



DHS/OIT – Chief Information Security Officer – (Fulton County) 00180935

**Job Number:
00180935**

Job Posting: January 9, 2017

Closing Date: January 31, 2017

Primary Location: 2 Peachtree St., Atlanta, GA (Fulton County)

Number of Openings: 1

Job: Office of Information Technology

Shift: Day Job

SALARY: Pay Grade: P

Salary Range: \$66,822 - \$95,459.43

(Salary Commensurate with Experience)

Current Georgia state government employees will be subject to State Personnel Board rule provisions.

The Georgia Department of Human Services (DHS) delivers a wide range of human services designed to promote self-sufficiency and well-being for all Georgians. The department is one of the largest agencies in state government with an annual budget of \$1.8 billion and nearly 9,000 employees. DHS is comprised of three Divisions: the Division of Aging Services, the Division of Child Support Services, and the Division of Family and Children Services.

The Office of Information Technology (OIT) supports the Department with applications management, IT procurement, network and telecommunications services.

OIT is seeking a **Chief Information Security Officer (CISO)**. This position is based at 2 Peachtree Street, NW, Atlanta, GA in Fulton County. The Chief Information Security Officer (CISO) will report to the Chief Information Officer (CIO).

Job Summary & Responsibilities:

Under limited supervision, the **Chief Information Security Officer** will:

- Direct a team of information security and cyber engineers, managing associated budgets, and understands financial performance of the budgets to include

forecasts, actuals, key risk indicators, and monthly variances to those plans as well as provides information security leadership to our enterprise infrastructure and application service organizations.

- Responsible for managing an enterprise-wide information security management program to ensure all agency information system resources are adequately protected by applying the required controls to enhance their availability, integrity and confidentiality.
- Build effective working relationships with service providers; external and internal business partners to ensure practices are aligned with the risk appetite.
- Meet defined policies and standards for information security and risk management.
- Oversee a variety of IT-related risk management activities.
- Serve as the process owner of all compliance activities, security awareness training, agency's information security policies and procedures.
- Collaborate with other executive managers to determine acceptable levels of risk for the organization.
- Establish the information security and risk management strategy, manage, and oversee a comprehensive enterprise information security and IT risk management program to ensure improvement of the integrity, confidentiality and availability of information system resources framework based on the following: National Institute of Standards and Technology (NIST) Cyber security Framework and ISO-27K standards as well as state of Georgia security policies and guidelines.
- Monitor the use of sensitive agency data files and regulates access to safeguard data and information in computer files. Manages and responds to all aspects of federal and state Information Technology (IT) audits for DHS. Report directly to the CIO and work closely with the CIO leadership team, including the Office of General Counsel to address any agency IT Security, Privacy and Audit concerns.
- Develop, maintain and publish information security policies, standards and guidelines. Oversee the approval, training, and dissemination of security policies and practices.
- Create and manage information security and risk management awareness training programs for all employees, contractors and approved system users.
- Must keep abreast with the ever-changing information security regulations requirements and ensure that security programs are in compliance with applicable federal laws, regulations and policies to minimize or eliminate risk and audit findings.
- Work directly with the service providers, external partners and business areas throughout the agency to facilitate and address IT risk assessment and risk management processes throughout the enterprise / agency on identifying acceptable levels of residual risk.
- Responsible for improving the information security risk posture of the agency by identifying, evaluating and mitigating information security risks to acceptable levels and also meets all applicable regulatory requirements.

Core Competencies:

- Must possess strong business acumen, inspire and foster team communication and trust.
- Must be a thought leader, a consensus builder, and an integrator of people and processes.
- Must demonstrate a high level of interpersonal skills to handle sensitive and confidential situations.
- Business leader and able to be capable of aligning the information security and risk strategy to the business objectives and goals.

Benefits:

In addition to a competitive salary, DHS offers a generous benefits package, which includes employee retirement plan; paid holidays annually; vacation and sick leave; health, dental, vision, legal, disability, accidental death and dismemberment, health and child care spending account. Visit: <http://team.georgia.gov/> for more information.

GEORGIA ON MY MIND: *It Doesn't Get Any Better Than This!*

Georgians enjoy a quality of life that would be hard to find in any area across the nation. Lower taxes and a lower cost of living enable you to do more with money you make and maintain a higher standard of living.

Within Georgia you will find an unlimited supply of recreational and cultural opportunities. Enjoy boating, camping, fishing, golf, hiking, picnicking, swimming, tennis or just relaxing against Georgia many scenic backdrops. Georgia is a 57,906 square-mile playground filled with natural beauty and immaculate resources. From the mountains to the coast from ballet to baseball, Georgia offers you a livable and quality of life that can help you achieve your dreams.

You are really going to like Metro Atlanta!

As the capital of Georgia, metro Atlanta, the ninth largest US population center has approximately 5.3 million residents. It is uniquely positioned to provide the best of everything. From its diverse economy, global access, abundant talent, and low costs of business and lifestyle, metro Atlanta is a great place to call "home." Residents have easy access to arts, culture, sports, world class shopping and nightlife. Atlantans experience all four seasons, with mild winters that rarely require a snow shovel. Yes, Atlanta is a great place to work and live!!! www.metroatlantachamber.com

Criminal Background Checks/Applicant Privacy Rights

All applicants may be subject to a drug screen and will be required to submit fingerprints to check for the existence of criminal history information through the Georgia Bureau of Investigation and the Federal Bureau of Investigation. Applicants have the right to challenge the contents of any criminal history record obtained for the purpose of

employment with DHS. For an explanation of these rights, please read, "Applicant Privacy Rights" at:

http://gbi.georgia.gov/sites/gbi.georgia.gov/files/related_files/document/ApplicantPrivacyRights.pdf

Due to the volume of applications received, we are unable to provide information on application status by phone or e-mail. All qualified applicants will be considered, but may not necessarily receive an interview. Selected applicants will be contacted by the hiring agency for next steps in the selection process. Applicants who are not selected will not receive notification. Former DHS employees must be eligible for rehire in order to be considered for the position.

This position is subject to close at any time once a satisfactory applicant pool has been identified.

Qualifications:

Bachelor's degree from an accredited college or university AND Five years in the specific field of IT Security, Two years of which include management experience.

Preferred Qualifications:

Preference will be given to candidates who, in addition to meeting the minimum qualifications, demonstrate some or all of the following skills/experience:

- Master's degree from an accredited college or university in information technology, computer science, information assurance or a related IT field.
- 10+ years of proven experience and demonstrated success in information security leadership.
- CISSP/CISM Certification; CISA certification a plus.
- Demonstrate knowledge of network, operating system, database, and application security.
- Experience implementing and complying with Federal and State laws.
- Experience with Cloud-based solutions and environments.
- Demonstrate knowledge of current and emerging (NextGen) information security technologies and practices.