HOUSE BILL 813
Committee Substitute Favorable 5/12/21

Short Title: Prohibit State Agencies Payment of Ransomware. (Public)

Sponsors:

Referred to:

May 5, 2021

A BILL TO BE ENTITLED

AN ACT TO PROHIBIT ANY STATE AGENCY, UNIT OF LOCAL GOVERNMENT, OR PUBLIC AUTHORITY FROM PAYING A RANSOM IN CONNECTION WITH A CYBERSECURITY INCIDENT AND TO CLARIFY THE REPORTING OF CYBERSECURITY INCIDENTS TO THE DEPARTMENT OF INFORMATION TECHNOLOGY.

The General Assembly of North Carolina enacts:

SECTION 1. Chapter 143 of the General Statutes is amended by adding a new Article to read:

"Article 84.

"Various Technology Regulations.

"**§ 143-800. State entities and ransomware payments.**

(a) No State agency or local government entity shall submit payment or otherwise communicate with an entity that has engaged in a cybersecurity incident on an information technology system by encrypting data and then subsequently offering to decrypt that data in exchange for a ransom payment.

(b) Any State agency or local government entity experiencing a ransom request in connection with a cybersecurity incident shall consult with the Department of Information Technology in accordance with G.S. 143B-1379.

(c) The following definitions apply in this section:

(1) Local government entity. – A local political subdivision of the State, including, but not limited to, a city, a county, a local school administrative unit as defined in G.S. 115C-5, or a community college.

(2) State agency. – Any agency, department, institution, board, commission, committee, division, bureau, officer, official, or other entity of the executive, judicial, or legislative branches of State government. The term includes The University of North Carolina and any other entity for which the State has oversight responsibility."

SECTION 2.(a) G.S. 143B-1320 reads as rewritten:

"**§ 143B-1320. Definitions; scope; exemptions.**

(a) Definitions. – The following definitions apply in this Article:

…

(4a) Cybersecurity incident. – An occurrence that:

a. Actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or

b. Constitutes a violation or imminent threat of violation of law, security policies, privacy policies, security procedures, or acceptable use policies.

…

(14a) Ransomware attack. – A cybersecurity incident where a malicious actor introduces software into an information system that encrypts data and renders the systems that rely on that data unusable, followed by a demand for a ransom payment in exchange for decryption of the affected data.

…

(16a) Significant cybersecurity incident. – A cybersecurity incident that is likely to result in demonstrable harm to the State's security interests, economy, critical infrastructure, or to the public confidence, civil liberties, or public health and safety of the residents of North Carolina. A significant cybersecurity incident is determined by the following factors:

a. Incidents that meet thresholds identified by the Department jointly with the Department of Public Safety that involve information:

1. That is not releasable to the public and that is restricted or highly restricted according to Statewide Data Classification and Handling Policy; or

2. That involves the exfiltration, modification, deletion, or unauthorized access, or lack of availability to information or systems within certain parameters to include (i) a specific threshold of number of records or users affected as defined in G.S. 75-65 or (ii) any additional data types with required security controls.

b. Incidents that involve information that is not recoverable or cannot be recovered within defined time lines required to meet operational commitments defined jointly by the State agency and the Department or can be recovered only through additional measures and has a high or medium functional impact to the mission of an agency.

…."

SECTION 2.(b) G.S. 143B-1379(c) reads as rewritten:

"(c) ~~County and municipal government agencies~~ Local government entities, as defined in G.S. 143-800(c)(1), shall report cybersecurity incidents to the Department. Information shared as part of this process will be protected from public disclosure under G.S. 132-6.1(c). Private sector entities are encouraged to report cybersecurity incidents to the Department."

SECTION 2.(c) G.S. 143B-1322(c) reads as rewritten:

"(c) Administration. – The Department shall be managed under the administration of the State CIO. The State CIO shall have the following powers and duty to do all of the following:

…

(22) Coordinate with the Department of Public Safety to manage statewide response to cybersecurity ~~incidents and~~ incidents, significant cybersecurity ~~incidents~~ incidents, and ransomware attacks as defined by G.S. 143B-1320."

SECTION 3. This act is effective when it becomes law.