



**GEORGIA STATE SENATE**  
**SENATE RESEARCH OFFICE**

204 Coverdell Legislative Office Building | 404.656.0015  
18 Capitol Square SW  
Atlanta, GA 30334

ANGIE FIESE, DIRECTOR

ALEX AZARIAN, DEPUTY DIRECTOR

ELIZABETH HOLCOMB, PROJECTS MANAGER

---

**THE FINAL REPORT OF THE  
SENATE STUDY COMMITTEE ON DATA SECURITY AND PRIVACY**

**COMMITTEE MEMBERS**

**Senator Bruce Thompson – Chair**  
**District 14**

**Senator Brandon Beach**  
**District 21**

**Senator Mike Dugan**  
**District 30**

**Senator Jack Hill**  
**District 4**

**LTC David Allen**  
**Georgia National Guard**

**Mr. Chris Klaus**  
**Kaneva LLC**

**Mr. Bobby Laurine**  
**University System of Georgia**

**Mr. Calvin Rhodes**  
**Georgia Technology Authority**

Prepared by the Senate Research Office  
2016

## TABLE OF CONTENTS

|   |                 |
|---|-----------------|
| <b>Committee Focus, Creation, and Duties.....</b> | <b>2</b>        |
| <b>Background.....</b>                            | <b>2</b>        |
| <b>Committee Testimony.....</b>                   | <b>4</b>        |
| Meeting 1: August 30, 2016.....                   | 4               |
| Meeting 2: September 20, 2016.....                | 4               |
| Meeting 3: October 27, 2016.....                  | 6               |
| Meeting 4: November 10, 2016.....                 | 7               |
| Meeting 5: November 21, 2016.....                 | 8               |
| <b>Findings and Recommendations.....</b>          | <b>9</b>        |
| <b>Signature Page.....</b>                        | <b>10</b>       |
| <b>Supplemental Material.....</b>                 | <b>Appendix</b> |
| EY and GTA Report.....                            | Exhibit A       |

## **COMMITTEE FOCUS, CREATION, AND DUTIES**

The Data Security and Privacy Senate Study Committee (Committee) was created by Senate Resolution 360 in order to study the conditions, needs, issues, and problems that may exist with existing security procedures, practices, and systems in place across the state and local government in Georgia.

Senator Bruce Thompson of the 14<sup>th</sup> chaired the Committee, while other members included Senator Brandon Beach of the 21<sup>st</sup>, Senator Mike Dugan of the 30<sup>th</sup>, Senator Jack Hill of the 4<sup>th</sup>, LTC David Allen from the Georgia National Guard, Mr. Chris Klaus from Kaneva LLC, Mr. Bobby Laurine from the University System of Georgia, and Mr. Calvin Rhodes from the Georgia Technology Authority.

The Committee held a total of five meetings; four at the State Capitol on August 30, 2016, October 27, 2016, November 10, 2016, and November 21, 2016 and one at VMWare Air Watch Global Headquarters in Sandy Springs, Georgia on September 20, 2016.

