



CHRIS CHRISTIE
GOVERNOR

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

CHRIS RODRIGUEZ
DIRECTOR

KIM GUADAGNO
LT. GOVERNOR

NOTICE OF JOB VACANCY

Posting Number: # 16-07 IWS

An opportunity currently exists in the Office of Homeland Security and Preparedness (OHSP) within the *unclassified service* for a candidate who meets the minimum job requirements specified below:

TITLE: Director of Cybersecurity (State Chief Information Security Officer), (Division Director)

NUMBER OF POSITIONS: One (1)

SALARY: \$130,000

LOCATION: Hamilton, New Jersey

JOB DESCRIPTION: The New Jersey Office of Homeland Security and Preparedness (OHSP) is seeking a full-time employee to serve as OHSP's Director of Cybersecurity and the State Chief Information Security Officer (CISO). Under the general direction of the Director of OHSP and in coordination with the Chief Technology Officer of the Office of Information Technology (OIT), the Director of Cybersecurity is the recognized State expert and authority on policies, procedures, guidance and technologies impacting the cybersecurity of the Executive Branch. The State CISO establishes the direction of Executive Branch's cybersecurity policy and strategy, to include management practices, budget priorities, and for overseeing implementation across the entire government. The State CISO functions collaboratively with OIT and Agency leaders, staff, and other stakeholders who are responsible for cybersecurity.

Duties include but not limited to:

- Overseeing and providing guidance to the bureaus reporting to the Division of Cybersecurity – NJ Cybersecurity and Communications Integration Cell (NJCCIC), Cyber Operations and Cyber Policy and Compliance.
- Advising the Homeland Security Advisor, Chief Technology Officer, and other agency officials on information security policy, governance, and compliance across Executive Branch information technology systems.
- Providing oversight of relevant agency cybersecurity practices, and implementation across Executive Branch information technology systems in accordance with relevant State and Federal policies and standards.
- Serving as the State Government's lead in the ongoing assessment of cybersecurity risks to the Executive Branch's IT environment. To the greatest extent possible, use widely accepted frameworks (for example, NIST, ISO 2700m COBIT) and stay current on market trends, industry practices, and current and emerging products and capabilities in order to assess risk, identify vulnerabilities, prioritize threats, secure investment, and measure and communicate progress.

- Serving as the liaison between the State and the Federal Government, private sector, other states, and Agency Information Security Officers (ISO) for all cybersecurity activities.
- Providing input into the development of the Governor's annual budget proposal so that it reflects cybersecurity priorities across Executive Branch departments and agencies, and ensure coordination and integration with the overall State IT budget process.
- Ensuring effective coordination and alignment among agency ISOs through the exercise of effective governance, for example, while serving as the Chair of the Enterprise Cyber Risk Management Committee, or through engagement with other committees as appropriate.
- Sponsoring and overseeing implementation of statewide cybersecurity role-based and awareness training, and agency alignment with cybersecurity best practices.
- Establishing a government-wide program, in coordination with the appropriate State agencies to address the recruitment, retention, and training of cybersecurity experts, with a particular focus on not just technical experts, but also versatile professionals who can effectively facilitate between IT and the mission and business functions.
- Designing, implementing, and maintaining effective cybersecurity performance measures for the Executive Branch, and ensuring that agency reviews are conducted in accordance with established policies, standards, and regulations.

MINIMUM REQUIREMENTS:

Education: Bachelor's degree and 7 years of progressive experience in information technology, including 5 years of information security or information assurance experience, with at least 3 years in an information technology management position.

Note: Applicants who do not possess the required education may substitute appropriate information security or information assurance experience indicated above on a year-for-year basis.

Note: Preference will be given to candidates having Professional certifications such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA) and/ or an educational background in information management or computer science.

Experience: Demonstrated experience in working with executives and managers on the identification of large enterprise business requirements; understanding cyber threat activities and methodologies; and establishing risk-based cyber security policies, strategies, and measures to address current and emerging cyber threats.

Senior level experience in successfully implementing cybersecurity policies, strategies, procedures, and guidelines that address the full lifecycle of information technology services development and delivery, in large enterprises, to include requirements for integrating security requirements into provisioned services agreements and other contractual arrangements.

Demonstrated technical expertise in understanding complex, interconnected, modern web and other current technology platforms/system architectures, software development practices, and cybersecurity solutions; securing enterprise IT architectures, networks, systems, data, and applications, to include mobile and customer facing applications; and leading responses to large-scale cyber incidents.

Notice of Job Vacancy
Posting # 16-07 IWS
Director of Cybersecurity

Senior level experience in presenting issues and recommendations through top-quality clear and concise written and oral communication to senior organization officials.

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 letter (including posting number) and resume to Roopa Trotter, Chief, Human Resources, Office of Homeland Security and Preparedness, PO Box 091, Trenton, NJ 08625 (or 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 **July 22, 2016.**

Applicants should be aware that all OHSP 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 OHSP 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