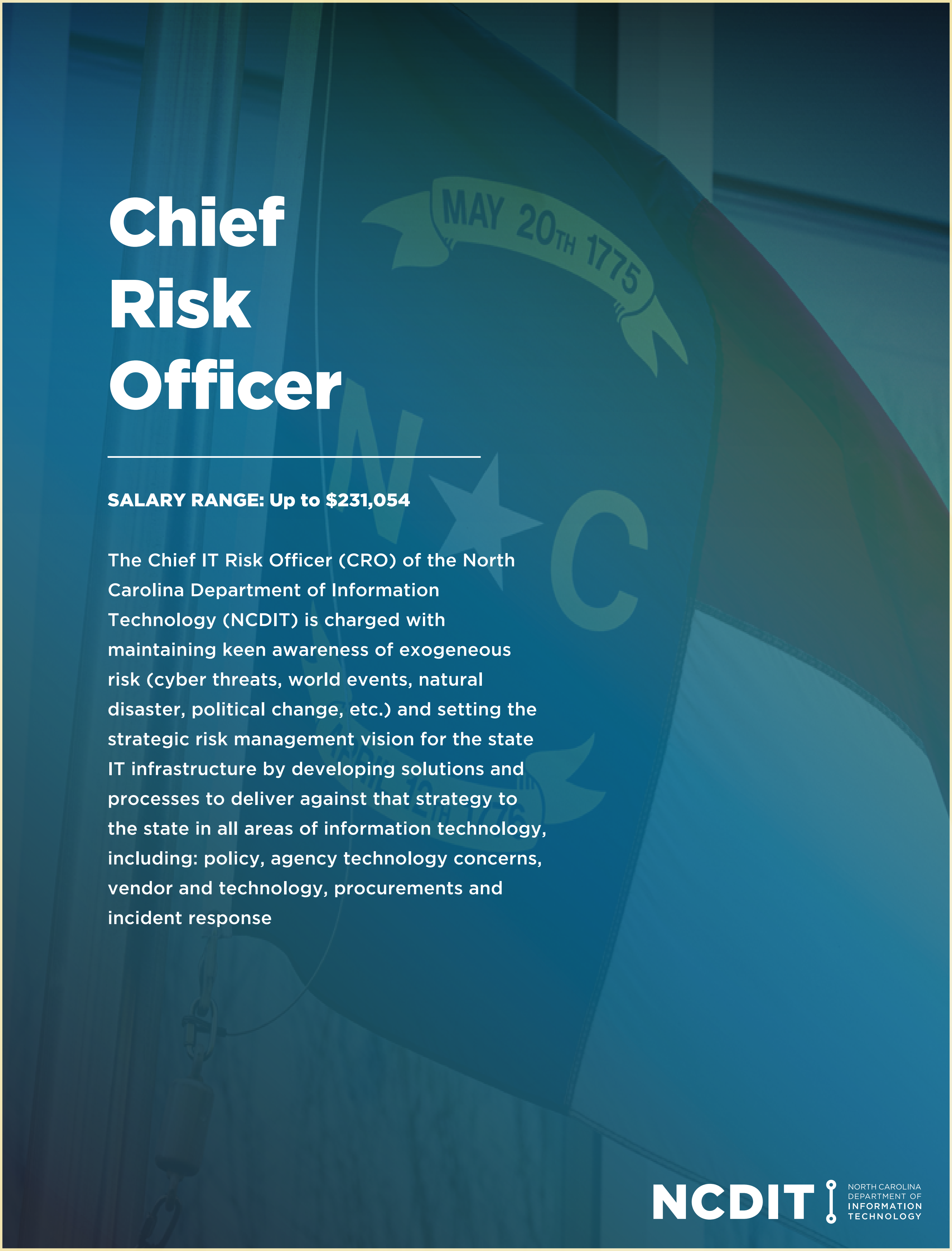

Chief Risk Officer

SALARY RANGE: Up to $231,054

The Chief IT Risk Officer (CRO) of the North Carolina Department of Information Technology (NCDIT) is charged with maintaining keen awareness of exogeneous risk (cyber threats, world events, natural disaster, political change, etc.) and setting the strategic risk management vision for the state IT infrastructure by developing solutions and processes to deliver against that strategy to the state in all areas of information technology, including: policy, agency technology concerns, vendor and technology, procurements and incident response

NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

AGENCY

NCDIT oversees and is the primary IT service provider to state agencies, local governments and educational institutions across North Carolina. The department was established as a cabinet-level agency in 2015 to consolidate enterprise information technology functions within the executive branch to meet the needs of residents, businesses and visitors while also realizing efficiencies and cost savings through economies of scale. The list of consolidated, or optimized, agencies is below.

