



SAN DIEGO COUNTY WATER AUTHORITY
invites applications for the position of:

Information Systems Analyst (Cyber Security)

An Equal Opportunity Employer

SALARY:

<u>Hourly</u>	<u>Monthly</u>	<u>Annually</u>
\$39.14 - \$52.64	\$6,783.75 - \$9,123.40	\$81,404.96 - \$109,480.80

OPENING DATE: 01/11/18

CLOSING DATE: 02/08/18 05:30 PM

THE ORGANIZATION:

Join one of the San Diego region's most reputable and progressive public agencies!

The San Diego County Water Authority is an independent public agency that serves as San Diego County's regional water wholesaler. The mission of the San Diego County Water Authority is to provide a safe and secure water supply to its 24 member agencies serving the region's \$222 billion economy and its 3.3 million residents.

With an acute awareness of San Diego's dependence on imported water sources, the Water Authority is executing a long-term strategy to diversify the region's supply sources, make major investments in the region's water delivery and storage system, and improve water-use efficiency. Through dynamic leadership, thoughtful planning, and prudent fiscal policies, the Water Authority is cost-effectively managing the region's water portfolio, while continuing to diversify supplies to enhance future reliability.

The Department

The Administrative Services Department provides services that support the efficient operation of the Water Authority. Responsibilities include administrative support to the Board of Directors; procurement support for solicitations and contracts; administration of the safety and risk management program; maintenance of computer Enterprise Resource Planning systems and other software; acquisition and maintenance of computer hardware; maintenance and development of Geographic Information Systems; administration of the records management program; and management of all facilities related maintenance and building systems for the Kearny Mesa office and surrounding landscape.

THE POSITION:

The candidate selected for this position will be responsible for developing, maintaining, optimizing, enhancing, and administering the Water Authority's cybersecurity systems; systems and tools may include items such as firewalls, intrusion detection/prevention systems, security event identification management systems, data loss prevention systems, anti-virus/anti-malware systems, application whitelisting systems, multi-factor authentication systems, web application proxies, web filters, vulnerability scanning/analysis tools, mobile device management systems and application/operating system patching tools; system/application log review and reports; user and computer account reviews and reports.

The job duties include, but are not limited to the following:

- Reviews, analyzes, alerts and reports on system logs and events; adjusts logging source and systems to better understand the true state of events, maintains current knowledge of the latest threats and understands how to spot them.
- Enumerates systems vulnerabilities through the regular applications of vulnerability scanning and system configuration review; maintains current best practices for the secure

configuration of servers, workstations, routers, switches, firewalls and other network-based systems.

- Provides regular security reports for management and staff; maintains trend data to enhance situational awareness; conducts regular presentations.
- Conducts formal end user awareness training sessions to improve user line of defense; administers web-based awareness training; conducts anti-phishing program.
- Works with support staff to ensure best practice configuration practices are applied; ensures that current systems documentation is always available; coordinate systems patching schedules.
- Provides daily emerging threats briefings for management and stays current with vendor updates.
- Provides project management for security initiatives; tracks budget, time, schedule and resource use for mid to large size initiatives.
- Administers change management program to ensure maximum system availability and stakeholder involvement; communicates planned and unplanned service changes to all users; coordinates with all technical stakeholders to improve results.
- Conducts regular status checks of all equipment and services; reports loss or degradation of services or systems; confirms that all logging sources are present and producing expected logging.
- Conducts process reviews and provides improvement reporting; applies critical analysis to add or improve security levels of technical and business processes; produces new processes where necessary to enhance overall security posture of the organization.

For further details regarding the duties and responsibilities, and qualification guidelines for this class specification, please click on the following link: [Information Systems Analyst](#)

QUALIFICATION GUIDELINES:

The qualification guidelines generally describe the knowledge and ability required to enter the job in order to successfully perform the assigned duties. Any combination of experience and training that would provide the required knowledge, skills, and abilities will be considered.

Graduation from a college or university with a major in computer science, geography, mathematics or a closely related field; and three years of progressively responsible experience in information systems or an equivalent combination of training and experience.

APPLICATION PROCEDURE:

To be considered for this position, please submit an employment application and supplemental questionnaire by **5:30 p.m. Friday, February 8, 2018**. Resumes will not be accepted in lieu of a completed application and supplemental questionnaire. All applications and supplemental questionnaires will be evaluated in relation to the criteria outlined in this job announcement. The selection process may consist of an appraisal interview, selection test, and/or other appropriate screening methods.

