	Control Systems Engineer I	Control Systems Engineer II	Control Systems Engineer III	Control Systems Engineer IV
Essential Functions	A fully skilled employee in this role is able to perform all of the essential functions listed below, and will work primarily on low risk and low complexity work assignments. Must be available to respond to call-outs 24x7x365	A fully skilled employee in this role is able to perform all of the essential functions listed below, and will work primarily on low-moderate risk and low-moderately complex work assignments. Must be available to respond to call-outs 24x7x365	A fully skilled employee in this role is able to perform all of the essential functions listed below, and will work primarily on moderate- high risk and moderately-highly complex work assignments. Must be available to respond to call-outs 24x7x365	A fully skilled employee in this role is able to perform all of the essential functions listed below, and will primarily work on the highest risk, broadest scope and most complex work assignments. Must be available to respond to call-outs 24x7x365
SCADA (EMS/GMS)	Learn about and perform work under close supervision on systems with a low level of risk to operational compliance, revenue stream, equipment and human safety, including: Implement, document and maintain the following for systems including Distribution, Generation, Hatcheries, Water/Wastewater and Compliance: Read-only Human Machine Interfaces Communication topology using Ethernet Work practices Provide Control Room Operators, Energy Planning & Trading, Outage Coordinators, Engineers and Project teams with the following: Procedures that enhance system reliability and departmental/ organizational efficiencies Engineering analysis and technical support to ensure continuing reliable operations of the electric power grid and District services Provide integration and interoperability for small-scale systems Maintain servers and workstations and associated hardware throughout its lifespan Configure 1 or more operating systems Research new display and tool technologies Serve as a contributor to the development strategy for the tools and applications needed by District Operations and Planning	<ul> <li>Perform work under general supervision on networked systems with a low-moderate level of risk to operational compliance, revenue stream, equipment and human safety, including:         <ul> <li>Implement, document and maintain the following for systems including Transmission, Distribution, Generation, Hatcheries, Water/Wastewater, Security and Compliance:                 <ul> <li>Interactive Human Machine Interfaces, automation interfaces and database structures for 1 or more systems</li></ul></li></ul></li></ul>	<ul> <li>Perform work on advanced, networked systems with a moderate-high level of risk to operational compliance, revenue stream, equipment and human safety, including:</li> <li>Design, develop, implement, document and maintain the following for systems including Transmission, Distribution, Generation, Hydro Optimization, Hatcheries, Water/Wastewater, Mid-Columbia Hourly Coordination, Security and Compliance:         <ul> <li>Interactive Human Machine Interfaces with embedded custom code, automation interfaces, and database structures that control 2 or more systems</li> <li>Single-order control system models</li> <li>Interconnected system architecture for 3 or more systems</li> <li>Communication topology using serial, fiber and Ethernet</li> <li>Code for control automation, calculations, generation and energy management, contract compliance (water rights, reliability, environment requirements), energy accounting, database management, fish ladder control</li> <li>Change Management</li> <li>Work Practices</li> <li>Historical data storage and maintenance for critical utility information</li> </ul> </li> </ul>	<ul> <li>Perform work on highly complex, interconnected, interdependent systems with the highest levels of risk to operational compliance, revenue stream, equipment and human safety, including:</li> <li>Design, develop, implement, document and maintain the following for systems including Transmission, Distribution, Generation, Hydro Optimization, Hatcheries, Water/Wastewater, Mid- Columbia Hourly Coordination, Security and Compliance:         <ul> <li>Interactive Human Machine Interfaces with embedded custom code using custom data structures, automation interfaces, and database structures that control 3 or more systems</li> <li>Multi-order control system models</li> <li>Interconnected system architecture for 4 or more systems</li> <li>Communication topology using serial, microwave, fiber and Ethernet</li> <li>Code for Mid-C coordination, slice and encroachment contracts, control and process automation, advanced calculations, generation, water and energy management, contract compliance (water rights, reliability, environment requirements), energy accounting, custom communication protocols, custom</li> </ul> </li> </ul>

	cheran POD Control System Enginee		
Provide documentation for the	system reliability and	<ul> <li>Tools and procedures to monitor interfaces, database</li> </ul>	al fiel
development of training and training	departmental efficiencies	and control 3 or more systems management, river control	rol, fish
material	<ul> <li>Engineering analysis and technical support to answer</li> </ul>	Provide Control Room Operators, Energy     ladder control     Change management	
Maintain asset information for assets	technical support to ensure	Planning & Trading, Outage Coordinators, o Change management	
critical to the reliability of the grid using	continuing reliable operations of	Engineers and Project teams with the o Work Practices	
Maximo, Primavera and other tools	the electric power grid and	following: o Historical data storage,	
Attend industry meetings, discussions and	District services.	<ul> <li>Analysis and visualization of data maintenance, and optim</li> </ul>	
forums pertinent to CSE areas of	<ul> <li>Documentation and guidance</li> </ul>	needed to maintain the reliability for critical utility informat	
responsibility	needed by Project teams in order	of District control system o Tools and procedures to	
	to deploy new tools	operations and control 4 or more sy	
	<ul> <li>Maintain servers and workstations and</li> </ul>	<ul> <li>Development and prototyping of</li> <li>Provide Control Room Operators</li> </ul>	
	associated hardware throughout its	operational awareness and Planning & Trading, Outage Coor	
	lifespan	analytical tools Engineers and Project teams with	n the
	Configure and manage 2 or more	<ul> <li>Development tools, processes</li> <li>following:</li> </ul>	
	operating systems	and procedures that enhance o Analysis and visualization	
	Serve as the Subject Matter Expert for 1	system reliability and needed to maintain the r	,
	or more system performance standards	departmental/organizational of District control system	1
	and contributes to the development	efficiencies operations	. ,
	strategy for the tools and applications	<ul> <li>Engineering analysis and</li> <li>Development and protot</li> </ul>	
	needed by District Operations and	technical support to ensure operational awareness a	and
	Planning	continuing reliable operations of analytical tools	
	<ul> <li>Act as mentor and advisor to less</li> </ul>	the electric power grid and o Development of operation	
	experienced engineers	District services. impact assessment stud	les and
	Maintain asset information for assets	Occumentation and guidance     mitigation plans	
	critical to the reliability of the grid using	needed by Project teams in order o Development tools, proc	
	Maximo, Primavera and other tools	to deploy new tools and procedures that enh	ance
	Maintain knowledge of emerging trends	Provide integration and interoperability for     system reliability and     departmental/arganization	anal
	and industry best practices	3 or more systems departmental/organization	Jnai
	<ul> <li>Represent the District in industry</li> </ul>	Analyze operational data to develop     efficiencies     Engineering analyzis on	d
	meetings, discussions and forums	solutions for current and future system o Engineering analysis an technical support to ensi	
	pertinent to CSE areas of responsibility		
			nu
			lance
			ability for
		operating systems	ability for
		• Develop vendor applications through	
		changes in software, processes and training • Analyze operational data to devel solutions for current and future sy	
			516111
			and
		Investigation, evaluation, and bench-     Purchase, implement, document     maintain converse workatations n	
		marking of new display and tool maintain servers, workstations, no	
		technologies equipment, appliances and associated and application of the second	Jaleo
		hardware throughout its lifespan	

			<ul> <li>Serve as the Subject Matter Expert for 2 or more system performance standards and contributes to the development strategy for the tools and applications needed by District Operations and Planning</li> <li>Provide documentation and guidance for the development of training and training material</li> <li>Act as mentor and advisor to less experienced engineers</li> <li>Maintain asset information for assets critical to the reliability of the grid using Maximo, Primavera and other tools</li> <li>Maintain knowledge of emerging trends and industry best practices</li> <li>Represent the District in industry meetings, discussions and forums pertinent to CSE areas of responsibility</li> </ul>	<ul> <li>Configure and manage 4 or more operating systems</li> <li>Develop vendor applications to their fullest extent through changes in software, processes and training</li> <li>Develop test scripts and test the functionality of tools developed</li> <li>Investigation, evaluation, bench-marking and implementation of new display and tool technologies</li> <li>Serve as the Subject Matter Expert for 3 or more system performance standards and contributes to the development strategy for the tools and applications needed by District Operations and Planning</li> <li>Provide documentation and guidance for the development of training and training material</li> <li>Act as mentor and advisor to less experienced engineers</li> <li>Maintain asset information for assets critical to the reliability of the grid using Maximo, Primavera and other tools</li> <li>Maintain knowledge of emerging trends and industry best practices</li> <li>Represent the District in industry meetings, discussions and forums pertinent to CSE areas of responsibility</li> </ul>