The department's primary functions are statewide strategy, governance, architecture and operations. A full list of the powers and duties of the department can be found in General Statute Chapter 143B, Article 15.

The State Chief Information Officer (SCIO) - also referred to as the Secretary of the department – leads the department and its 1,300 employees. The SCIO is appointed by the Governor.

The department is dedicated to transforming the state's shared IT services by adopting modern technology solutions and improving communications and collaboration platforms to meet our customers' needs, while effectively managing risks and security.

ARCHITECTURE AND DESIGN

NCDIT ensures that solutions, either to be built or procured, align with the state's and agencies' goals to support digital transformation, IT growth and modernization. The department works to proactively identify and implement new solutions based on identified gaps to reduce redundancy of solutions, optimize costs and mitigate risks. In addition, NCDIT works with agencies to apply existing, new and emerging technologies to transform and optimize business and operating models, helping agencies plan, design, innovate, orchestrate, facilitate, navigate and operationalize the digital enterprise.

BROADBAND AND DIGITAL EQUITY

NCDIT serves as a statewide resource for broadband access, digital inclusion and digital literacy initiatives that the state leads. To elevate Gov. Cooper's priority to close the digital divide in North Carolina, the Office of Digital Equity and Literacy was established in 2021 as the first office of its kind in the nation. NCDIT is working to deliver digital equity to North Carolina by leveraging data to identify and understand community needs, expanding broadband access, increasing digital literacy and enabling more North Carolinians to afford high-speed internet.

DATA

NCDIT provides the infrastructure to host state projects, services, data, and applications. The department also manages and coordinates enterprise data integration efforts through the Government Data Analytics Center (GDAC). Currently, GDAC integrates data and develops analytics to support business needs associated with criminal justice, child safety, fraud, compliance, health care and longitudinal and performance analysis.

OPERATIONS AND ENGINEERING

With a few legislative exceptions, NCDIT provides all IT support for consolidated, or optimized, agencies. The department also partners with other state agencies, local governments and education entities to provide reliable, cost-effective services that meet current and future requirements, service levels and budgets, centralizing services, as necessary, for ease of use and security as well as optimizing cost and efficiencies across all services.

SECURITY AND RISK MANAGEMENT

NCDIT provides leadership in the development, delivery and maintenance of a whole-of-state cybersecurity program that safeguards North Carolina's information and supporting infrastructure against unauthorized use, disclosure, modification, damage or loss. The department coordinates with the N.C. Department of Public Safety to manage statewide response to cybersecurity incidents and significant cybersecurity incidents. In addition, the department helps executive branch agencies comply with legal and regulatory requirements as well as technical architecture and industry best practices.

STATEWIDE IT PROCUREMENT

NCDIT is responsible for procuring IT goods and services for optimized agencies and approving IT procurements for separate agencies to ensure they meet current technology standards, are not duplicative, meet business objectives, are cost-effective, and are adequately funded. The department establishes processes, specifications and standards for IT products and services that are purchased, licensed or leased by state agencies and educational entities.

STRATEGY AND GOVERNANCE

NCDIT is responsible for working with state agencies to develop and administer a comprehensive strategic plan to ensure the proper management of the state's information technology resources. This plan is used to create and maintain a strategically aligned portfolio of IT services and solutions that meets the state's business needs and effectively leverages state resources to service residents, businesses and visitors.

In addition, the department is responsible for establishing a consistent process for planning, maintaining, and acquiring the state's information technology resources, and ensuring that state programs and projects align with policies, standards and architecture.

CULTURAL DIVERSITY

NCDIT is an equal opportunity employer and committed to diversity, equity and inclusion. We are an Employment First state ensuring that people with disabilities have equal opportunity to succeed in the state government workplace (Executive Order 92).

Governor Cooper has in recent years signed additional executive orders to address pay equity for women (Executive Order 93) and establish paid parental leave (Executive Order 95) for birth, adoption, or foster care.

VISION

Government that strategically leverages technology for an equitable, prosperous, healthier and educated North Carolina.

MISSION

Enable trusted business-driven solutions that meet the needs of North Carolinians.

GUIDING PRINCIPLES

- Accountability
- Agility
- Collaboration
- Creativity & Innovation
- Customer Focused
- Integrity
- Transparency

ABOUT THE POSITION

SALARY RANGE: Up to $231,054

The Chief IT Risk Officer (CRO) of the North Carolina Department of Information Technology (NCDIT) is charged with maintaining keen awareness of exogenous risk (cyber threats, world events, natural disaster, political change, etc.) and setting the strategic risk management vision for the state IT infrastructure by developing solutions and processes to deliver against that strategy to the state in all areas of information technology, including: policy, agency technology concerns, vendor and technology, procurements and incident response.

