

**Idaho Judicial Branch
Position Description**

Position Title:	IT Security Analyst I/II/Sr.
Effective Date:	October 2018
Salary Grade/Range:	Grade 15/16
	Level I: \$49,852 - \$62,315
	Level II: \$62,315 - \$74,778
	Sr. Level: \$71,585 - \$85,902
FLSA Status:	Exempt – Computer
EEO Job Category:	Professional

General Position Summary:

The Idaho Supreme Court is seeking a highly dedicated, technical candidate for the IT Security Analyst position to implement and provide security services to ensure networks, systems, and applications are appropriately designed, configured, secured and maintained to protect the Idaho Judiciary's information assets. This position will determine, analyze, and propose security requirements and technical solutions. The IT Security Analyst will work in partnership with all Information Division team members, as well as county IT staff and statewide functional business areas to drive security improvements. The individual will be responsible for implementation, maintenance and administration of the Court's security technologies and processes. This position works under the direction of the Manager, IT Operations and Infrastructure.

Major Duties and Responsibilities: (The examples provided do not cover all the duties which the incumbent in this position may be required to perform.)

- Determine, analyze, and propose an enterprise security architecture and associated security requirements;
- Assist in proposing technical solutions and system configurations to meet specified security requirements;
- Conduct detailed security technical reviews of new or existing technologies and/or applications;
- Develop solutions and coordinate actions to mitigate system security threats and risks;
- Perform security product evaluations, provide recommendations, and implement products/services to improve the Court's security posture;
- Implement and conduct security incident monitoring to identify and minimize threats to the Court's operations and technical environment;
- Monitor and assess activity and events from intrusion detection/prevention systems, other security technologies, and system log data collected to identify and react to new threats and incidents;
- Review and identify root causes of security incidents, develop corrective actions, reassess inherent risks and drive future proactive/preventive actions;
- Establish formal vulnerability/risk management processes including but not limited, to vulnerability assessments, penetration testing, vulnerability remediation and compliance testing;
- Develop and manage a process to track vulnerability and threat trends, to include metrics for tracking and analyzing vulnerability remediation efforts;
- Assist with the management of security technologies to include, but not limited to, firewalls, access control lists, anti-virus software, web content filtering, authentication systems, and other technologies;
- Work with application teams to implement and audit appropriate security controls, to include user/role management, segregation of duties, encryption, password controls and other security configuration items;
- Provide technical security advice and serve as a technical training resource to management and staff;
- Perform other information security or technology tasks as required to meet business requirements;
- Maintain security consistent with court policy;
- Configure, tune and optimize intrusion detection/prevention systems, security event/incident management systems, and other security technologies, as applicable;
- Perform other duties as assigned.

Minimum Qualifications:

Education and Experience

- Bachelor's Degree in Computer Science, Information Security or a related;
- One (1) year of preferred work experience;
- Experience with application security, network, host, and data;
- Hands-on experience with multiple operating system environments (such as Windows, Linux, Unix);
- Strong familiarity with enterprise security architecture principles;

Knowledge, Skills, and Abilities

- Knowledge of enterprise security architecture principles;
- Knowledge of infrastructure and application security design;
- Knowledge of operating systems such as Windows, Windows Server, and VMware as well as Linux and Unix;
- Knowledge of Social Media Platforms;
- Knowledge of SQL Server security;
- Knowledge of Citrix systems;
- Knowledge of application and operating systems security configuration and best practices to include a detailed understanding of operating systems security and functionality requirements;
- Ability to work independently;
- Ability to communicate effectively verbally and in writing;
- Ability to match system solutions to specific user requirements and functions;
- Ability to follow complex verbal and written instructions;
- Ability to detect and define obscure problems and propose feasible, cost-effective solutions;
- Ability to write, read, and interpret flow charts and other documentation;
- Ability to display an attitude of cooperation and work harmoniously with all levels of court employees, the general public, and other organizations;
- Ability to manage competing priorities;
- Ability to complete assignments in a timely fashion;
- Ability to travel throughout the State of Idaho.

Distinguishing Features of the Job Class:

The IT Security Analyst I is the entry-level position in the Security Analyst job class. The position performs the duties as listed above. The position requires a Bachelor's Degree in Computer Science, Information Security or a related field and one (1) year of relevant work experience preferred.

The IT Security Analyst II is the second level in the Security Analyst job class. The position requires a Bachelor's Degree in Computer Science, Information Security or a related field and three (3) years of relevant work experience preferred.

In addition to the duties listed above, the IT Security Analyst II possesses the following qualifications:

- Identify security risks, threats and vulnerabilities for the Court's network, systems, and applications;
- Experience working with firewall, vulnerability scanning, host protection, and intrusion detection/prevention products preferred;
- Knowledge of training principles and practices for teaching and instruction for individuals and groups, and the measurement of training effects preferred;
- Certifications such as CISSP, CISA, CCNA, Sigma 6, ITIL, and ISO 9000.

The Sr. IT Security Analyst is the third level in the Security Analyst job class. The position requires a Bachelor's Degree in Computer Science, Information Security or a related field and five (5) years of relevant work experience preferred.

In addition to the duties listed above, the Sr. IT Security Analyst possesses the following qualifications:

- Lead security initiatives to design, assess, implement, and remediate systems to ensure appropriate protection of the Court's information, and to comply with applicable security standards, regulations, and policies;
- Develop and assess security policies, standards, and guidelines;
- Knowledge of Change Management principles and practices;
- Certifications such as CISSP, CISA, CCNA, Sigma 6, ITIL, and ISO 9000

The Judicial Branch reserves the right to consider an equivalent combination of education, training, and/or experience in determining whether an applicant is capable of performing the assigned duties and fulfilling the assigned responsibilities of this position.

Application Instructions:

If interested in being considered for this position, please complete the employment application on our website at www.isc.idaho.gov/careers and submit it, along with your cover letter and résumé, to hr@idcourts.net or to the Idaho Judicial Branch, Human Resources Office, P.O. Box 83720, Boise, ID 83720-0101. Application packets must be received by **5:00 p.m. MST, Friday, November 16, 2018.**

The Idaho Courts are an equal opportunity employer. Hiring is done without regard to race, color, national origin, sex, age, religion, socioeconomic status, sexual orientation, gender identity, disability or any other applicable legally protected status. In addition, preference may be given to veterans who qualify under state and federal laws and regulations. If you need special accommodation for applying or interviewing, please notify Human Resources.