Cyber Security	<ul> <li>Learn about and perform work under close supervision on systems with a low level of risk to operations, regulatory compliance and company reputation, including:</li> <li>Provide support to internal teams to define and develop secure architecture and solutions for projects</li> <li>Prepare and maintain technical user guides, System Operating Procedures, security architecture documentation and diagrams</li> <li>Participate in project meetings</li> <li>Monitor alerts and logs</li> <li>Maintain security tools and technologies, including:</li> </ul>	<ul> <li>Perform work under general supervision on networked systems with a low-moderate level of risk to operations, regulatory compliance and company reputation, including:</li> <li>Provide support to internal teams to define and develop secure architecture and solutions for projects, conduct discovery sessions to gain the necessary background and review findings to ensure sustained compliance</li> <li>Assist with the assessment and documentation of the design of secure solutions</li> <li>Assist with the implementation of technical security solution policies in alignment with</li> </ul>	<ul> <li>Perform work on advanced, networked systems with a moderate-high level of risk to operations, regulatory compliance and company reputation, including:</li> <li>Define and develop secure architecture and solutions for projects, conduct discovery sessions to gain the necessary background and review findings to ensure sustained compliance, remediation of control gaps and escalation of possible critical issues</li> <li>Guide, assess and document design of secure solutions</li> <li>Implementation of technical security solution policies in alignment with</li> </ul>	<ul> <li>Perform work on highly complex, interconnected, interdependent systems with the highest levels of risk to operations, regulatory compliance and company reputation, including:</li> <li>Define, develop, and implement secure architecture and solutions for projects, conduct discovery sessions to gain the necessary background and review findings to ensure sustained compliance, remediation of control gaps and escalation of possible critical issues</li> <li>Guide, assess, implement and document design of secure solutions</li> <li>Architect and direct implementation of</li> </ul>

<ul> <li>Logging</li> <li>Anti-YunaMakarar Detections risk</li> <li>Prepare and maintain technical user guides. System Operating Procedures, and protection management services</li> <li>Participate in cycler security incident response plan tests</li> <li>Participate in cycler security incident response plan tests</li> <li>Participate in cycler and maintain security cycle emaining remaintain of a pas and differences as project meetings and provide emaining remaintain of a pas and differences as project meetings and provide emaining remaintain of a pas and differences as project meetings and provide emaining remaintain of a pas and differences as project meetings and provide emaining remaintain of a pas and differences as project meetings and provide emaining remaintain of a pas and differences as project meetings and provide emaining remaintain of a pas and differences as project meetings and provide emaining remaintain of a pas and differences as project meetings and provide emaining remaintain of a pas and differences as project meetings and provide emaining remaintain security emaintements</li> <li>Devide and maintain estimation of lang security provides and security maintements</li> <li>Anti-YunaMakares Detection on Anti-YunaMakares Detection on Sacinty Plant security provides and entrasion Detection approvement of control trasport parts</li> <li>Devide and maintain and Eventhic (DS) and non Thermeticas on Sacinty Plantmation and Event</li></ul>		chelan FOD control System Enginee		
<ul> <li>Configuration management septors sourchy calculated by the sector response plan tests</li> <li>Participate in project meetings and purch againers</li> <li>Participate in project meetings</li> <li>Parti</li></ul>				
<ul> <li>Support security includer:</li> <li>Participate in project meetings and provide recommendations and strategies for ecommendations and strategies and provide recommendations and strategies for ecommendations and strategies for ecommendation strategies and strategies for ecommendations and strate</li></ul>				
<ul> <li>beridget in cyber security indident response plan tests</li> <li>diagrams</li> <li>diagrams</li> <li>diagrams</li> <li>diagrams</li> <li>diagrams</li> <li>excitigate in project meetings and provide resonance mediation of gaps and dialicative as projects</li> <li>excitigate in project meetings and provide resonance mediation and strategies for excommediations and strategies for excommediations and strategies for excommediations and strategies for excommediation strategies for excommediation strategies for excommediations and strat</li></ul>				
<ul> <li>Participate in cycler executly incident response plan tests</li> <li>Participate in project meetings and provide recommendations and strategies for ensuing remediation of gaps and deficiencies as projects develop.</li> <li>Monitor allers and togs</li> <li>Monitor allers and togs</li> <li>Monitor allers and togs</li> <li>Monitor allers and togs</li> <li>Confluctation management Baseline montoring</li> <li>Asset management Baseline montoring</li> <li>Asset with mit-party preduction sets</li> <li>Conduct and participate in cycle.</li> <li>Software and security updates</li> <li>Conduct and participate in cycle.</li> <li>Multifactor authentication and security updates</li> <li>Conduct and participate in cycle.</li> <li>Multifactor authentication and security updates</li> <li>Conduct and participate in cycle.</li> <li>Multifactor authentication and security updates</li> <li>Conduct and participate in cycle.</li> <li>Multifactor authentication and security updates</li> <li>Conduct and participate in cycle.</li> <li>Multifactor authentication and security updates</li> <li>Conduct and participate in cycle.</li> <li>Asset management Baseline monitoring</li> <li>Asset management Baseline monitoring</li> <li>Conduct and participate in cycle.</li> <li>Software and security updates</li> <li>Conduct and participate in cycle.</li> <li>Asset with hird-party prematedion tass</li> <li>Software and security updates</li> <li>Develop, inplement and main security equitation and security updates</li> <li>Develop and ingeneration and participate in cycle.</li> <li>Network Access Control (NAC)</li> <li>Least access provides generation of ages samelis.</li> <li>Develop and participate in cycle.</li> <li>Network Access Control (NAC)</li> <li>Least access provides generation of ages and tesocolis provide generation of ages and tesocolis provide samelism.</li> <li>Develop and parelisten</li></ul>		security architecture documentation and	security architecture documentation and	
<ul> <li>response plan tests</li> <li>recommendations and stratégies for ensuing remediation of gaps and deficiencies as projects develop</li> <li>Mointor alets and logs</li> <li>Mointor alets and logs</li> <li>Mointor alets and logs</li> <li>Mointor alets and logs</li> <li>Continuously audit security colors de technologies, including.</li> <li>Continuously audit security colors de technologies, including.</li> <li>Software and security including.</li> <li>Mointor alets and logs</li> <li>Continuously audit security colors de technologies, including.</li> <li>Software and security including.</li> <li>Mointor alets and logs</li> <li>Continuously audit security colors de technologies, including.</li> <li>Mointari astabilished security requirements</li> <li>Mointari astabilished security requirements</li> <li>Periodit security informencialis as excity- incident response plan tests</li> <li>Software and security requirements</li> <li>Manistain setabilished security- requirements</li> <li>Periodit security informencialisa security- recontinentialisa security- recontinentialisa security- recontinentialisa security- requirements</li> <li>Software and security updates</li>     &lt;</ul>				
<ul> <li>ensuring remediation of gaps and deficiencies as projects develop</li> <li>Monitor alerts and logs</li> <li>Maintain security tools and technologies, including:</li> <li> <ul> <li>Logging net monitoring</li> <li>Anti-Virus/Maiwre Detection</li> <li>Asset management/Baseline monitoring</li> <li>Maintain in established security-requirements</li> <li>Condituation services</li> <li>Condituates a phase services</li> <li>Condituates a phase services</li> <li>Condituates a phase services</li> <li>Condituates a phase services</li> <li>Condituates phase services</li> <li>Conducts and participate in revealable security-focused tools and services</li> <li>Software and security produets and tests</li> <li>Software and security produets and tests</li> <li>Conduct and participate in revealable security-focused tools and services</li> <li>Conduct and participate in revealable security-focused tools and services</li> <li>Conduct and participate in revealable security-focused tools and services</li> <li>Conduct and participate in revealable security-focused tools and services</li> <li>Conduct and participate in revealable security-focused tools and services</li> <li>Conduct and participate in revealable security-focused tools and services</li> <li>Conduct and participate in revealable security-focused tools and services</li> <li>System stricting and monitoring</li> <li>Multi-factor suffering and monitoring</li> <li>System stricting and restoration</li> <li>Multi-factor authenication</li> <li>System stricting and monitoring</li> <li>System stricting and controls to mighter six and security requirements and salinguards and services</li> <li>Conduct and participate in revealable decords</li> <li>System stricting and monitoring</li> <li>Multi-factor authenication</li> <li>Sys</li></ul></li></ul>	Participate in cyber security incident			
<ul> <li>deficiencies as projects develop</li> <li>Monitor alters and logs</li> <li>Maintain security tools and technologies, including:</li> <li>Logging and monitoring</li> <li>Data relation and or Anti-Virus/Maware Detection</li> <li>Continuously audi security controls</li> <li>Develop, implement and maintain security control of age. and develop mitigation ip inso</li> <li>Develop, implement and maintain security control</li> <li>Maintain estabilished security requirements</li> <li>Provide technical revew of standardized District security products and technologies</li> <li>Assist with hird part parentials</li> <li>Evelup and there in degrase in projects develop</li> <li>Multi-factor security products and technologies</li> <li>Develop, implement and maintain security requirements</li> <li>Provide technical revew of standardized District security products and technologies</li> <li>System hardening</li> <li>Network Access Control (NAC)</li> <li>Valuer and maintain security requirements</li> <li>System hardening</li> <li>Develop and the security requirements</li> <li>System hardening</li> <li>Develop and the security products and technologies</li> <li>Network Access Control (NAC)</li> <li>Valuer and maintain security requirements</li> <li>System hardening</li> <li>Network Access Control (NAC)</li> <li>Valuer and maintain security requirements</li> <li>System hardening</li> <li>Network Access Control (NAC)</li> <li>Valuer and maintain security requirements</li> <li>System hardening</li> <li>Network Access Control (NAC)</li> <li>Valuer and maintain security requirement security focused to and services</li> <li>System hardening</li> <li>Network Access Control (NAC)</li> <li>Develop and implement defines in degra and annitoring</li> <li>Network Access Control (NAC)</li> <li>Valuer and maintain security requirement security focused to and and revices</li> <li>System hardening</li> <li>Network Access Control (NAC)</li> <li>Develop and implement defines in degra control in the security focused to security focused to and</li></ul>	response plan tests			