The CRO and staff must respond to ever changing risks and threats due to the pace of technology innovation and exogenous threat agents. The CRO is tasked with developing and executing an integrated approach to risk management and advising state agencies and NCDIT business units. The CRO interfaces with agency secretaries, CIOs, and CISOs to address all areas of statewide IT risk, participates in gubernatorial-level staff meetings in areas of risk management or emergency response, and works with national, state and federal officials to pre-plan responses to incidents.

The CRO is based in Raleigh, but a hybrid remote work arrangement is possible. This position is designated as Exempt Policymaking and is appointed by the Governor.

PRIMARY RESPONSIBILITIES

- Coordinates with federal, state and local entities in North Carolina on a proactive cybersecurity posture that includes identifying and responding to cybersecurity risks
- Work with local, state and federal entities to create a cybersecurity and data protection plan and integrated strategies around risk identification, mitigation and elimination to position the state to protect the public and state from known or unknown threats
- Assures statewide IT security compliance and ensures resolution of IT security incidents
- Monitors compliance with cybersecurity and data protection standards
- Identifies internal and external risks while creating a plan and process to respond to outside or unforeseen circumstances
- Develops and issues an annual state agency information technology and data security scorecard and assures that cited deficiencies are resolved as quickly as possible
- Works closely with all NCDIT (and agency) executive leadership to identify and analyze emerging trends that may impact or present new risk to the state's information technology security so that policies, procedures, plans and strategies are revised accordingly
- Ensures risk and security incidents are handled promptly and root causes are reported to all necessary stakeholders and operation for resolution

KNOWLEDGE, SKILLS & ABILITIES

- Thorough knowledge of risk management in the areas of data center operations, information technology, cybersecurity, data protection/management, exogenous factors, incident response and disaster recovery
- Considerable experience with strategic planning to create cybersecurity and data risk strategies and standards
- Exceptional management skills, including the ability to effectively deploy resources and manage multiple projects with a various scopes in a cross-functional environment
- Experience with creating policies and/or programs across multiple areas of risk
- Demonstrated ability to lead and effectively work within a team by using interpersonal skills and the ability to communicate with employees, senior management and stakeholders
- Excellent oral and written communication and ability to present and discuss technical information in a manner that can be understood by non-subject matter experts
- Demonstrated ability to interpret laws, regulations, and statutes across all areas of risk
- Leadership experience with task forces, committees and cross-functional or matrixed teams

MINIMUM EDUCATION & EXPERIENCE

- Bachelor's degree in computer science or an IT related field or related degree from an appropriately accredited institution and eight years of progressive experience in the field of information technology including at least four years of management experience related to IT security
OR
- Associate degree in computer science or an IT related field or related degree from an appropriately accredited institution and ten years of progressive experience in the field of information technology including at least four years management experience related to IT security
OR
- An equivalent combination of education and experience

MANAGEMENT PREFERENCES

- At least ten years of progressive information technology risk management experience, including at least six years of managerial experience in information technology
- Relevant cybersecurity certifications and security clearance(s)

IN 2021-2022, THE ENTERPRISE SECURITY AND RISK MANAGEMENT OFFICE:

1,205

Investigations supported that involved compromised email accounts.

4,363

Investigations involving security alerts received and triaged them through the state Security Operations Center

Application process

Hiring is to be as early as January 30th, 2023, and no later than March 13th, 2023.

To be considered, please either send a CV or resume and cover letter to the Executive Recruiter listed below or apply to the posting on https://www.governmentjobs.com/careers/northcarolina

Applicants deemed to have the most relevant demonstrated experience will be contacted for further interview and selection.

For additional information or questions contact Executive Recruiter Anchal Mishra at anchal.mishra@nc.gov.

COMPENSATION AND BENEFITS

The state of North Carolina offers excellent comprehensive benefits. Employees can participate in health insurance options, standard and supplemental retirement plans, and the NCFlex program (numerous high-quality, low-cost benefits on a pre-tax basis).

Employees also receive paid vacation, sick, and community service leave. In addition, paid parental leave is available to eligible employees.

Some highlights include:

- The best funded pension plan/retirement system in the nation according to Moody's Investor's Service
- Twelve (12) holidays/year
- Fourteen (14) vacation days/year which increase as length of service increases and accumulate year-to-year
- Twelve (12) sick days/year which are cumulative indefinitely
- Longevity pay – lump sum payout yearly based on length of service
- 401K, 457, and 403(b) plans

Learn more about employee perks/benefits:

- Why Work For NC?
- NC OSHR: Benefits
- NC OSHR: Total Compensation Calculator

it.nc.gov

NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY