NEW YORK STATE SENATOR

Jack M. Martins

Senator Martins Announces Senate Passage of Legislation Targeting Cyber Terrorism

JACK M. MARTINS March 5, 2015

ISSUE: TERRORISM

Bills Focus on Enforcing Stricter Penalties and Create Cyber Security Measures To Protect New York From Future Threats

Senator Jack M. Martins (R-7th Senate District) announced that the New York State Senate recently passed legislation to crack down on cyber terrorism and its rapidly expanding threat to the state's security and finances. The legislation, which Senator Martins cosponsored, would enact tougher penalties for cyber-related crimes, create cyber security

programs to identify potential risks and threats, and require the state to perform a comprehensive review of all its cyber security measures every five years.

"In the digital age, where our society is more dependent than ever on computers, cyber security has never been more important. Enhancing security to protect the state's vital cyber infrastructure and residents' private information, along with tougher penalties for cyber crimes, are critical and necessary steps. Just as technology continues to evolve, so too must our laws to ensure that our residents are protected," said Senator Martins.

The bills passed by the Senate would:

• Establish the New York State Cyber Security Initiative to ensure that the state has a proper cyber security defense system in place (S3407). It includes:

o The New York State Cyber Security Sharing and Threat Prevention Program to increase the state's quality and readiness of cyber threat information that will be shared with the public and private sectors;

o A New York State Cyber Security Critical Infrastructure Risk Assessment Report to seek recommendations from experts to identify security threats facing the state, its businesses, and its citizens, as well as develop effective ways to combat these security threats; and

o The New York State Cyber Security Advisory Board, which assists the state in making recommendations and finding ways to protect its critical infrastructure and information systems, being codified into law.

• Create new penalties for cyber crimes. Under the measure, it would be a Class A felony for any person found guilty of intimidating, coercing, or affecting the public or a government

entity by causing mass injury, damage, or debilitation of people or their property, including computers and related programs, data networks, or material. A new Class C felony would include anyone who uses a computer to cause serious financial harm affecting more than 10 people (S3404).

• Make it a Class B felony for those who use a computer or device to carry out a cyber attack when such an attack causes financial harm in excess of $100,000 to another person, partnership, or corporation, individually or collectively (S3406).

• Require the Division of Homeland Security and Emergency Services to work with the Superintendent of State Police, the Chief Information Officer, and the President of the Center for Internet Security to complete a comprehensive review of New York's cyber security measures every five years, and create a sequential report to summarize its findings. The report would identify the state's security needs and detail how those needs are being met to ensure that the best security practices are in place to protect New Yorkers from cyber terrorism (S3405).

The legislation has been sent to the Assembly.