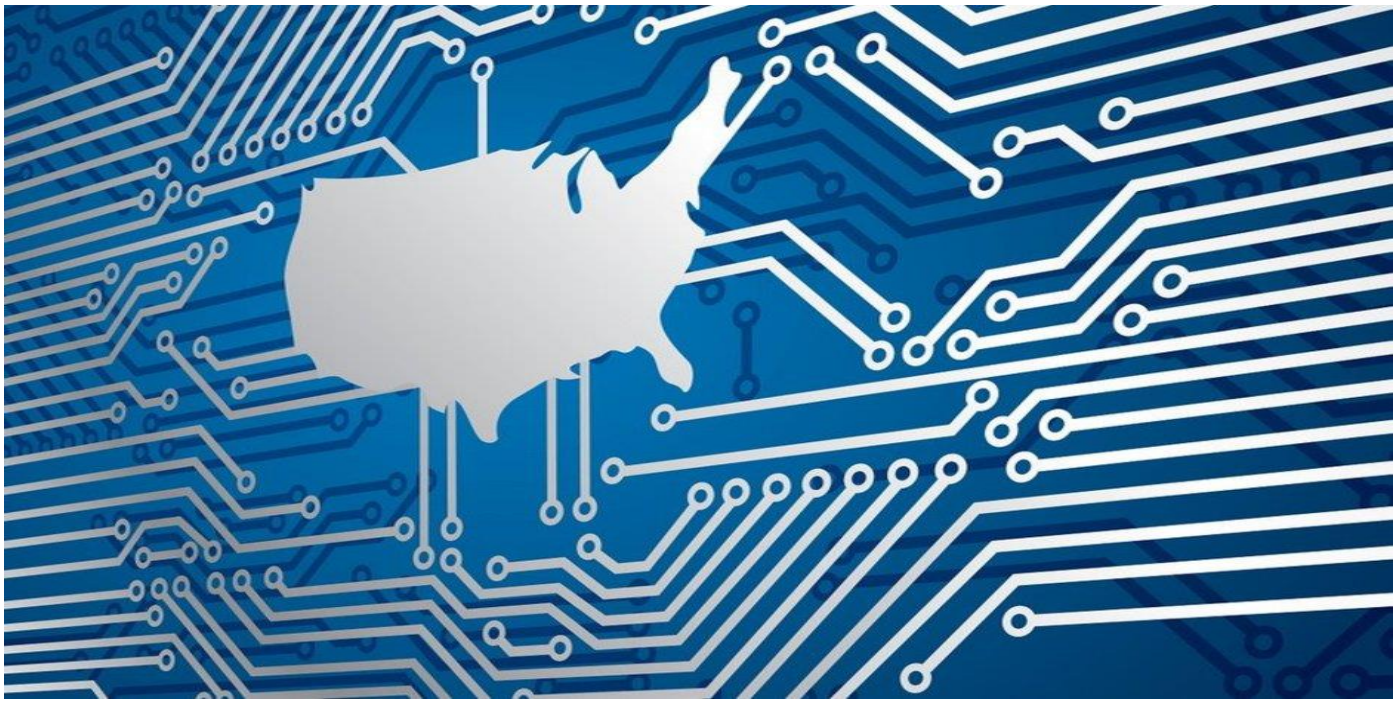
WHITE PAPER #3



WHY SHOULD EVERY STATE GOVERNMENT HAVE AN IT SECURITY POLICY FOR STATE AGENCIES & OFFICES UNDER THE STATE'S EXECUTIVE BRANCH?

DeBora King

CSIA 360 7980

Cybersecurity in Government Organizations (2172)

April 23, 2017

University of Maryland University College – Spring Semester, 2017

INTRODUCTION

The Tenth Amendment of the U.S. Constitution states that "all powers not granted to the federal government are reserved for the states and the people" (Whitehouse.gov., n.d.). Although not required by the Constitution, state governments mirror the structure of the federal government in that they have an executive, legislative, and judicial branch. So, it is fitting that agencies such as local law enforcement, public schools and the office of motor vehicles (all of which encompass extremely sensitive and personal identifiable information) fall under the umbrella of state government. The elected governor of each state heads the executive branch. The lieutenant governor, attorney general, secretary of state, auditors and commissioners are also elected officials servicing states. Each state is mandated by the U.S. Constitution to uphold a "republican form" of government, but they are given the freedom to organize their structure as they see fit (Whitehouse.gov. n.d.). Hence, like fingerprints, no two state executive organizations re exactly alike. Most states have IT Security policies governed by their executive branch. This policy is designed to outline how the government will protect the data of its citizens. It may also include information about training and how security is enforced to protect data and plans to mitigate against security breaches including cybercrime and malicious activity.

In 2014, the State and Local Government Cybersecurity Framework Kickoff Event was hosted by the National Cybersecurity Center of Excellence (NCCoE) and the National Institute of Standards and Technology (NIST) as a part of the White House initiative to promote Obama's Executive Order (EO 13636) on Improving Critical Infrastructure Cybersecurity (Daniel, 2014). This forum follows the premise to implement this executive order promoting collaboration between state, local, tribal, and territorial governments. This is especially important because local entities are often the first line of defense in the event of a cybercrime or threat.

To answer the question addition, "why should every state in the nation have a comprehensive IT security policy for state agencies and offices?" The answer is to provide uniformity of information, interaction, and implementation of IT cybersecurity policy plans whether independent of state government economic stature or population size.

For the purposes of this white paper, the states of North Carolina and Georgia will be examined in comparison and contrast to support why every state government should have an IT security policy for state agencies and offices under the state's executive branch.