<ul> <li>Monitor alerts and logs</li> <li>Monitor alerts and logs</li> <li>Continuously audit security controls</li> <li>Setware and security updates</li> <li>Continuously audit security controls</li> <li>Setware and security protection and restoration</li> <li>Setware and security updates</li> <li>Continuously audit security controls</li> <li>Setware and security protection and restoration</li> <li>Setware and security protection and restoration</li> <li>Security findense in depth controls to miligate risk</li> <li>Provide technical review of standardized District security framework</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Evaluate and recommend new and emerging security products and technologies</li> <li>Assist with finder party penetration tests</li> <li>Evaluate and recommend new and emerging security products and technologies protection figuration management dense in depth controls and technologies including:</li> <li>Assist with finder party penetration tests</li> <li>Evaluate and recommend new and emerging security products and technologies in the dening</li> <li>Nassist with finder party penetration tests</li> <li>Evaluate and recommend action sports and security products and technologies in the dening</li> <li>Numerability assessments</li> <li>Implement store and and and and and and and and and and</li></ul>				
<ul> <li>Maintain security tools and technologies, including:         <ul> <li>Continuously audit security controls</li> <li>Anti-Virus/Malware Detection</li> <li>Anti-Virus/Malware Detection colos and technologies, including:</li> <li>Continuously audit security controls</li> <li>Develop, implement and maintain security tools and technologies, including:</li> <li>Schware and security update risk</li> <li>Develop, implement admains and Event Management (SEM)</li> <li>Multi-factor authentication</li> <li>Introlement defense in depth controls to mitigate risk</li> <li>Dodat security controls</li> <li>Introlement defense in depth controls to mitigate risk</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Evaluate and recommend new and technologies in threading</li> <li>Newlop and implement adfense in depth controls to mitigate risk</li> <li>Develop, mitigments</li> <li>Newlop and implement defense in depth controls to mitigate risk</li> <li>Develop, mitigments</li> <li>Ansit virus/Malware Detection</li> <li>Software and security products and technologies</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Develop, mitigment, support and evaluate security controls to mitigate risk</li> <li>Develop, mitigment, support and evaluate security controls to mitigate risk</li> <li>Develop, mitigments</li> <li>Develop, mitigment and maritain sec</li></ul></li></ul>				
<ul> <li>Parform Security Risk Assessments, identify security subsets and risks, best management Baseline monitoring</li> <li>Okati-Virush Malware Detection</li> <li>Software and security updates</li> <li>Configuration management Baseline monitoring</li> <li>Maintain established security reparents and maintain security including:</li> <li>Maintain established security information and Event Management (SEM)</li> <li>Implement support and evaluate security framework</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Evaluate and recommend new and technologies</li> <li>Evaluate and recommend new and technologies</li> <li>Evaluate and recommend new and technologies</li> <li>Develop, mighement and maintain security incident response plan tests</li> <li>Develop inglement and maintain security incident response plan tests</li> <li>Develop inglement and maintain security incident response plan tests</li> <li>Develop inglement and maintain security incident response plan tests</li> <li>Develop inglement and maintain security incident response plan tests</li> <li>Develop inglement and maintain security incident response plan tests</li> <li>Develop inglement and maintain security incident response plan tests</li> <li>Develop inglement dering tervice of standardized District security framework</li> <li>Develop, inglement, support and evaluate security incident response plan tests</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Develop, inglement, support and evaluate security incident response plan tests</li> <li>Develop, inglement, support and evaluate security incident response plan tests</li> <li>Develop, inglement, support and evaluate</li></ul>				
<ul> <li>balar restoration</li> <li>Datar restoration</li> <li>Anti-Vitus/Mayare Detection</li> <li>Software and security updates</li> <li>Configuration management</li> <li>Asset management asbalshed security requirements</li> <li>Maintain established security requirements</li> <li>Maintain established security requirements</li> <li>Maintain established security requirements</li> <li>Indiverse in defense in depth controls to mitigate risk</li> <li>Provide technical review of standardized Distirct security framework</li> <li>Evaluate and participate in cyber security incident response plan issues</li> <li>System ragement (Selens)</li> <li>Assist with Intrd-party penetration tests</li> <li>Provide technical review of standardized Distirct security framework</li> <li>Evaluate and percommend new and emerging security fracuses control (NAC)</li> <li>Evaluate and recommend new and emerging security fracuses to so and services</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>System hardening emerging security requirements and recommend adequards</li> <li>Develop, implement, support and exists</li> <li>Provide technical review of standardized Distirt security requirements</li> <li>Develop in plement, support and exists</li> <li>Co</li></ul>				
<ul> <li>Data restoration</li> <li>Anti-Virus/Malware Detection</li> <li>Software and security updates</li> <li>Condiguration management/Baseline monitoring</li> <li>Maintain estabilished security requirements</li> <li>Implement and maintain security requirements</li> <li>Provide technologies, including:</li> <li>Software and security products and technologies</li> <li>Assist with hird-party penetration technologies</li> <li>Assist with hird-party penetration technologies</li> <li>Assist with hird-party penetration technologies</li> <li>Evaluate and recommend new and emerging security products and technologies</li> <li>Evaluate and recommend new and emerging security products and technologies</li> <li>Develop, miligation plans</li> <li>Develop, miligation plans</li> <li>Develop miligation plans</li>     &lt;</ul>				
<ul> <li>Anti-Virus/Malware Detection</li> <li>Software and security updates</li> <li>Configuration management Baseline monitoring</li> <li>Maintain established security requirements</li> <li>Implement defense in depth controls to migate risk.</li> <li>Provide technical review of standardized District security products and technologies.</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Assist with tink-pary penetration tests</li> <li>Feury and technical review of and devices on controls to migate risk.</li> <li>Provide technical review of standardized District security fragment/ focused tools and services</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Assist with tink-pary penetration tests</li> <li>Feury and technical review of and additional emerging security products and technologies.</li> <li>Implement and maintain security requirements</li> <li>Assist with tink-pary penetration tests</li> <li>Provide technical review of and additional emerging security products and technologies</li> <li>Conduct and participate in cyber security requirements</li> <li>Maintain response plan tests</li> <li>Network Access Control (NAC)</li> <li>Least access privilege implementation</li> <li>System Nardioning</li> <li>System Nardioning</li> <li>System Nardioning</li> <li>System Nardioning</li> <li>System Nardioning</li> <li>System Nardioning</li> <li>Network Access Control (NAC)</li> <li>Least access privilege implementation</li> <li>Develop, and implement defense in depth controls to mitigate risk.</li> <li>Provide technical review of standardized District security framework</li> <li>Develop, and inplement defense in depth controls to mitigate risk.</li> <li>Provide technical review of and applicate in cyber security incident response plan tests</li> <li>Conduct and participate in cyber security requirements</li></ul>				
<ul> <li>Software and security updates</li> <li>Configuration management/Baseline monitoring</li> <li>Maintain established security requirements</li> <li>Maintain established security requirement defense in depth controls to mitigate risk</li> <li>Implement defense in depth controls to mitigate risk</li> <li>Provide technical review of standardized District security framework</li> <li>Conditurat and participate in cyber security reguirements</li> <li>Software and security updates</li> <li>Software and security updates</li> <li>Software and security updates</li> <li>Software and security updates</li> <li>Network Access privilege implementation</li> <li>System sifting and maintain security requirements</li> <li>Evaluate and recommend new and emerging security products and technologies</li> <li>Evaluate and recommend new and emerging security products and technologies</li> <li>Provide technical review of standardized District security framework</li> <li>Develop and implement defense in optor security incident response plan tests</li> <li>Develop and implement defense in optor security requirements</li> <li>Develop and implement defense in optor security incident response plan tests</li> <li>Develop and implement defense in optor security requirements</li> <li>Develop and implement defense in optor security incident response plan tests</li> <li>Develop and implement defense in optor security incident response plan tests</li> <li>Develop and implement defense in optor security requirements and salegurads</li> <li>Provide technical review of standardized District security framework</li> <li>Develop and implement defense in optor security incident response plan tests</li> <li>Develop and implement defense in optor security incident response plan tests</li> <li>Develop and implement defense in optor security incident response plan tests</li> <li>Develop and implement defense in optor security incident response plan tests</li> <li>Develop and implement defense in optor security incident response plan tests</li> <li>Prov</li></ul>				
