2026 NASCIO NOMINATION

Cybersecurity

North Carolina's Cybersecurity Strategic Plan

Initiated: March 2025
Completed: June 2025

Agency: N.C. Department of Information Technology

Contact: Nate Denny, NCDIT Secretary and State Chief Information Officer
natedenny@nc.gov

NCDIT | NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

EXECUTIVE SUMMARY

The State of North Carolina's 2025–2030 Cybersecurity Strategic Plan represents the most comprehensive modernization of statewide cyber governance, risk management, and resilience in the state's history. In response to escalating cyber threats against state agencies, local governments, and educational institutions, the plan establishes a unified enterprise approach that integrates statewide policy, technology, workforce development, and governance. Developed by the N.C. Department of Information Technology (NCDIT), the plan moves North Carolina from a decentralized, compliance-oriented model toward a holistic, risk-informed, and whole-of-state cybersecurity framework.
The plan organizes North Carolina's cybersecurity future around six strategic pillars:

- Threat surface management
- Statewide CISO accountability
- Governance
- Education
- Resilience
- Workforce development

Each pillar includes measurable objectives and enterprise-level actions that enable shared visibility, common standards, and unified risk reduction across state agencies and broader public-sector partners. The plan aligns and elevates cybersecurity efforts across state government, counties, municipalities, universities, community colleges, and K–12 school districts. It establishes new enterprise governance structures, strengthens statewide leadership accountability, expands workforce development programs, and delivers shared cybersecurity services that raise baseline maturity for all public entities. As a result, North Carolina is shifting from reactive cybersecurity practices to a coordinated, proactive enterprise strategy that improves statewide readiness, reduces systemic risk, and protects North Carolinians.

IDEA

Recognizing the Need for Enterprise Cyber Reform

North Carolina's public-sector ecosystem is large, distributed, and technologically diverse. Rapid modernization, hybrid work expansion, cloud adoption, and the interconnectedness of government services are creating a dramatically expanding attack surface. At the same time, cyber incidents — including ransomware and extortion attacks — are impacting counties, school districts, and state agencies with increasing frequency and severity. On their own, many public-sector organizations lack the resources or workforce to sustain dedicated cybersecurity programs, leading to inconsistent controls and uneven security maturity.

North Carolina's State Chief Information Security Officer has identified several enterprise-level challenges that demand a unified statewide strategy. Among them are limited statewide visibility into vulnerabilities and risk, fragmented governance structures, inconsistent security leadership roles, workforce shortages, and an underutilized education and training ecosystem. Without a cohesive framework, public-sector entities would often be left to defend themselves independently against rapidly evolving cyber threats.

Developing a Whole-of-State Cyber Vision

The Cybersecurity Strategic Plan provides a comprehensive blueprint for addressing these challenges. The vision for a more secure North Carolina centers on unified governance, shared enterprise services, coordinated risk management, statewide workforce development, and sustained resilience. Unlike previous approaches focused narrowly on compliance, this plan establishes cybersecurity as an enterprise business function and a shared responsibility across all levels of government.

The plan emphasizes the importance of collaboration with public-sector partners, community colleges, universities, and private-sector organizations. It also underscores the necessity of consistent statewide cybersecurity standards, risk reporting processes, and shared service models that improve protection across the entire public ecosystem. By transitioning to an enterprise-level strategy, North Carolina ensures that residents' data and public services are protected regardless of which agency or government entity collects or manages the information.

IMPLEMENTATION

After joining NCDIT in March 2025, State Chief Information Security Officer Bernice Russell-Bond initiated development of the cybersecurity strategic plan as one of the goals for her first 100 days in the role and ensured that it was completed by the end of the fiscal year on June 30, 2025. Following its completion, the plan was presented to the North Carolina Information Technology Strategy Board for review and approval and was then submitted to NCDIT's Secretary for final endorsement.

The plan was structured using a template developed for previous strategic documents while also incorporating elements from other state cybersecurity strategic plans. This approach ensured consistency and alignment with established best practices across the sector.

Implementation of the plan encompasses several key activities aligned with the state's cybersecurity vision and goals.

Building Enterprise Governance

NCDIT has strengthened statewide governance by establishing a statewide structure led by the State Chief Information Security Officer with clear authority to define standards, set policy direction, and provide accountable leadership. A formalized Cyber Subcommittee, created within the state's Information Technology Strategy Board, brings together security leaders from across state government, local government, education, and private industry. This governance structure ensures consistent prioritization, oversight, and communication across all cybersecurity initiatives.

Developing a Statewide Risk and Threat Surface Model

The plan introduces an enterprise approach to identifying, quantifying, and prioritizing cyber risks. This includes standardized methods for reporting vulnerabilities, understanding statewide exposure, and ensuring that remediation efforts align with the most critical risks. This model enables coordinated decision-making and helps leaders use shared data to guide investments.

