State of South Carolina
Office of the Inspector General

December 3, 2012

Honorable Nikki R. Haley
Governor of South Carolina
1205 Pendleton Street
Columbia, SC 29201

Re: State Government Information Security Initiative

Dear Governor Haley,

Enclosed with this letter is the Office of the Inspector General's interim report on the State Government Information Security Initiative titled, "Current Situation & A Way Forward."

South Carolina statewide government has a less than adequate information security (INFOSEC) posture. Currently, there are no statewide INFOSEC standards or policies. By default, each agency decides its own risk tolerance for data loss and its own INFOSEC plan. This decentralized approach undermines an effective statewide security posture, as well as creates unmanaged and uncontrolled statewide INFOSEC risks having a potential impact on the entire state government.

This less than adequate statewide INFOSEC assessment is based on data collected from 18 state agency Chief Information Officers, the Division of State Information Technology, and experts in the private and public sectors. The data was consistent and compelling. Given the state's low risk tolerance for absorbing another significant data loss, the current level of statewide INFOSEC risk is not acceptable. Further, regardless of the assessment of statewide risk, the current decentralized INFOSEC environment provides no visibility of INFOSEC risks within agencies, which is incompatible with state government's due diligence responsibility to do everything possible to protect citizens' information.

The data for a way forward was equally consistent and compelling. The direction, to meet the goal of doing everything possible to protect citizens' information, starts with establishing a statewide INFOSEC program led by a statewide Chief Information Security Officer. Moving from a decentralized environment to a statewide model is a common challenge for states, and there are ample consultants with the expertise and experience to assist the state in this effort. It will require developing a statewide governance mechanism with authority to establish statewide solutions and a standard policy framework for all agencies. This standard policy framework can then be delegated, in most areas, to agencies to tailor statewide policies to their operational environment, yet still be subject to oversight and audit.

OFFICE OF THE INSPECTOR GENERAL • KINGSTREE BUILDING • 110 CENTERVIEW DRIVE, SUITE 201 • COLUMBIA, SOUTH CAROLINA 29210
OFFICE: 803.896.4729 • FAX: 803.896.4309 • EMAIL: OIG@OIG.SC.OIG • TOLL-FREE HOTLINE: 1.855.SCFRAUD (1.855.723.7283)

While the state deliberates on a way forward, to include this report's recommendation for a statewide program for long-term INFOSEC health, state agencies are still conducting INFOSEC activities every day. Every agency CIO fully understands the duty to protect information and implement INFOSEC protective measures. Since the recent breach, agencies have created a more proactive posture to aggressively identify and address risks. These agencies just need the leadership and support from a statewide INFOSEC program to systematically improve their capabilities to the security threshold to meet our goal---to do everything possible to protect our citizens' information.

The next interim report will focus on implementation options and recommendations, in terms of cost and schedule, to develop a long term sustainable statewide INFOSEC program to reduce agency and statewide risk.

If you or your staff needs any additional information, please do not hesitate to call me.

Sincerely,

Patrick J. Maley
Inspector General

cc: Glenn McConnell, Lieutenant Governor,
John E. Courson, President Pro Tempore
Hugh Leatherman, Senator
Robert W. Harrell, Jr., House Speaker
Brian White, Representative