<ul> <li>Configuration management <ul> <li>Asset management/Baseline monitoring</li> <li>Maintain established security requirements</li> <li>Implement defense in depth controls to mitigate risk Provide technical review of standardized District security information and Event Management (SIEM)             <ul> <li>Multi-factor authentication</li> <li>Multi-factor authentication</li> <li>Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)</li> <li>Data releation and restruction conduct and participate in cyber security incident response plan tests</li> <li>Conduct and participate in cyber security incident response plan tests</li>             Design, develop, implement and maintain System is conduct and participate in cyber security incident response plan tests</ul></li>             Develop, and induce security requirements</ul></li>             Develop, and induce security requirements             Develop, implement defense in depth configuration management System in freeining system indening implement and maintains security requirements             Develop, and implement defense in depth configuration management develop and implement defense in depth configuration management develop, implement, support and evaluate security inderwets             develop and implement defense in depth configuration managements             develop, implement, support and evaluate security-focused tools and services configuration managements             develop and implement defense in depth configuration m</ul>				
<ul> <li>o. Asset management/Baseline monitoring</li> <li>Maintain established security requirements</li> <li>Implement defense in depth controls to miligate risk</li> <li>Provide Iechnical review of standardized District security framework</li> <li>Implement, support and evaluate security- rocused tools and services</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Evaluate and recommend new and emerging security products and technologies</li> <li>Provide technical review of standardized bistrict security rocused tools and services</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Evaluate and recommend new and evaluate security products and technologies</li> <li>Network Access fortori (NAC)</li> <li>Legaing end maintain security requirements</li> <li>Develop and implement adforase in depth controls to milgate risk.</li> <li>Develop and implement adforase in depticentical review of standardized District security framework</li> <li>Develop and implement adforase in depticentical review of standardized District security framework</li> <li>Develop and implement adforase in depticentical review of standardized District security framework</li> <li>Develop and implement adforase in depticentical review of and security requirements</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Develop and implement adforase in depticentical review of and security requirements and recommend additional security framework</li> <li>Develop and implement adforase in depticentics to milgate risk</li> <li>Provide technical review of and security framework</li> <li>Develop and implement security focused tools and services</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Cordicat and participate in cyber security incident response plan tests</li> <li>Develop and implement atono set and</li></ul>				
<ul> <li>Multi-factor authemication</li> <li>Multi-factor authemication</li> <li>Implement defense in depth controls to mitigate risk</li> <li>Provide technical review of standardized District security framework</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Assist with third-party penetration tests</li> <li>Evaluate and recommend new and emerging security products and technologies</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Develop, implement, support and evaluate security framework</li> <li>Develop, implement, support and evaluate security requirements</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Develop, implement, support and evaluate security requirements</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Conduct and participate in cyber security requirements</li> <li>Develop, implement and maintain security requirements and recommend additional security requirements and security requirements and security requirements and security framework</li> <li>Develop and implement defense in depth controls to mitigate risk</li> <li>Develop and implement defense in depth controls to mitigate risk</li> <li>Develop and implement defense in depth controls to mitigate risk</li> <li>Develop and implement defense in depth controls to mitigate risk</li> <li>Develop and implement defense in depth controls to mitigate risk</li> <li>Develop and implement defense in depth controls to mitigate risk</li> <li>Develop and implement defense endepting indemt response plan tests</li> <li>Conduct and participate in cyber security in</li></ul>				
<ul> <li>Maintain seablished security requirements</li> <li>Implement, support and evaluate bistrict security framework</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Evaluate and recommend new and emerging security products and technologies</li> <li>Forvide technical review of standardized District security products and technologies</li> <li>Intrusion Detection Systems (IDS) and Intrusion Detection System Sitems (IDS) and Intrusion and restoration o Stata retention and restoration o Software and security protection o Software and security incident response plan tests</li> <li>Evaluate and recommend new and technologies</li> <li>Provide technical review of standardized District security framework</li> <li>Develop, miliptement and maintain security requirements</li> <li>Provide technical review of standardized District security framework</li> <li>Develop, miliptement defense in depth controls to miligate risk</li> <li>Provide technical review of standardized District security framework</li> <li>Develop, miliptement defense in other security incident response plan tests</li> <li>Develop, miliptement security framework</li> <li>Design, develop and implement standardzed District security framework</li> <li>Design, develop and implement standardzed District security framework</li> <li>Design, develop and implement standardzed District security framework</li> <li>Design, develop and</li></ul>				
<ul> <li>requirements</li> <li>Implement defense in depth controls to mitigate risk</li> <li>Provide technical review of standardized District security framework</li> <li>Implement, support and evaluate security-focused tools and services</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Assist with hird-party penetration tests</li> <li>Evaluate and recommend new and technicigies</li> <li>System hardening</li> <li>Vulnerability assessments</li> <li>Implement and maintain security requirements and recommend additional security requirements</li> <li>Develop and implement defense in cyber security incident response plan tests</li> <li>Develop and implement and maintain security requirements</li> <li>Develop and implement defense in cyber security incident response plan tests</li> <li>Develop and implement and maintain security requirements and recommend defense in cyber security incident response plan tests</li> <li>Develop and implement and participate in cyber security incident response plan tests</li> <li>Develop and implement and maintain security requirements</li> <li>Develops and implement defense in cyber security incident response plan tests</li> <li>Develops and implement defense in cyber security incident response plan tests</li> <li>Develops and implement defense in cyber security incident response plan tests</li> <li>Develops and implement defense in cyber security incident response plan tests</li> <li>Develops and implement defense in cyber security incident response plan tests</li> <li>Develops and implement defense in cyber security incident response plan tests</li> <li>Develops and implement defense in cyber security incident response plan tests</li> <li>Develops and implement test on and area security updates</li> <li>Develops and implement defense in cyber security incident response plan tests</li> <li>Develops and implement test of and participate in cyber security incident tesponse plan tests</li> <li>Develops implement and maintain security requirements a</li></ul>				
<ul> <li>Implement defense in depth controls to mitigate risk</li> <li>Provide technical review of standardized District security framework</li> <li>Implement, support and evaluate security focused tools and services</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Evaluate and recommend new and emerging security products and technologies</li> <li>System hardening</li> <li>Network Access Control (NAC)</li> <li>Unrelability assessments</li> <li>Develop and implement adefense in depth controls to mitigate risk</li> <li>Provide technical review of standardized District security framework</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Conduct and participate in cyber security requirements</li> <li>Develop, and implement admantian security requirements security requirements and recommend additional security requirements and resonmend additional security requiremen</li></ul>		-		• • •
<ul> <li>mitigate risk</li> <li>Provide technical review of standardized District security framework</li> <li>Implement, support and evaluate security focused tools and services</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>E valuate and recommend new and emerging security products and technologies</li> <li>Lesst access privilege implementation</li> <li>Umplement and maintain security requirements</li> <li>Develop, implement, support and evaluate response plan tests</li> <li>Configuration management/Baseline monitoring</li> <li>System hardening</li> <li>Network Access Control (NAC)</li> <li>Vulnerability assessments</li> <li>Implement and maintain security requirements</li> <li>Develop and implement defense in depth controls te onity framework</li> <li>Develop, implement, support and evaluate security-forcused tools and services</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Conduct and participate in cyber security requirements</li> <li>Develop, and implement defense in cyber security requirements</li> <li>Develop, implement, support and evaluate security-forcused tools and services</li> <li>Conduct and participate in cyber security requirements</li> <li>Develop, implement, support and evaluate security-forcused tools and services</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Conduct and participate in cyber security incident security-forcused tools and services</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Conduct and participate in cyber security incident response plan tests</li> </ul>				
<ul> <li>Provide technical review of standardized District security framework</li> <li>Implement, support and evaluate security frocused tools and services</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Assist with hird-party penetration tests</li> <li>Evaluate and recommend new and emerging security products and technologies</li> <li>Evaluate and recommend new and emerging security products and technologies</li> <li>Valuerability assessments</li> <li>Develop and implement defense in depting conduct and participate in cyber security incident response plan tests</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Design, develop and implement standardized District security framework</li> <li>Design, develop, mplement, support and evaluate security-focused tools and security-coused tools and services</li> <li>Conduct and participate in cyber security incident response plan tests</li> </ul>				