Expanding Workforce Pathways and Partnerships

To address persistent talent shortages, North Carolina has strengthened partnerships with the Carolina Cyber Network, community colleges, and universities. These collaborations support internships, apprenticeships, entry-level training, and professional development opportunities for government cybersecurity professionals. These dedicated pipelines help ensure long-term sustainability and workforce readiness.

Rolling Out Shared Enterprise Cyber Services

Several enterprise security services have been expanded or initiated under this strategy, including centralized monitoring, statewide incident response capabilities, vulnerability management platforms, identity modernization efforts, and resilience exercises. These services provide consistent protection across agencies while reducing duplication of resources and enabling smaller organizations to access capabilities they could not support individually.

IMPACT

Establishing Statewide Cyber Governance

The plan's most significant achievement is the establishment of a robust, enterprise-wide governance framework that brings consistency, accountability, and transparency to cybersecurity across North Carolina's public sector. Agencies, counties, municipalities, and educational institutions now share common standards, expectations, and decision-making structures. This unified approach improves communication, facilitates collaboration, and reduces the fragmentation that often undermines cybersecurity efforts in decentralized environments.

Statewide CISO Accountability

By elevating the role of the State Chief Information Security Officer and establishing clear statewide accountability, North Carolina has created a governance model in which agency security leaders align their efforts with enterprise priorities. This ensures consistent implementation of policies, improves the quality of incident reporting, strengthens enforcement of statewide standards, and accelerates alignment with national best practices. The shift to enterprise accountability significantly reduces systemic risk and improves the state's ability to prepare for and respond to cyber threats.

Transition from Compliance to Risk-Based Management

The Cybersecurity Strategic Plan fundamentally changes how cybersecurity decisions are made across North Carolina's public sector. Agencies have moved from compliance-focused checklists to a risk-based approach grounded in threat intelligence, vulnerability data, and enterprise-level analysis. This transition has led to more efficient use of resources, more effective security investments, and a stronger statewide cybersecurity posture. Agencies can now prioritize remediation efforts based on shared data that identifies the highest risks to statewide operations.

Improved Resilience and Incident Preparedness

Resilience is one of the plan's core pillars. The plan drives improvements to incident response capabilities, enterprise recovery standards, and statewide resilience exercises. Enhanced coordination among agencies and local government partners reduces response time and improves the ability to contain and mitigate cyber incidents. These initiatives ensure continuity of public services, minimize disruption, and reduce long-term impacts on residents.

Strengthening Local Government and Education Security

One of the most important impacts of the plan is its benefit to counties, municipalities, K–12 school districts, community colleges, and universities. Many of these organizations face resource constraints and struggle to sustain robust cybersecurity programs. Through statewide guidance, shared resources, and enterprise cyber services, North Carolina is raising the cybersecurity baseline for every public-sector organization in the state. This whole-of-state model ensures that residents receive consistent protection regardless of where they live or interact with government services.

Workforce Development Gains

Cyber workforce shortages remain one of the greatest risks to public-sector cybersecurity. The Cybersecurity Strategic Plan directly addresses this through expanded partnerships with the Carolina Cyber Network, community colleges, and universities. Internship and apprenticeship programs are preparing students for entry-level roles, while expanded professional development opportunities are improving retention among current cybersecurity professionals. These workforce initiatives are essential to building a sustainable, long-term cybersecurity talent pipeline.

Increased Public Trust

Improved cybersecurity protections directly enhance public trust in state government. Residents rely on secure and reliable public services, and the Cybersecurity Strategic Plan ensures that the systems they depend on are defended against evolving threats. By safeguarding resident data and improving service continuity, North Carolina strengthens confidence in digital government services.

National Leadership and Model for Other States

North Carolina's whole-of-state cybersecurity model is gaining national attention as states look for effective strategies to protect diverse, distributed public-sector ecosystems. The enterprise governance structure, shared services approach, and statewide workforce development programs offer a scalable template for other states seeking to strengthen cybersecurity without increasing complexity or duplication.

North Carolina's 2025–2030 Cybersecurity Strategic Plan marks a transformational shift toward a unified, enterprise-wide approach to protecting the state's public-sector ecosystem now and into the future. By replacing fragmented, compliance-based practices with coordinated risk management, statewide governance, and shared services, the plan strengthens cybersecurity readiness across agencies, local governments, and educational institutions. Through its six strategic pillars, the state has established clear leadership structures, modernized security capabilities, and built sustainable workforce pathways. These efforts not only improve resilience and reduce systemic risk but also elevate public trust and position North Carolina as a national leader in whole-of-state cybersecurity.

Supplemental Link

State of North Carolina Cybersecurity Strategic Plan: State of North Carolina Cybersecurity Strategic Plan 2025-2030