchorage-based position on an urban schedule of a 40-hour week or 9/80-work schedule. Relocation benefits may apply.
Number of Positions:	One (1)
Recruiting Contact:	Tracey L. Mueller, Employee Relations Manager Alyeska Pipeline Service Company E-Mail: alyeska_jobs@alyeska-pipeline.com Apply on-line at www.alyeska-pipe.com
Minimum Qualifications:	**Applicants must meet or exceed these minimum job requirements to apply for this position.** ▪ Bachelor's degree (or equivalent) in IT, Business Administration, Engineering, or related discipline ▪ Four (4) 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
Accountabilities and Specific Requirements:	**Under the direction of the Cyber Security & Infrastructure Manager, the Cyber Security Engineering Lead is accountable for the following:** ▪ System-wide cyber security for TAPS. ▪ Accountable for the development, implementation, and enforcement of cyber security strategy and cyber security policies for TAPS. ▪ Ensures procedures are developed and in place to protect APSC's intellectual property, assets, and

	systems. ▪ Serves as cyber security liaison with outside government agencies (FBI, TSA, DHS, etc.) and interacts with law enforcement agencies. ▪ Oversees IT and cyber risk assessments, audits, and cyber security investigations for all of TAPS. Manages prevention and reduction of Alyeska's vulnerabilities to cyber security threats, evaluation of cyber security risk, and understanding threat and implementing actions to mitigate risks. ▪ Elevates risks as needed within the organization. ▪ Requires strict attention to the cyber threats/actors and countermeasures to protect the infrastructure supporting business and control systems from cyber threats. ▪ Routinely engages cyber security counterparts from intelligence communities, Homeland Security, and other agencies and cyber security communities and organizations. ▪ Works across the organization to collaborate with and influence peers and others outside the chain of authority to recognize and enforce critical policies and procedures to protect TAPS assets. ▪ Works closely with Legal, HR, Operations, and others for investigations and to ensure confidentiality and security of systems to protect against cyber threats and ensures protection of HIPAA-related data and PII. ▪ Leads and directs the work of others, including contract personnel. ▪ Team performs periodic information security and privacy risk assessments. ▪ Oversees the management and investigation of cyber security incidents. This position is responsible for determining and implementing cyber security standards and procedures. Responsible for leading the strategic initiatives related to cyber security and infrastructure, as well as driving projects for infrastructure and cyber security. This position provides briefs and reports on current and ongoing cyber security threats and vulnerabilities that could impact TAPS.
Knowledge, Skills and Abilities:	▪ 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
TAPS Safety Culture	**Act With Discipline** Be prepared to work and arrive to work rested. Complete all pre-job planning steps. Complete all training and qualifications. Follow all required processes and procedures and use the right tools for the job. Complete all post-work activities. **Take a System View** Assess how a task can impact others, seek input, and make all necessary notifications. **Make Sound Decisions** Involve the right people at the right time. Identify if conditions change and act accordingly. **Learn, Improve, Innovate** No task on TAPS is routine; be alert to emerging risks. Communicate hazards and share lessons learned from past experiences. **Speak Up, Step Up** Alyeska fully supports the authority of every TAPS worker to speak up, take action, and stop work, regardless of role or responsibility. Participate in developing and implementing solutions.
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 drug test makes you ineligible for APSC employment.

	▪ It is important to note that APSC does not seek or accept any genetic information as part of the hair testing procedure or any other process that could directly or inadvertently provide genetic information (family medical history).
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	▪ The Alyeska Valdez Marine Terminal (VMT) is 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 for this job will be notified if a TWIC will be required and will then be responsible for enrolling and 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