District security framework <ul> <li>District security framework</li> <li>Implement, support and evaluate security updates</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Assist with third-party penetration tests</li> <li>Evaluate and recommend new and emerging security products and technologies</li> <li>System hardening</li> <li>Network Access privilege</li> <li>Network Access privilege</li> <li>Unplement, support and evaluate security requirements</li> <li>Network Access privilege</li> <li>Implement and maintain security requirements</li> <li>Develop and implement defense in depth; controls to mitigate risk</li> <li>Provide technical review of and safeguards</li> <li>Develop, implement, support and evaluate security requirements</li> <li>Develop, and participate in cyber security incident response plan tests</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Develop and implement defense in depth;</li> <li>Develop, implement, support and evaluate security requirements and recommend additional security requirements and seleguards</li> <li>Deseign, develop and implement defense</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Conduct and participate in cyber security framework</li> <li>Design, develop and implement defense in depth controls to mitigate risk</li> <li>Provide technical review of and implement defense in depticate executive focused tools and services</li> <li>Conduct and participate in cyber security framework</li> <li>Design, develop and implement and evaluate security focused tools and services</li> <li>Conduct and par</li></ul>				
<ul> <li>Implement, support and evaluate security-focused tools and services</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Assist with hird-party penetration tests</li> <li>Software and security updates</li> <li>Configuration management</li> <li>Asset management/Baseline monitoring</li> <li>System hardening</li> <li>Network Access Control (NAC)</li> <li>Least access privilege implementation</li> <li>Vulnerability assessments</li> <li>Implement and maintain security requirements</li> <li>Develop and implement defense in depth controls to mitigate risk</li> <li>Provide technical review of standardized District security framework</li> <li>Develop, implement, support and evaluate security-focused tools and services</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Develop, implement and participate in cyber security incident response plan tests</li> <li>Develop and implement defense in depth controls to mitigate risk</li> <li>Develop and implement defense in cyber security incident response plan tests</li> <li>Develop and tervices</li> <li>Conduct and participate in cyber security framework</li> <li>Design, develop and implement defense in cyber security framework</li> <li>Design, develop, and and evaluate security-focused tools and services</li> <li>Conduct and participate in cyber security incident trieparty penetration tests</li> </ul>				
focused tools and services <ul> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Assist with third-party penetration tests</li> <li>Evaluate and recommend new and technologies</li> <li>System hardening</li> <li>Network Access Control (NAC)</li> <li>Least access privilege implementation tests</li> <li>Umplement and maintain security requirements</li> <li>Develop and implement defense in depth controls to mitigate risk</li> <li>Develop, implement, support and evaluate security framework</li> <li>Develop, implement, support and evaluate security framework</li> <li>Develop, implement tests</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Configuration management</li> <li>Asset management/Baseline monitoring</li> <li>System hardening</li> <li>System hardening</li> <li>System hardening</li> <li>System hardening</li> <li>Network Access Control (NAC)</li> <li>Least access privilege implementation</li> <li>Vulnerability assessments</li> <li>Hinglement and maintain security requirements and recommend additional security requirements and arecommend additional security framework</li> <li>Develop, implement, support and evaluate security framework</li> <li>Develop, implement, support and evaluate security framework</li> <li>Design, develop, implement, support and evaluate security framework</li> </ul> <ul> <li>Provide technical review of and implement support and evaluate security framework</li> <li>Design, develop, implement, support and evaluate security framework</li> <li>Deseign, develop, implement, support and evaluate security</li></ul>				
<ul> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Assist with third-party penetration tests</li> <li>Evaluate and recommend new and emerging security products and technologies</li> <li>Vulnerability assessments</li> <li>Implement and maintain security requirements</li> <li>Develop and implement defense in depth controls to mitigate risk</li> <li>Develop, implement, support and evaluate security-focused toils and services</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Coordinate third-party penetration tests</li> <li>Software and security updates on toring</li> <li>Asset management/Baseline monitoring</li> <li>Asset management/Baseline monitoring</li> <li>Network Access Control (NAC)</li> <li>Least access privilege implementation</li> <li>Vulnerability assessments</li> <li>Develop and implement defense in depth controls to mitigate risk</li> <li>Develop, implement, support and evaluate security-focused tools and services</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Coordinate third-party penetration tests</li> <li>Software and security for security framework</li> <li>Design, develop and implement and standardized District security framework</li> <li>Design, develop and implement and standardized District security framework</li> <li>Design, develop in plement, support and evaluate security-focused tools an</li></ul>				
<ul> <li>incident response plan tests</li> <li>Assist with third-party penetration tests</li> <li>Evaluate and recommend new and emerging security products and technologies</li> <li>System hardening</li> <li>Network Access Control (NAC)</li> <li>Usats access privilege implementation</li> <li>Vulnerability assessments</li> <li>Implement and maintain security requirements</li> <li>Develop and implement defense in depth controls to mitigate risk</li> <li>Provide technical review of standardized District security framework</li> <li>Develop, implement, support and evaluate security-focused tools and services</li> <li>Conduct and participate in cyber security incident response plan tests</li> </ul>				
<ul> <li>Assist with third-party penetration tests</li> <li>Evaluate and recommend new and emerging security products and technologies</li> <li>Evaluate and recommend new and emerging security products and technologies</li> <li>Implement and maintain security requirements</li> <li>Implement and maintain security requirements</li> <li>Develop and implement defense in depth controls to mitigate risk</li> <li>Provide technical review of standardized District security framework</li> <li>Develop, implement, support and evaluate security-focused tools and services</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Coordinate third-party penetration tests</li> </ul>			5	
<ul> <li>Evaluate and recommend new and emerging security products and technologies</li> <li>Network Access Control (NAC)</li> <li>Least access privilege implementation</li> <li>Vulnerability assessments</li> <li>Implement and maintain security requirements</li> <li>Implement and maintain security requirements</li> <li>Develop and implement defense in depth controls to mitigate risk</li> <li>Provide technical review of standardized District security framework</li> <li>Develop, implement, support and evaluate security-focused tools and services</li> <li>Conduct and participate in cyber security incident response plant ests</li> <li>Coordinate third-party penetration tests</li> </ul>				
<ul> <li>Least access privilege implementation</li> <li>Least access privilege</li> <li>Multiplement and maintain security requirements</li> <li>Develop and implement defense in depth controls to mitigate risk</li> <li>Develop, implement, support and evaluate security-focused tools and services</li> <li>Conduct and participate tists</li> <li>Develop, implement, support and evaluate security-focused tools and services</li> <li>Conduct and participate tists</li> <li>Develop, implement, support and evaluate security-focused tools and services</li> <li>Conduct and participate tists</li> <li>Develop, implement, support and evaluate security-focused tools and services</li> <li>Conduct and participate tists</li> <li>Develop, implement, support and evaluate security-focused tools and services</li> <li>Conduct and participate tists</li> <li>Design, develop, implement, support and evaluate security-focused tools and services</li> <li>Conduct and participate tists</li> <li>Design, develop, implement, support and evaluate security-focused tools and services</li> <li>Design, develop, implement, support and evaluate security-focused tools and</li> </ul>				
<ul> <li>implementation</li> <li>Vulnerability assessments</li> <li>Implement and maintain security requirements</li> <li>Develop and implement defense in depth controls to mitigate risk</li> <li>Develop and implement, support and evaluate security-focused tools and services</li> <li>Develop, implement, support and evaluate security-focused tools and services</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Coordinate third-party penetration tests</li> <li>Develop, implement defense in depth controls to mitigate risk</li> <li>Develop, implement, support and evaluate security-focused tools and services</li> <li>Coordinate third-party penetration tests</li> <li>Develop, implement ferse</li> <li>Coordinate third-party penetration tests</li> </ul>				5
<ul> <li>Vulnerability assessments</li> <li>Implement and maintain security requirements</li> <li>Implement and maintain security requirements</li> <li>Develop and implement defense in depth controls to mitigate risk</li> <li>Provide technical review of standardized District security framework</li> <li>Develop, implement, support and evaluate security-focused tools and services</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Coordinate third-party penetration tests</li> <li>Coordinate third-party penetration tests</li> <li>Conduct and participate in cyber security framework</li> <li>Design, develop, implement, support and evaluate security-focused tools and evaluate security-focused tools and</li> </ul>				
<ul> <li>Implement and maintain security requirements</li> <li>Develop and implement defense in depth controls to mitigate risk</li> <li>Develop and implement defense in depth controls to mitigate risk</li> <li>Provide technical review of standardized District security framework</li> <li>Develop, implement, support and evaluate security-focused tools and services</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Coordinate third-party penetration tests</li> <li>Implementation</li> <li>Vulnerability assessments</li> <li>Analyze and validate established security requirements and recommend additional security requirements and safeguards</li> <li>Design, develop, implement, support and evaluate security-focused tools and evaluate security-focused tools and</li> </ul>		lecinologies		
