CHRIS CHRISTIE
GOVERNOR

KIM GUADAGNO
LT. GOVERNOR

State of New Jersey

Office of Homeland Security and Preparedness
PO Box 091
TRENTON, NJ 08625-0091

CHRIS RODRIGUEZ
DIRECTOR

NOTICE OF JOB VACANCY

POSTING NUMBER: # 16-13 Statewide **Pages: 3**

An opportunity currently exists in the Office of Homeland Security and Preparedness (NJOHSP) within the *unclassified service* for applicants who meet the minimum job requirements specified below:

TITLE: **Cybersecurity Analyst (Administrative Analyst 3, Information Systems)**

NUMBER OF POSITIONS: **Two (2)**

ISSUE DATE: **September 27, 2016**

CLOSING DATE: **October 12, 2016**

SALARY: **$64,677.09 - $92,011.89**

LOCATION: **Hamilton, New Jersey**

JOB DESCRIPTION: As a member of the Division of Cybersecurity within the New Jersey Office of Homeland Security and Preparedness the Cybersecurity Analyst plays a vital role in protecting the State of New Jersey's information assets by proactively identifying risks and implementing appropriate controls in accordance with the State's cybersecurity program.

Duties include but not limited to:

- Develop and implement information security policies and standards in accordance with the State's goals and objectives and in compliance with regulatory and statutory requirements including PCI-DSS, HIPAA, IRS-1075, etc.
- Monitor, analyze, manage and report on security risks, threats and vulnerabilities
- Coordinate, lead or participate in penetration tests, vulnerability scans and other risk assessments as necessary to protect the State of NJ's information assets
- Perform information security risk assessments on new products and systems; periodic information security risk assessments of existing systems; and information security risk assessments of third-party vendors
- Monitor compliance with information security policies and directives
- Manage and drive remediation efforts related to information security - remediation may be from incidents, penetration tests, vulnerability scans, internal/external audits, or other assessments
- Investigate potential security incidents using forensically sound methods and techniques
- Participate in the continued development and implementation of the State's information security awareness program
- Assist with the development and implementation of information security metrics, measurement criteria and reporting to ensure compliance and continuous improvement

- Provide information security technology expertise/consultation as requested.
- Perform other cybersecurity duties as required.

MINIMUM REQUIREMENTS:

Education: Graduation from an accredited college or university with a Bachelor's degree.

Experience: Three (3) years of experience in work involving the review, analysis and evaluation of the administrative, business, and/or operational policies, procedures, practices, and processes and/or technological requirements of an organization for the purpose of revising/enhancing existing information systems and/or developing/acquiring and implementing new IT solutions and services.

Substitution: Applicants who do not possess the required education may substitute additional experience as indicated on a year for year basis with thirty (30) semester hour credits being equal to one (1) year of experience. A Master's degree in Public Administration, Business Administration, Computer Science, Information Technology, Software Engineering, Information Security, Network Administration, or Database Management from an accredited college or university may be substituted for one (1) year of the indicated experience.

Note: Preference will be given to candidates with the following knowledge and experience:

- Demonstrable network, system and application security experience
- Strong knowledge of information systems security standards and practices (e.g., access control, system hardening, system audit and log file monitoring, security policies, and incident handling)
- Excellent understanding of TCP/IP and network communications
- Proven knowledge of network and server infrastructure technologies and devices including firewalls, routers, switches, etc.
- Demonstrable knowledge and experience with SIEM, IPS/IDS, VPN, Vulnerability Scanner, Active Directory, Malware Analysis, Penetration Testing, UNIX/Linux, Incident Response, Firewalls and APT Methodologies;
- Functional knowledge and experience with text and data representation and manipulation (XML, HTML, Regular Expressions, Scripting, SQL)
- Experience working as a member of an information security incident response team, conducting computer forensics analyses and performing investigative duties related to security policy violations
- Demonstratable knowledge of regulatory compliance requirements including PCI-DSS, HIPAA, IRS-1075, etc.
- Strong problem solving and analytical skills
- Strong written and verbal communication skills
- Proficiency in Microsoft software: Outlook, Word, Excel, PowerPoint, and Visio
- Ability to quickly understand security systems in order to identify and validate security requirements
- Ability to manage multiple projects, priorities and deadlines
- Demonstrated initiative, customer orientation and team work competencies
- Adaptability, flexibility and ability to work as part of a team or in an individual capacity
- Must demonstrate effective, decision making, results delivery, and the ability to stay current with relevant technologies and security practices.
- Willingness to work outside of regular business hours as required which can include evenings, weekends and holidays

- Ability to handle and maintain the integrity and confidentiality of highly sensitive material and information

Note: Preferred certifications: CISSP, CRISC, CISA, CEH, Security+

License: Appointee will be required to possess a driver's license valid in New Jersey only if the operation of a vehicle, rather than employee mobility, is necessary to perform essential duties of the position.

Interested applicants should send a cover letter, resume and writing sample to: Roopa Trotter, Chief, Human Resources, Office of Homeland Security and Preparedness, PO Box 091, Trenton, NJ 08625 by mail or by email to careers@njohsp.gov. (**Please reference the posting number in subject line of the email.**) All submissions must be received no later than close of business on **October 12, 2016.**

Applicants should be aware that all NJOHSP employees must be a U. S. Citizen due to the fact that they need to be eligible to obtain a Secret or Top Secret Clearance from the federal government. U. S. Citizenship is a requirement for obtaining such clearance. Additionally, a criminal background investigation is conducted on all NJOHSP personnel.

In accordance with the New Jersey First Act P.L. 2011 c70, effective September 1, 2011, new public employees are required to obtain New Jersey residency within one (1) year of employment.

This office is committed to the principles and practices of Equal Employment Opportunities and Affirmative Action and the Americans with Disabilities Act.

Roopa Trotter
Chief, Human Resources