COMMON PRINCIPLES & POLICY STATEMENTS BETWEEN NC & GA

In this section, both state IT Security Policies will be examined between North Carolina and Georgia. Outlined below are five commonalities between the two policies:

1. Some citizens do not know an IT Security Policy entails. Both state documents do a good job in providing an overview of their policies and both outline their standards and resources.
2. The Chief Information Officer (CIO) holds authority in both state documents. In both cases, the CIO has authorization to adopt and approve amendments to policy standards.
3. Both documents have a section outlining a glossary of information technology terms. While NC has a more detailed link, Georgia Technology Authority (GTA) incorporates terms into its IT Security Policy document.
4. Employees and contractors are mentioned in both policies, as training and the importance in the expectations of the positions they hold.
5. The documents both mention the importance of confidentiality and integrity.

ASPECTS OF NORTH CAROLINA'S IT SECURITY POLICY

North Carolina has a link to its Statewide Security Information Security Manual. The manual outlines the following features:

- Classifying data and legal requirements
- Securing the end user
- Securing the network
- Securing systems
- Physical security
- Cyber incident response
- Business continuity and risk management

Some of the unique aspects of North Carolina's IT Security policy is that it has a links to the following important information:

- An extensive glossary of terms.
- Statewide acceptable use policy.
- Data classification and handling policy which outlines how data is safeguarded, data and system classifications and roles and responsibilities.
- Instructions for Corrective Action Plan (CAP).
- Configurations in securing multifunctional devices MFDs
- How cloud storage is implemented

ASPECTS OF GEORGIA'S IT SECURITY POLICY

Georgia has a great introductory identification portion of its IT Security policy. The top of the page gives the document type, title, issue date, person to contact for changes and a synopsis of the policy. The document outlines the following:

- Purpose
- Scope
- Policy
- Technology Security Authority
- Enforcement
- Expectations

The document often references its Official Code of Georgia Annotated (OCGA) which is what GTA is governed by. Some great references this document refers to are ISO 27000, Federal Information Security Management Act (FISMA of 2002, and supporting NIST documentation. It also refers to the State Department of Audits and Accounts (DOAA) and it talks about how the Office of Information Security (OIS) reviews policies.

In addition to state requirements, the GTA also emphases compliance requirements for the following federal policies for citizenship protection:

- Health Insurance Probability & Accountability Act (HIPPA)
- The Family Educational Rights and Privacy Act (FERPA)
- Children's Online Privacy Protection Act (COPPA)
- Gramm-Leach-Bliley Act (GLBA)

EVALUATION OF NC & GA IT SECURITY POLICIES/ BEST PRACTICE RECOMMENDATIONS

The IT Alliance for Public Sector produced a document that recommends best practices for state governments. The table below lists some of these findings along with how each state government document measures up to its IT Security Policies.

WHY SHOULD EVERY STATE GOVERNMENT HAVE A COMPREHENSIVE IT SECURITY POLICY?

IT Alliance Recommendation	Examination of NC IT Security Policy	Examination of GA IT Security Policy
Adopt Industry-Recognized Security Standards	**CON:** Although links and resources are clearly outlined in detail, industry-recognized security standards are not evident when reviewing the initial documentation of the NC IT Security Policy.	**PRO:** The GA IT Security Policy references framework by the Federal Information Security Management Act (FISMA), the National Institute of Standards (particularly ISO 27000). It also has a link for an Introduction to Computer Security (NIST Pub 8--=12).
Standardize Cloud Security	**PRO:** The NC IT Security Policy has a link to its Secure Cloud Storage, File Sharing and Collaboration documentation.	**CON:** The GA NC IT Security policy is a very generalized document. It fails to mention specific policy implementations, such as how standardized cloud security will be used to mitigate against threats.
Create a Culture of Awareness	**CON**: The NC IT Security Policy document has a broken link to their Annual Security Training for Department IT Employees and Contractors.	**PRO:** The GA IT Security Policy addresses the importance of employee awareness in its purpose section.

CONCLUSION

With the exception of the broken link, North Carolina's IT Security Policy provided a more informative documentation of how the state protects its citizen's information. In researching the policy, one can clearly find anything from looking up the definition of a particular word or finding a specific link to a policy affiliated to the overall standards. The GTA IT Security Policy was very general, provided only two links (one referring to an exemption request and the other to an NIST publication). These links were fine, but it would have been good practice to have the ability to delve more into the specifics of how data is collected, handled, stored, and maintained. The documentation defining Confidentiality, Integrity, Availability, Information Security Infrastructure and Due Diligence/Due Care are great guides, but the U.S. C. policy sections do not provide detailed explanations like the North Carolina policy. When state government entities are more uniform in implementing IT policies from its executive branch, there is a better chance of nations building a better universal, centralized, streamlined network to champion cybersecurity and protect citizen data.

References:

The White House. (n.d.). State & Local Government. Powers not granted the federal government are reserved for states and the people, which are divided between state and local governments. Retrieved from https://www.whitehouse.gov/1600/state-and-local-government

Daniel, M. (2014, April 2). State and local government cybersecurity. The White House. Retrieved from https://obamawhitehouse.archives.gov/blog/2014/04/02/state-and-local-government-cybersecurity

NC Information Technology. (n.d.). Policies. Retrieved from https://it.nc.gov/statewide-resources/policies

Georgia Technology Authority. (2008, March 20). Enterprise Information Security Charter. Retrieved from http://gta.georgia.gov/sites/gta.georgia.gov/files/imported/vgn/images/portal/cit_1210/0/26/99359541Enterprise%20Information%20Security%20Charter%20PS-08-005.01.pdf

Crawford, L. (n.d.). State cybersecurity principles & best practices. IT Alliance for Public Sector. Retrieved from https://www.itic.org/dotAsset/6b96ecc0-53d8-4068-b2a5-4fd79676c9ed.pdf