The Committee heard official testimony from the following: Ms. Sarah Geffroy, Director of Global Public Policy at AT&T; Mr. Tom Wilson, Vice President and Chief Information Security Officer of the Southern Company; Mr. Robert Swiggum, Chief Information Officer for the Georgia Department of Education; Mr. Chris Foster, Strategic Account Executive for VMWare AirWatch; Mr. John Lens, Global Account Manager at VMWare AirWatch; Mr. Patrick Gaul, Executive Director of the National Technology Security Coalition (NTSC); Ms. Megan Howell, Manager of Public Affairs at First Data Corporation; Ms. Linda Montgomery, President of the Cyber World Institute (CWI); Col. Robin "Montana" Williams, Chief Operating Officer of CWI; Brigadier Gen. Joe Jarrard, Adjutant General of the Georgia Department of Defense; Mr. Calvin Rhodes, Chief Information Officer for the Georgia Technology Authority; Mr. Stan Gatewood, Chief Information Security Officer for the Georgia Technology Authority; Mr. David Upton, Secure Infrastructure Solutions Director with Microsoft; Ms. Yejin Cooke, Director of Government Affairs with the National Association of State Chief Information Officers (NASCIO); Mr. Jeff Collins, Director of Managed Network Services with AT&T; Mr. James O'Dell, Senior Cyber-Security Strategist with AT&T Business; Mr. Drew Morefield, Cybersecurity and Risk Executive at Capgemini; Mr. Wade Damron, Director of Risk Management Services for the Georgia Department of Administrative Services; Mr. Bill Schaumann, Senior Manager at Ernst & Young (EY); Mr. Christopher Smoak, Division Chief of the Cyber Technology and Information Security Laboratory at the Georgia Institute of Technology; and Mr. Wayne Mattadeen, Executive Director of Advisory Services for EY.

## **BACKGROUND**

### **Current Threat Landscape**

With recent cyber-attacks such as the Sony Picture Entertainment hack of 2014 and the Democratic National Committee (DNC) email leak of 2016, cybersecurity has become a top priority for both the private and public sector alike, with nation-state actors as the primary target. Most cybersecurity strategies today focus on a "perimeter" type security system (i.e. firewall); however, most reported cyber incidents happened within a network, where perimeter security is ineffective.

According to a survey conducted and produced by IBM, the "2016 Cyber Security Intelligence Index," the fields of healthcare, manufacturing, financial services, government, and transportation saw the most

cyber-attacks throughout 2015.<sup>1</sup> The report found that within those cyber-attacks, unauthorized access was and continues to be the leading cause of cyber incidents. This, along with an evolution in the cyber threat landscape including a rise in ransomware and advanced persistent threats (APT), has caused the need to better understand and protect against cyber-attacks.

### **Current Georgia Initiatives**

The Georgia Technology Authority's (GTA) Office of Information Security (OIS) currently focuses on three major areas of assurance for citizens of the state in the area of cybersecurity: (1) providing statewide cyber strategic direction and leadership in the protection of the state's information assets; (2) safeguarding the confidentiality, integrity and availability of state systems and applications; and (3) fostering a culture of security awareness throughout Georgia state agencies.<sup>2</sup> OIS functions include:

- Security Governance;
- Strategic Planning;
- IS and ITSec Policy and Compliance;
- IT/IS Risk Management;
- Security Awareness, Training Education, Professional Development, and Cyber Workforce Development;
- Continuity of Operations Planning (COOP);
- Cyber Fusion and Threat Information;
- Cybersecurity Consulting and Advisory Services; and
- Supporting the Governor's Cyber Security Board.

On June 25, 2015, Governor Nathan Deal issued an Executive Order creating the State Government Systems Cybersecurity Review Board, also known as the **Cybersecurity Board**, in order to "focus internally on the protection and privacy of state data."<sup>3</sup> The Cybersecurity Board is tasked with reviewing each executive state agency's cybersecurity preparedness relating to critical state operations and the risks concerning Georgia's citizens and government.

### **Enacted Legislation**

#### **Student Data Privacy, Accessibility, and Transparency Act** – Senate Bill 89 (2015-2016) – Effective 7/1/15

Senate Bill 89, also known as the "Student Data Privacy, Accessibility, and Transparency Act", provides measures relating to the protection of sensitive student data while also encouraging local boards of education to provide all instructional material is in digital or electronic format on and after July 1, 2020. The legislation also encourages each local board of education to provide a free laptop, tablet, or other wireless electronic device to each student, or allow students to provide their own, on and after July 1, 2020. Senate Bill 89 provides that funding to assist local boards of education to attain complete digital access be subject to the appropriations process, while also requiring the State Board of Education to annual present their recommended level of funding to the General Assembly for consideration.