<ul> <li>requirements</li> <li>Develop and implement defense in depth controls to mitigate risk</li> <li>Provide technical review of standardized District security framework</li> <li>Provide technical review of standardized District security framework</li> <li>Develop, implement, support and evaluate security-focused tools and services</li> <li>Conduct and participate in cyber security framework</li> <li>Design, develop, implement, support and evaluate security framework</li> <li>Design, develop, implement, support and evaluate security framework</li> </ul>				
<ul> <li>Develop and implement defense in depth controls to mitigate risk</li> <li>Provide technical review of standardized District security framework</li> <li>Develop, implement, support and evaluate security-focused tools and services</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Coordinate third-party penetration tests</li> <li>Develop, implement defense in depth controls to mitigate risk</li> <li>Develop, implement, support and evaluate security framework</li> <li>Develop, implement, support and evaluate security framework</li> <li>Develop, implement, support and evaluate security framework</li> <li>Design, develop and implement defense in depth controls to mitigate risk</li> <li>Provide technical review of and implement standardized District security framework</li> <li>Design, develop, implement, support and evaluate security framework</li> </ul>				<ul> <li>Vulnerability assessments</li> </ul>
<ul> <li>controls to mitigate risk</li> <li>Provide technical review of standardized District security framework</li> <li>Develop, implement, support and evaluate security-focused tools and services</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Coordinate third-party penetration tests</li> </ul>				
<ul> <li>Provide technical review of standardized District security framework</li> <li>Develop, implement, support and evaluate security-focused tools and services</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Coordinate third-party penetration tests</li> <li>Coordinate third-party penetration tests</li> </ul>				
<ul> <li>District security framework</li> <li>Develop, implement, support and evaluate security-focused tools and services</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Coordinate third-party penetration tests</li> <li>Design, develop and implement defense in depth controls to mitigate risk</li> <li>Provide technical review of and implement standardized District security framework</li> <li>Design, develop, implement, support and evaluate security framework</li> </ul>			ů, se	
<ul> <li>Develop, implement, support and evaluate security-focused tools and services</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Coordinate third-party penetration tests</li> <li>in depth controls to mitigate risk</li> <li>Provide technical review of and implement standardized District security framework</li> <li>Design, develop, implement, support and evaluate security-focused tools and services</li> </ul>				
<ul> <li>security-focused tools and services</li> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Coordinate third-party penetration tests</li> <li>Provide technical review of and implement standardized District security framework</li> <li>Design, develop, implement, support and evaluate security-focused tools and</li> </ul>				in depth controls to mitigate risk
<ul> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Coordinate third-party penetration tests</li> <li>Standardized District security framework</li> <li>Design, develop, implement, support and evaluate security-focused tools and</li> </ul>				
<ul> <li>incident response plan tests</li> <li>Design, develop, implement, support and evaluate security-focused tools and</li> </ul>				standardized District security framework
Coordinate third-party penetration tests     evaluate security-focused tools and				<ul> <li>Design, develop, implement, support and</li> </ul>
			Coordinate third-party penetration tests	evaluate security-focused tools and
			Define network standards for IPS/IDS and	services

	<i>/</i> /		
		<ul> <li>authentication and authorization controls</li> <li>Evaluate and recommend new and emerging security products and technologies</li> </ul>	<ul> <li>Conduct and participate in cyber security incident response plan tests</li> <li>Coordinate third-party penetration tests</li> <li>Define and implement network standards for IPS/IDS and authentication and authorization controls</li> <li>Evaluate, recommend and implement new and emerging security products and technologies</li> </ul>
Reliability Compliance       Learn about and perform v         supervision on systems witto regulatory compliance, i       Maintain Program Dorperform applicable promeet NERC CIP requipation         Provide support for intraudits including:       Annual self-control         Peer review       Act as a Contributor to Standards         Research regulatory bulletins ar information       Prepare reports by control and related industry e         Document and maintata and security controls is compliance objectives program documentation	<ul> <li>th a low level of risk ncluding:</li> <li>cumentation and occesses in order to iregulatory compliance, including:</li> <li>Create and maintain Program Documentation and perform applid processes in order to meet NERC requirements</li> <li>Provide support for internal and external and external and external</li> <li>Provide support for internal and external and external and external</li> <li>Provide support for internal and external and is including: <ul> <li>Annual self-certifications</li> <li>Standards peer review</li> <li>Reliability Standard Audit Worksheets maintenance</li> </ul> </li> <li>Illecting, analyzing mation wrking groups, forums vents in technical tools required to meet is identified in the</li> </ul>	<ul> <li>with a moderate-high level of risk to regulatory compliance and company reputation, including:</li> <li>Create and maintain Program Documentation and perform applicable processes in order to meet NERC CIP requirements</li> <li>Provide support for internal and external audits including: <ul> <li>Annual self-certifications</li> <li>Standards peer review</li> <li>Reliability Standard Audit Worksheets development and maintenance</li> <li>Audit interviews</li> </ul> </li> <li>solve Evaluate NERC Alerts</li> <li>Develop and implement mitigation actions to resolve potential compliance concerns</li> <li>Create work orders for other work groups to address NERC CIP-related requirements</li> <li>Act as a Standard Owner, Subject Matter Expert and Contributor to NERC CIP Standards</li> <li>Research regulations by reviewing regulatory bulletins and other sources of information</li> <li>Attend compliance working groups, forums and related industry events</li> <li>Develop, implement, document and maintain technical tools and security</li> </ul>	<ul> <li>Perform work on highly complex, interconnected, interdependent systems with the highest levels of risk to regulatory compliance and company reputation, including:</li> <li>Create, maintain, and optimize Program Documentation and perform applicable processes in order to meet NERC CIP requirements</li> <li>Provide support for internal and external audits including: <ul> <li>Annual self-certifications</li> <li>Standards peer review</li> <li>Reliability Standard Audit Worksheets development and maintenance</li> <li>Audit interviews</li> </ul> </li> <li>Evaluate and respond to NERC Alerts</li> <li>Design, develop and implement mitigation actions to resolve potential compliance concerns</li> <li>Create work orders for other work groups to address NERC CIP-related requirements</li> <li>Act as a Standard Owner, Subject Matter Expert and Contributor to NERC CIP Standards, including those that may include other groups in the District</li> <li>Research regulations by reviewing regulatory bulletins and other sources of information</li> <li>Prepare reports by collecting, analyzing, and summarizing information</li> <li>Represent the District at compliance working groups, forums and related industry events</li> <li>Design, develop, implement, document and maintain technical tools and security</li> </ul>

				controls required to meet compliance objectives identified in the program documentation
Project Management	<ul> <li>Learn about and perform work under close supervision on projects with a low level of risk to operations and revenue stream, including:</li> <li>Work with others in EMS group to provide tasks and time estimates for projects requiring CSE time</li> <li>Technical resource for project teams assigned to implementing or modifying District control systems</li> <li>Participate in technical meetings associated with project work that impacts SCADA design</li> </ul>	<ul> <li>Perform work under general supervision on projects with a low-moderate level of risk to operations and revenue stream, including:</li> <li>Lead small project teams that may include consultants, contractors, legal, procurement, and other District departments</li> <li>Work with others in EMS group to provide tasks and time estimates for projects requiring CSE time</li> <li>Technical resource for project teams assigned to implementing or modifying District control systems</li> <li>Organize technical meetings associated with project work that impacts SCADA design</li> </ul>	<ul> <li>Perform work on advanced projects with a moderate-high level of risk to operations and revenue stream, including:</li> <li>Lead multi-disciplinary project teams that may include consultants, contractors, legal, procurement, and other District departments</li> <li>Work with District Project Managers to provide tasks and time estimates for projects requiring CSE time</li> <li>Technical resource for project teams assigned to designing, implementing or modifying District control systems</li> <li>Perform project intake processes to add project work to DWP</li> <li>Organize technical meetings associated with project work that impacts SCADA/EMS design</li> </ul>	<ul> <li>Perform work on highly complex, multi-system projects with the highest levels of risk to operations and revenue stream, including:</li> <li>Perform project management activities including schedule, budget and execution for complex projects</li> <li>Lead multi-disciplinary and multi-functional teams that may include consultants, contractors, legal, procurement, and other District departments</li> <li>Work with Contractor, Vendor and District Project Managers to provide tasks and time estimates for projects requiring CSE time</li> <li>Technical resource for project teams assigned to designing, implementing or modifying District control systems and similar or related systems</li> <li>Perform project intake processes to add project work to DWP</li> <li>Organize technical meetings associated with project work that impacts SCADA/EMS design</li> </ul>
