

April 5, 2001

S 1096. SECURITY STANDARDS FOR STATE IT. PROVIDING FOR THE ADOPTION OF ENTERPRISE-WIDE SECURITY AND ENCRYPTION STANDARDS FOR STATE GOVERNMENT INFORMATION TECHNOLOGY. Adds new GS 147-33.89 to require State Chief Information Officer (CIO) to establish an enterprise-wide set of standards for information security and to review existing standards and practices to determine whether they meet security and encryption requirements. Sets out process for adopting, reporting on, and revising standards. Adds new GS 147-33.89 requiring every information technology security feature purchased with state funds or for use in a state agency or facility to be subject to approval by CIO in accordance with state standards. Allows exemption for CIO's approval (1) if legislative or judicial branch develops security standards that exceed CIO's standards, legislative branch and judicial branch may choose to be governed by their own standards or (2) if Governor certifies that a state agency has developed standards that exceed CIO's standards, then agency may chose to be governed by its own standards. Allows CIO to assume responsibility of providing for information technology security for any state agency that fails to follow standards adopted under act. Requires head of each state agency to cooperate with CIO as CIO carries out responsibilities. Applies to every state agency (as defined in act), Judicial Department, General Assembly, The University of North Carolina and its constituent institutions. Amends GS 147-64.6(c) to add investigation of reported information technology breaches, cyber attacks, and cyber fraud in state government to list of State Auditor's duties.

Intro. by Reeves.

Ref. to Information Tech.	GS 147
---------------------------	--------