---

<sup>1</sup> <http://www-03.ibm.com/security/data-breach/cyber-security-index.html>

<sup>2</sup> <https://gta.georgia.gov/cybersecurity>

<sup>3</sup> [https://gov.georgia.gov/sites/gov.georgia.gov/files/related\\_files/document/06.25.15.01.pdf](https://gov.georgia.gov/sites/gov.georgia.gov/files/related_files/document/06.25.15.01.pdf)



## COMMITTEE TESTIMONY

### Meeting 1: August 30, 2016

The first meeting, held at the Georgia State Capitol in Atlanta, Georgia focused on several issues including cybersecurity policies and legislation at the State and Federal levels, the current cyber threat landscape, industry strategies, and privacy and security in K12 education. The following individuals provided testimony:

- Sarah Geffroy, Director of Global Public Policy at AT&T;
- Tom Wilson, Vice President and Chief Information Security Officer for the Southern Company; and
- Robert Swiggum, Chief Information Officer for the Georgia Department of Education.

Sarah Geffroy presented first on cybersecurity policy and legislative recommendations for both the State and Federal levels. At the Federal level, Ms. Geffroy proposed a private-public partnership in order to create and promote effective regulation along with forward thinking strategic plans that are unencumbering and agile to navigate the every changing cyber landscape. On a State level the public-partnership would also come into play, but Ms. Geffroy also mentioned that enhancing current and creating new awareness and education programs would be beneficial to the State and local governments. Overall, Ms. Geffroy promoted the idea of flexible solutions, whether through legislative or other means, to allow public entities and private corporations to have the capability to adapt to the quickly changing cyber threat environment.

Tom Wilson spoke to the Committee concerning the current cyber threat landscape along with effective cybersecurity strategies to mitigate risks. Mr. Wilson stated that nation-state actors have become increasingly involved in cyber-attacks, with primary focuses on the Middle East and Central Asia. He noted that the landscape has evolved to include cyber-extortion and election-year network breaches. Mr. Wilson provided several solutions to better enhance cybersecurity and reduce cyber risk including segmentation of assets, leveraging Federal capabilities and funding, defense evolution, and sharing of intelligence.

Speaking from a utility company's point-of-view, grid resiliency and electromagnetic pulse (EMP) protection is an important concern. Mr. Wilson promotes an approach to grid protection that includes standards, private-public partnership, and incident response.

Robert Swiggum spoke to the Committee on the current cybersecurity and IT policy infrastructure used by the Georgia Department of Education (DoE). Mr. Swiggum elaborated on the types of information the DoE considers private and keeps secure, along with their compliance of Senate Bill 89 (2015). The DoE maintains and operates their own internal cybersecurity with methods such as email phishing tests and training. Mr. Swiggum followed the same sentiment of the previous presenters promoting non-prescriptive cybersecurity policies or legislation.

### Meeting 2: September 20, 2016

The Committee held its second meeting at the Global Headquarters of VMWare AirWatch, an enterprise mobility management company, in Sandy Springs, Georgia, where they discussed a number of cybersecurity topics ranging from current technologies available to help combat cyber threats and the cybersecurity issues specifically surrounding the financial and ecommerce sector to the current

workforce scenario surrounding IT and cybersecurity. The following individuals presented to the Committee:

- Chris Foster, Strategic Account Executive for VMWare AirWatch;
- John Lens, Global Account Manager at VMWare AirWatch;
- Patrick Gaul, Executive Director of the National Technology Security Coalition (NTSC);
- Megan Howell, Manager of Public Affairs at First Data Corporation;
- Linda Montgomery, President of the Cyber World Institute (CWI); and
- Col. Robin “Montana” Williams, Chief Operating Officer of CWI.

Chris Foster first presented information on VMWare AirWatch, the company history, and current clients who have implemented their technologies. John Lens then discussed the different problems that VMWare AirWatch clients frequently experience including, lack of network segmentation, poor server discipline, and poor workforce education. Mr. Lens promoted cybersecurity strategies and approaches such as micro-segmentation or “Zero Trust.”