Education	BS in Electrical Engineering, Systems Engineering, Industrial Engineering, Computer Science or closely related field.	BS in Electrical Engineering, Systems Engineering, Industrial Engineering, Computer Science or closely related field.	BS in Electrical Engineering, Systems Engineering, Industrial Engineering, Computer Science or closely related field.	<ul> <li>BS in Electrical Engineering, Systems Engineering, Industrial Engineering, Computer Science or closely related field. Master's Degree preferred.</li> </ul>
Experience	Entry level. No experience required.	<ul> <li>Typically requires two (2) years of experience performing as a Level I or closely related experience.</li> <li>Candidates with a Master's degree who also have at least 6 months experience in the Utility industry working with SCADA systems may be hired as a Level II.</li> </ul>	<ul> <li>Typically requires three (3) years of experience performing as a Level II, or a total of five (5) years progressively responsible experience with Control System Engineering.</li> <li>Candidates with a Master's Degree may reduce total experience by 2 years.</li> </ul>	<ul> <li>Master's Degree preferred.</li> <li>Typically requires three (3) years of experience performing as a Level III or a total of eight (8) years progressively responsible experience with Control System engineering.</li> <li>Candidates with a Master's Degree may reduce total experience by 2 years.</li> </ul>
Knowledge	<ul> <li>Engineering and Industrial Control Systems security principles and practices</li> <li>Control systems theory</li> <li>Computer programming in 1 or more object-oriented or script language</li> <li>Data communications protocols and computer operating systems</li> </ul>	<ul> <li>Industrial control systems design, selection and specification of equipment and design of industrial communication and control networks for systems including Transmission, Distribution, Generation, Hydro Optimization, Hatcheries, Water/Wastewater, Security and</li> </ul>	Industrial control systems design, selection and specification of equipment and design of industrial communication and control networks for systems including Transmission, Distribution, Generation, Hatcheries, Water/Wastewater, Mid- Columbia Hourly Coordination, Security	<ul> <li>Industrial control systems design, selection and specification of equipment and design of industrial communication and control networks for systems including Transmission, Distribution, Generation, Hydro Optimization, Hatcheries, Water/Wastewater, Mid-Columbia Hourly</li> </ul>

		illeidil FOD Colltiol System Lingillee		1
	<ul> <li>Mathematical concepts such as scaling, conversions and raising to a power, logic ops (AND/OR/XOR)</li> <li>Open-loop and closed-loop control theory algorithms for linear systems</li> </ul>	<ul> <li>Compliance</li> <li>Engineering and Industrial Control Systems security principles and practices</li> <li>Distributed control (DCS), host centric (SCADA) and Embedded System environments utilizing 1 or more computing platforms, PLCs and RTUs</li> <li>Control systems theory and its practical application to process control and field instrumentation</li> <li>Computer programming in 2 or more languages, preferably one object-oriented and one script language</li> <li>Control protocols including DNP and Allen-Bradley</li> <li>Data communications protocols, networking equipment and computer operating systems</li> <li>Operating system hardening, configuration, troubleshooting and maintenance techniques</li> <li>Automation, system and communications integration methodologies</li> <li>Power generation for hydro unit operation</li> <li>Regulatory laws, standards and requirements including NERC CIP Reliability Standards</li> <li>Complex spreadsheets and database applications</li> <li>Basic knowledge of project management concepts, principles and practices</li> </ul>	<ul> <li>and Compliance</li> <li>Engineering and Industrial Control Systems security principles and practices</li> <li>Distributed control (DCS), host centric (SCADA) and Embedded System environments utilizing 2 or more computing platforms, PLCs and RTUs</li> <li>Control systems theory and its practical application to process control and field instrumentation</li> <li>Computer programming in 3 or more languages, preferably a combination of object-oriented and script languages</li> <li>Control protocols including DNP, OPC, Allen-Bradley and MODBUS</li> <li>Data communications protocols, networking equipment and computer operating systems</li> <li>Operating system hardening, configuration, troubleshooting and maintenance techniques</li> <li>Automation, system and communications integration methodologies</li> <li>Mid-Columbia control and hourly coordination</li> <li>Power generation for hydro unit operation</li> <li>Energy accounting</li> <li>Regulatory laws, standards and requirements including FERC/ NERC Reliability Standards</li> <li>Complex spreadsheets and database applications</li> <li>Project management concepts, principles and practices</li> </ul>	<ul> <li>Coordination, Security and Compliance</li> <li>Engineering and Industrial Control Systems security principles and practices</li> <li>Distributed control (DCS), host centric (SCADA) and Embedded System environments utilizing 3 or more computing platforms, PLCs and RTUs</li> <li>Control systems theory and its practical application to process control and field instrumentation</li> <li>Computer programming in 4 or more languages, preferably a combination of object-oriented and script languages</li> <li>Control protocols including DNP, OPC, ICCP, Allen-Bradley, L&amp;G 8979 and MODBUS</li> <li>Data communications protocols, networking equipment and computer operating systems</li> <li>Operating system hardening, configuration, troubleshooting, maintenance, and optimization techniques</li> <li>Automation, system and communications integration methodologies</li> <li>Mid-Columbia control and hourly coordination</li> <li>Power generation for hydro unit operation</li> <li>Energy accounting</li> <li>Regulatory laws, standards and requirements including FERC/ NERC Reliability Standards</li> <li>Complex spreadsheets and database applications</li> <li>Project management concepts, principles and practices</li> </ul>
Systems & Technical Skills	<ul> <li>Work with a field support team to diagnose issues.</li> </ul>	<ul> <li>Collect, process, preserve, analyze, and present computer-related evidence in support of network vulnerability mitigation, counterintelligence or law enforcement investigations.</li> <li>Work with a field support team to diagnose issues and propose resolution</li> <li>Respond to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats. Use mitigation, preparedness, and response</li> </ul>	<ul> <li>Vulnerability Assessment and Management - Conduct assessments of threats and vulnerabilities. Determine deviations from acceptable configurations, enterprise or local policy. Assess the level of risk, and develop and/or recommend appropriate mitigation countermeasures in operational and non-operational situations.</li> <li>Synthesize and place intelligence information in context; draws insights</li> </ul>	<ul> <li>Analyze threat information from multiple sources, disciplines, and agencies across the Intelligence Community.</li> <li>Vulnerability Assessment and Management - Conduct assessments of threats and vulnerabilities. Determine deviations from acceptable configurations, enterprise or local policy. Assess the level of risk, and develop and/or recommend appropriate mitigation countermeasures in operational and non-operational</li> </ul>

		Enclair I OD Control System Enginee		
		<ul> <li>and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.</li> <li>Participates as a reviewer in technical reviews</li> </ul>	<ul> <li>about the possible implications.</li> <li>Collect, process and preserve computer-related evidence in support of network vulnerability mitigation, counterintelligence or law enforcement investigations.</li> <li>Work with a field support team to diagnose issues and propose resolution</li> <li>Respond to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats. Use mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.</li> <li>Participates as a reviewer in technical reviews</li> </ul>	<ul> <li>situations.</li> <li>Use defensive measures and data from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.</li> <li>Synthesize and place intelligence information in context; draws insights about the possible implications.</li> <li>Collect, process, preserve, analyze, and present computer-related evidence in support of network vulnerability mitigation, counterintelligence or law enforcement investigations.</li> <li>Work with a field support team to diagnose issues and propose resolution</li> <li>Respond to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats. Use mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.</li> <li>Participates as a reviewer in technical reviews</li> </ul>
Other Skills	<ul> <li>Strong reasoning, analytical and problem solving skills</li> <li>Data analysis and research</li> <li>Communicate logically and clearly, both orally and in writing</li> <li>Communicate technical information effectively to non-department and non-technical staff</li> <li>Technical writing</li> </ul>	<ul> <li>Strong reasoning, analytical and problem solving skills</li> <li>Data analysis, research and report development</li> <li>Communicate logically and clearly, both orally and in writing</li> <li>Interpret engineering problems and solutions and communicate technical information effectively to non-department and non-technical staff</li> <li>Technical writing</li> <li>Estimates project cost and schedule</li> <li>Actively look ahead to plan for and respond to project challenges</li> <li>Contribute to the development of department policies, procedures, and standards.</li> </ul>	<ul> <li>Strong reasoning, analytical and problem solving skills</li> <li>Data extraction, data analysis, research and report development</li> <li>Understand contract documents</li> <li>Communicate logically and clearly, both orally and in writing</li> <li>Interpret engineering problems and solutions and communicate technical information effectively to non-department and non-technical staff</li> <li>Technical writing</li> <li>Estimates project cost and schedule</li> <li>Seek long term benefits to the overall project when determining system and control design approach</li> <li>Actively look ahead to plan for and respond to project challenges</li> </ul>	<ul> <li>Strong reasoning, analytical and problem solving skills</li> <li>Data extraction, data analysis, research and report development</li> <li>Understand, interpret and contribute to the development of contract documents</li> <li>Communicate logically and clearly, both orally and in writing</li> <li>Interpret engineering problems and solutions and communicate technical information effectively to non-department and non-technical staff</li> <li>Technical writing</li> <li>Estimates project cost and schedule</li> <li>Aware of the "business" of control engineering as well as the technical design issues</li> <li>Seek long term benefits to the overall</li> </ul>

