



# State of North Carolina

**ROY COOPER**  
GOVERNOR

**March 16, 2022**

**EXECUTIVE ORDER NO. 254**

## **ESTABLISHMENT OF THE NORTH CAROLINA JOINT CYBERSECURITY TASK FORCE**

**WHEREAS**, cybersecurity threats are increasing in volume and sophistication, requiring a need to understand the threat landscape to prevent attacks and to protect the State's information technology networks and critical infrastructure from acts of terrorism and criminal, organized-crime or gang activity; and

**WHEREAS**, geopolitical events like Russia's recent unlawful invasion of Ukraine can lead to an increase in cybersecurity threats and attacks; and

**WHEREAS**, cybersecurity breaches have the potential to impact the delivery of essential public services and private services to the people of North Carolina, threaten the confidentiality, integrity and availability of state data, and can cause loss of reputation and significant economic disruption and harm; and

**WHEREAS**, the State must identify, protect against, and respond to cyberattacks aimed at causing privacy violations, identity theft, and disruption of business continuity; and

**WHEREAS**, state agencies, local governments, tribal governments, the private sector, academic institutions, federal agencies and other state entities must mitigate cyber risks through information sharing, monitoring, forensics and incident response to protect public security and individuals' data; and

**WHEREAS**, in order to prepare for and combat against these public security threats, the North Carolina Department of Information Technology/Enterprise Security and Risk Management Office, the North Carolina Division of Emergency Management, the North Carolina National Guard, and the North Carolina Local Government Information Systems Association Cybersecurity Strike Team have created a Joint Cybersecurity Task Force ("Task Force"); and

**WHEREAS**, the Task Force provides crucial services to North Carolina in preventing and responding to cybersecurity breaches and attacks, including increased cybersecurity threats arising from Russia's recent unlawful invasion of Ukraine; and

**WHEREAS**, the cybersecurity of North Carolina's critical infrastructure will be enhanced through greater interaction and communication between the Task Force and public and private stakeholders to identify and respond to cybersecurity threats; and

**WHEREAS**, there are sixteen Critical Infrastructure Sectors as defined by Presidential Policy Directive ("PPD-21") whose assets, systems, and networks, whether physical or virtual, are vital to the State of North Carolina and their incapacitation or destruction would have a debilitating effect on security, economic security, public health or safety, or any combination thereof; and

**WHEREAS**, there are a wide variety of Critical Infrastructure Sector facilities in North Carolina, some of which are open to the public or contain highly sensitive business functions, that

include cyber elements such as, general-use office buildings, military installations, courthouses, state laboratories, and others that may contain critical equipment, systems, networks, and functions essential to the State of North Carolina; and

**WHEREAS**, Critical Infrastructure and Key Resources (“CIKR”) across the United States are under constant threat of malicious activity by individual threat actors, such as terrorists, cyber-criminal gangs, and other malicious actors; and

**WHEREAS**, the “Whole-of-State” approach to cybersecurity adopted by the Task Force is a proven and effective strategy that prioritizes the protection of CIKR; and

**WHEREAS**, to best mitigate against risk, North Carolina needs to have an accurate understanding of CIKR entities across the state and the status of their cybersecurity programs; and

**WHEREAS**, there is a need for CIKR entities to coordinate and report significant cybersecurity incidents to remediate and address root causes of a significant cybersecurity incident during the recovery from an event; and

#### Statutory Authority and Determinations

**WHEREAS**, pursuant to Article III of the North Carolina Constitution and N.C. Gen. Stat. §§ 143A-4 and 143B-4, the Governor is the chief executive officer of the state and is responsible for formulating and administering the policies of the executive branch of state government; and

**WHEREAS**, pursuant to N.C. Gen. Stat. § 147-12, the Governor has the authority and the duty to supervise the official conduct of all executive and ministerial officers; and

