**§ 143B-1379. State agency cooperation and training; liaisons; county and municipal government reporting.**

(a) The head of each principal department and Council of State agency shall cooperate with the State CIO in the discharge of the State CIO's duties by providing the following information to the Department:

(1) The full details of the State agency's information technology and operational requirements and of all the agency's significant cybersecurity incidents within 24 hours of confirmation.

(2) Comprehensive information concerning the information technology security employed to protect the agency's data, including documentation and reporting of remedial or corrective action plans to address any deficiencies in the information security policies, procedures, and practices of the State agency.

(3) A forecast of the parameters of the agency's projected future cybersecurity and privacy needs and capabilities.

(4) Designating an agency liaison in the information technology area to coordinate with the State CIO. The liaison shall be subject to a criminal background report from the State Repository of Criminal Histories, which shall be provided by the State Bureau of Investigation upon its receiving fingerprints from the liaison. Military personnel with a valid secret security clearance or a favorable Tier 3 security clearance investigation are exempt from this requirement. If the liaison has been a resident of this State for less than five years, the background report shall include a review of criminal information from both the State and National Repositories of Criminal Histories. The criminal background report shall be provided to the State CIO and the head of the agency. In addition, all personnel in the Office of the State Auditor who are responsible for information technology security reviews shall be subject to a criminal background report from the State Repository of Criminal Histories, which shall be provided by the State Bureau of Investigation upon receiving fingerprints from the personnel designated by the State Auditor. For designated personnel who have been residents of this State for less than five years, the background report shall include a review of criminal information from both the State and National Repositories of Criminal Histories. The criminal background reports shall be provided to the State Auditor. Criminal histories provided pursuant to this subdivision are not public records under Chapter 132 of the General Statutes.

(5) Completing mandatory annual security awareness training and reporting compliance for all personnel, including contractors and other users of State information technology systems.

(b) The information provided by State agencies to the State CIO under this section is protected from public disclosure pursuant to G.S. 132-6.1(c).

(c) County and municipal government agencies 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. (2015-241, s. 7A.2(b); 2019-200, s. 6(e).)