Systems & Technical	Learn new computer systems from	Learn new computer systems from	<ul> <li>Reviews company policies and industry practices, and develops and implements procedures, and standards.</li> <li>Learn new computer systems from</li> </ul>	<ul> <li>project when determining system and control design approach</li> <li>Actively look ahead to plan for and respond to project challenges</li> <li>Reviews company policies and industry practices, and develops and implements procedures, and standards.</li> <li>Learn new computer systems from</li> </ul>
Abilities	<ul> <li>documentation and training</li> <li>Diagnose problems to isolate cause</li> <li>Maintain, troubleshoot and modify program HMI components</li> <li>Analyze programming, observe monitoring signals, troubleshoot systems</li> <li>Think beyond past approaches and propose practical approaches to control design</li> <li>Follow test plans for Security Controls and Automation</li> <li>Apply the principles of software management to organize and maintain software integrity</li> <li>Act as a Contributor for assigned SCADA and associated supporting systems</li> </ul>	<ul> <li>documentation and training</li> <li>Act as a Subject Matter Expert for 2 or more SCADA, Compliance and associated supporting systems</li> <li>Diagnose problems to isolate cause</li> <li>Maintain, troubleshoot and modify program HMI components</li> <li>Analyze programming, observe monitoring signals, troubleshoot systems</li> <li>Think beyond past approaches and propose practical approaches to control design</li> <li>Identify solutions of low complexity by analyzing data, evaluating alternatives and recommending an appropriate course of action</li> <li>Write clear system requirements and test plans for Security Controls and Automation</li> <li>Apply the principles of software management to organize and maintain software integrity</li> <li>Apply mathematical concepts such as scaling, conversions, raising to a power and logic ops (AND/OR/XOR)</li> <li>Apply open-loop and closed-loop control theory algorithms for linear systems</li> <li>Carry out complex technical tasks</li> </ul>	<ul> <li>documentation and training</li> <li>Act as a Subject Matter Expert for 3 or more SCADA, Compliance and associated supporting systems</li> <li>Diagnose problems to isolate cause</li> <li>Maintain, troubleshoot and modify program HMI components</li> <li>Analyze programming, observe monitoring signals, troubleshoot systems</li> <li>Think beyond past approaches to propose and implement practical approaches to control design</li> <li>Identify solutions of moderate complexity by analyzing data, evaluating alternatives and recommending an appropriate course of action</li> <li>Apply technical knowledge of legacy systems to design new functionality</li> <li>Write clear system requirements and test plans for Security Controls and Automation</li> <li>Apply the principles of software management to organize and maintain software integrity</li> <li>Apply mathematical concepts such as scaling, conversions, raising to a power, logic ops (AND/OR/XOR), integration, and totalization</li> <li>Apply open-loop, closed-loop, time- weighted, and weighted-sum control theory algorithms for linear systems</li> <li>Act as a Subject Matter Expert as it relates to cyber security in industrial control systems</li> <li>Carry out highly complex technical tasks</li> </ul>	<ul> <li>documentation and training</li> <li>Act as a Subject Matter Expert for 4 or more SCADA, Compliance and associated supporting systems</li> <li>Diagnose problems to isolate cause</li> <li>Maintain, troubleshoot and modify program HMI components</li> <li>Analyze programming, observe monitoring signals, troubleshoot systems</li> <li>Think beyond past approaches to propose and implement practical approaches to control design</li> <li>Identify solutions of high complexity by analyzing data, evaluating alternatives and recommending an appropriate course of action</li> <li>Apply technical knowledge of legacy systems to design new functionality</li> <li>Write clear system requirements and test plans for Security Controls and Automation</li> <li>Apply the principles of software management to organize and maintain software integrity</li> <li>Apply mathematical concepts such as scaling, conversions, raising to a power, logic ops (AND/OR/XOR), integration, totalization, linear fit approximation and extrapolation</li> <li>Design and apply open-loop, closed-loop, time-weighted, and weighted-sum control theory algorithms for linear and non-linear systems</li> <li>Provide technical direction and act as a Subject Matter Expert as it relates to cyber security in industrial control systems</li> </ul>

				Carry out highly complex technical tasks
Other Abilities	<ul> <li>Identify, research and gather relevant information from a variety of sources</li> <li>Meet deadlines on multiple simultaneous priorities for multiple stakeholders</li> <li>Respond to after-hours call-outs</li> <li>Attend industry meetings and conferences, which may involve travel</li> <li>Contribute training material to other engineers and dedicated District training professional staff</li> <li>Clearly communicate technical information to end users and stakeholders</li> </ul>	<ul> <li>Identify, research and gather relevant information from a variety of sources</li> <li>Meet deadlines on multiple simultaneous priorities for multiple stakeholders</li> <li>Respond to after-hours call-outs</li> <li>Represent District at industry meetings and conferences, which may involve travel</li> <li>Train other engineers and dedicated District training professional staff</li> <li>Clearly communicate technical information to end users and stakeholders</li> </ul>	<ul> <li>Identify, research and gather relevant information from a variety of sources</li> <li>Meet deadlines on multiple simultaneous priorities for multiple stakeholders</li> <li>Respond to after-hours call-outs</li> <li>Represent District at industry meetings and conferences, which may involve travel</li> <li>Train other engineers and dedicated District training professional staff</li> <li>Clearly communicate technical information to end users and stakeholders</li> </ul>	<ul> <li>Identify, research and gather relevant information from a variety of sources</li> <li>Meet deadlines on multiple simultaneous priorities for multiple stakeholders</li> <li>Respond to after-hours call-outs</li> <li>Represent District at industry meetings and conferences, which may involve travel</li> <li>Train other engineers and dedicated District training professional staff</li> <li>Clearly communicate technical information to end users and stakeholders</li> </ul>
Leadership	None	None	Mentor lower level engineers	Train and mentor lower level engineers     and provide effective feedback
Decision making	<ul> <li>Works to achieve established goals under close supervision</li> <li>Consults supervisor or lead when problems occur</li> <li>Regularly provides work status updates to the responsible lead</li> </ul>	<ul> <li>Works to achieve established goals under general supervision</li> <li>Consults supervisor or lead when problems occur</li> <li>Regularly provides work status updates to the responsible lead</li> <li>Work is reviewed by senior engineers for application of sound engineering judgment</li> </ul>	<ul> <li>Informs lead or supervisor of unusual, complex, difficult or controversial problems</li> <li>Performs moderately complex assignments under limited supervision</li> <li>Regularly provides work status updates to the responsible lead</li> <li>Required to make decisions that will affect project objectives</li> <li>Exercise sound and independent judgment, conduct independent analyses and make recommendations on difficult and sensitive issues</li> </ul>	<ul> <li>Informs lead or supervisor of unusual, complex, difficult or controversial problems and is expected to propose and be able to implement effective solutions</li> <li>Independently performs complex and high priority assignments with limited supervision and guidance regarding overall objectives, critical issues, priorities and policy matters</li> <li>Regularly provides work status updates to the responsible lead</li> <li>Required to make decisions that give direction to project teams and significantly affect project outcomes</li> <li>Exercise sound and independent judgment, conduct independent analyses and make recommendations on difficult and sensitive issues</li> </ul>
Complexity	<ul> <li>Requires basic knowledge of Industrial Control Systems principles, practices and engineering theory</li> <li>Work on systems is limited to assignments with little to no impacts on worker safety and asset operations</li> </ul>	<ul> <li>Working knowledge of Industrial Control Systems principles, practices and engineering theory</li> <li>Work on systems has limited impact on worker safety and asset operations</li> </ul>	<ul> <li>Intermediate knowledge of Industrial Control Systems principles, practices and engineering theory</li> <li>Basic knowledge of other functions across the District</li> <li>Work assignments have moderate impacts on worker safety and asset operations</li> </ul>	<ul> <li>Expert knowledge of Industrial Control Systems principles, practices and engineering theory</li> <li>Working knowledge of other engineering disciplines across the District</li> <li>Work assignments have significant impacts on worker safety and asset operations</li> </ul>
Career Path/Advancement	This is the entry-level position within the Control Systems Engineering Job Family.	This is the second level position within the Control Systems Engineering Job Family.	This is the third level position within the Control Systems Engineering Job Family.	This is the highest level individual contributor (non-leadership) position within the Control Systems Engineering Job Family.

To advance to Level II, incur able to perform all the essen the higher level position, at a Advancement is subject to a business need for a higher le salary budget availability.	able to perform all the essential function a basic level. abasic level. abasic level. abasic level. abasic level. able to perform all the essential function the higher level position, at a higher level competency than a level II. Advancement is subject to approval of the business need for a higher level position salary budget availability.	<ul><li>able to perform all the essential functions of the higher level position, at a higher level of competency than a level III.</li><li>Advancement is subject to approval of the</li></ul>	Advancement to the Lead Level will generally be the result of a competitive recruitment process and is subject to availability of a vacant approved position.
Employees in Level I are exp to Level II within a reasonab typical timeline for advancer from entry into the Level I cla	bected to advance le time frame. The The typical timeline for advancement is nent is 2 years from entry into the Level II classification.	3 years The typical timeline for advancement is 3 years	