All applications and supplemental questionnaires will be evaluated in relation to the criteria outlined in this job announcement. The selection process may consist of an appraisal interview, writing exercise, and/or other appropriate screening devices.

To ensure timely and successful navigation, please consider applying early if you are new to the [governmentjobs.com](#) application system. For technical assistance with the online application system, please review the Government Jobs [online application guide](#), or contact their toll-free applicant support line at (855) 524-5627. If you have questions regarding the position, please contact Corinne Russell, Human Resources Analyst, at (858) 522-6663.

APPLICATIONS MAY BE FILED ONLINE AT:
<http://agency.governmentjobs.com/sdcwa/default.cfm>
OUR OFFICE IS LOCATED AT:
4677 Overland Avenue
San Diego, CA 92123
858-522-6660
hr@sdca.org

Job #18-17
INFORMATION SYSTEMS ANALYST (CYBER SECURITY)
CR

An Equal Opportunity Employer

Information Systems Analyst (Cyber Security) Supplemental Questionnaire

- * 1. Each applicant must complete this supplemental questionnaire as part of the application screening and selection process. The information you provide will be reviewed and used to determine your eligibility to move forward in the selection process. Incomplete responses, false statements, omissions, or partial information may result in disqualification from the selection process. Do you agree to answer each supplemental question truthfully and that your responses can be verified from information included within the application?
- Yes No
- * 2. Do you possess a valid driver's license (equivalent to California Class A, B, or C)?
- Yes No
- * 3. I have graduated from a four-year college or university with major course work in the following:
- Computer Science
 Geography
 Mathematics
 Other / Closely Related Field (Please describe in #4)
 Do Not Possess 4-Year Degree
- * 4. If you indicated "Other / Closely Related Field," for Question #3, please list your relevant education. Please type "N/A" in the box if this question does not apply.
- * 5. Do you possess at least three years of progressively responsible experience in cyber security or an equivalent combination of training and experience?
- Yes No
- * 6. How many years of professional cyber security experience do you possess?
- No Experience
 Less than 1 Year
 1 - 2 Years
 2 - 3 Years
 3 - 4 Years
 4 - 5 Years
 5 - 6 Years
 6 or more Years
- * 7. Do you have experience with any of the following technologies (Check all that apply):
- Firewalls
 Intrusion Detection/Prevention Systems
 Anti-Virus/Anti-Malware
 Data Loss Prevention Systems
 Web Proxy/Filtering Systems
 Application Whitelisting
 Computer Forensics
 Mobile Device Management Systems
 Vulnerability Scanning
 Incident Handling
 SIEM Security Information and Event Management Systems
 Virtualization
 None of the Above

- * 8. Please describe your experience with at least six (6) of the above listed technologies. If you have experience with fewer than six (6) of the technologies listed above, list the ones you have experience with. Please include the name of the employer, your title, and describe your level of proficiency with each technology. If you have no experience in these areas, please type "N/A."

- * 9. Please check all of the certifications that you possess from the list below:
 - Certified Information System Manager
 - Certified Information Systems Auditor
 - Certified Ethical Hacker
 - Offensive Security Certified Professional
 - Global Information Assurance Certifications
 - Other/Closely Related Certifications (Please describe in #10)
 - None of the Above

- * 10. Please list any additional certifications you possess that were not checked in supplemental question #9 above. If you have no additional certifications to add, please type "N/A" in the box below.

- * 11. Do you possess a current Certified Information Systems Security professional (CISSP) certification?
 - Yes No

- * 12. I have read the job description and reviewed the salary range for this position.
 - Yes No

- * 13. **APPLICANT'S ACKNOWLEDGMENT - NOTIFICATION VIA ELECTRONIC MAIL (E-MAIL)** The San Diego County Water Authority Human Resources Division uses e-mail to notify applicants of important information relating to the status and processing of your application. We do so as part of our ongoing efforts to increase operational efficiency, promote the conservation of resources, and minimize delays and costs. Therefore, as an applicant, please ensure that the e-mail address and contact information you provide are current, secure, and readily accessible to you. Do not share e-mail addresses. Spam or other filters should be adjusted to accept our e-mails. **We will not be responsible in any way if you do not receive our e-mails** (i.e., for the non-delivery of e-mail or if you fail to check your e-mail inbox on a timely basis). Read any notices that we send carefully and in a timely manner. Follow further instructions, if any. We recommend that you print and keep hard copies of our notices for your records. **I acknowledge that I have read, understand, and agree to the above.**
 - Yes No

* Required Question