**WHEREAS**, pursuant to N.C. Gen. Stat. § 166A-19.12(23), the North Carolina Division of Emergency Management (“NCEM”), the State Chief Information Officer (“State CIO”) of the North Carolina Department of Information Technology (“NCDIT”) and the Adjutant General of the North Carolina National Guard (“NCNG”) coordinate to manage the statewide response to cybersecurity incidents and significant cybersecurity incidents as defined in N.C. Gen. Stat. § 143B-1320 and that purview includes, but is not limited to, the classification and handling of restricted or highly restricted data through the Statewide Data Classification and Handling Policy, the development and promulgation of necessary policies, plans, and procedures for cybersecurity and critical infrastructure protection, and annual review, update, and testing of cybersecurity incident response plans and procedures; and

**WHEREAS**, pursuant to N.C. Gen. Stat. § 143B-1321(a)(5) NCDIT must plan and coordinate information technology efforts with state agencies, nonprofits, and private organizations as required; and

**WHEREAS**, pursuant to N.C. Gen. Stat. §§ 143B-1322(c)(5) and (11), the State CIO must ensure the security of state information technology systems and networks, as well as associated data, must develop standardized systems and processes, and is responsible for managing and protecting the State’s data; and

**WHEREAS**, pursuant to N.C. Gen. Stat. § 143B-1376, the State CIO shall be responsible for the security and privacy of all state information technology systems and associated data; and

**WHEREAS**, pursuant to N.C. Gen. Stat. § 143B-1376, the State CIO shall manage all executive branch information technology security and shall establish a statewide standard for information technology security and privacy to maximize the functionality, security, and interoperability of the State’s distributed information technology assets, including, but not limited to, data classification and management, communications, and encryption technologies.

**NOW, THEREFORE**, by the power vested in me as Governor by the Constitution and laws of the State of North Carolina, **IT IS ORDERED:**

#### **Section 1. Establishment of the Joint Cybersecurity Task Force**

The State of North Carolina Joint Cybersecurity Task Force is hereby established.

- a. Members from the following entities comprise the Task Force:
  1. The North Carolina Department of Information Technology/Enterprise Security and Risk Management Office.
  2. The North Carolina Division of Emergency Management.

3. The North Carolina National Guard.
  4. The North Carolina Local Government Information Systems Association Cybersecurity Strike Team.
- b. A member from each of the following agencies is invited to participate in the Task Force:
1. The North Carolina Information Sharing and Analysis Center.
  2. The Federal Bureau of Investigation.
  3. The United States Secret Service.
  4. Other federal agencies, North Carolina state agencies, or other stakeholders on an as-needed basis and upon invitation from the Task Force.

## **Section 2. Partnering to Protect North Carolina Critical Infrastructure and Key Resources**

1. North Carolina public and private sector CIKR entities are strongly encouraged to report public-facing internet protocol addresses to the Task Force in order for the Task Force to assist those entities in identifying and responding to cybersecurity vulnerabilities.
2. North Carolina public and private sector CIKR entities are strongly encouraged to report significant cybersecurity incidents to the Task Force to mitigate the cascading impacts from a cybersecurity incident.
3. North Carolina public and private sector CIKR entities are strongly encouraged to coordinate significant cybersecurity incident response and recovery efforts with the Task Force.

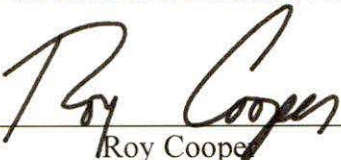
## **Section 3. No Private Right of Action**

This Executive Order is not intended to create, and does not create, any individual right, privilege or benefit, whether substantive or procedural, enforceable at law or in equity by any party against the State of North Carolina, its agencies, departments, political subdivisions, or other entities, or any officers, employees, or agents thereof.

## **Section 4. Effective Date and Duration**

This Executive Order is effective immediately. It shall remain in effect until rescinded, provided, however, that the Joint Cybersecurity Task Force may continue to operate upon expiration or repeal of this Executive Order.

**IN WITNESS WHEREOF**, I have hereunto signed my name and affixed the Great Seal of the State of North Carolina at the Capitol in the City of Raleigh, this 16<sup>th</sup> day of March, in the year of our Lord two thousand twenty-two.

  
\_\_\_\_\_  
Roy Cooper  
Governor

**ATTEST:**

  
\_\_\_\_\_  
Elaine F. Marshall  
Secretary of State