A zero trust environment prevents unauthorized lateral movement within the data center by establishing automated governance rules that manage the movement of users and data between business systems and/or applications within the data center network. VMWare AirWatch believes that cybersecurity approaches, such as “Zero Trust” and micro segmentation, should be mandatory to enhance the government’s cyber security practices.

Patrick Gaul presented information about the newly created NTSC, a spin-off organization of the Technology Association of Georgia (TAG). The NTSC plans to act as a coalition of chief information security officers (CISOs) to promote the development of technology solutions and policies through advocacy, industry research and information, cybersecurity awareness program, professional development, professions networking. There will be six regions within the NTSC, with ten CISOs in each region. Currently, they have 11 private and public CISOs participating in the Coalition.

Megan Howell provided testimony to the Committee concerning the current state of cybersecurity problems surrounding the financial and ecommerce industry. First Data, an electronic financial transactions company, has seen a rise in credit card fraud, specifically in the quick service restaurant and hotel industries, where there are the weakest vulnerabilities.

Ms. Howell mentioned that the actual “theft” of data and credit card fraud are not always synonymous (i.e. a system can be hacked by an individual or group and that information can be sold on the black market for use by another individual or group). Currently, First Data employs two strategic solutions to help combat against financial cyber-attacks or incidents: (1) TransArmor<sup>4</sup>, a multilayer security solution which involves encryption and tokenization; and (2) EMV (Europay, MasterCard, and Visa) or “chip” cards.

Linda Montgomery first presented to the Committee on the purpose of the Cyber World Institute (CWI), a division of The Learning Center, Inc. The CWI is an organization which focuses on IT education and provides training and certification training in all areas of IT. Ms. Montgomery was joined by Col. Robin “Montana” Williams who spoke to the current cybersecurity and IT workforce landscape. Currently, there is a zero percent unemployment rate in Information Technology, with an estimated 1.5 million

---

<sup>4</sup> [https://www.firstdata.com/downloads/marketing-merchant/301-654-transarmor\\_ss\\_2p.pdf](https://www.firstdata.com/downloads/marketing-merchant/301-654-transarmor_ss_2p.pdf)

person shortage by 2020. Both Ms. Montgomery and Col. Williams focused on the need for talent and workforce development.

### **Meeting 3: October 27, 2016**

---

At the third meeting, held at the Georgia State Capitol, the Committee heard testimony regarding the current cybersecurity efforts of the State and the National Association of State Chief Information Officers, along with other private solutions available on the market. Presenters at this meeting included:

- Brigadier Gen. Joe Jarrard, Adjutant General of the Georgia Department of Defense;
- Calvin Rhodes, Chief Information Officer for the Georgia Technology Authority;
- Stan Gatewood, Chief Information Security Officer for the Georgia Technology Authority;
- David Upton, Secure Infrastructure Solutions Director with Microsoft; and
- Yejin Cooke, Director of Government Affairs with the National Association of State Chief Information Officers (NASCIO).

Adjutant Gen. Joe Jarrard and Calvin Rhodes discussed the creation, purpose, and current status of the Georgia Cybersecurity Board. Currently there are five executive agency assessments underway and the plans to add six more at the beginning of 2017. The assessments are trying to identify the cybersecurity gaps within each agency, specifically regarding training and enterprise tools which can be implemented to easily look at cybersecurity threats and procedure across state agencies.

Stan Gatewood presented on the current cybersecurity efforts of the Georgia Technology Authority (GTA), specifically concerning the Cybersecurity Board. In regards to cyber education and training, Mr. Gatewood promoted the concept of building a culture of cyber awareness, preparedness, and resilience, which should be applied to workers as well as citizens. Mr. Gatewood promoted the development and funding of a state-wide strategic plan, which would support a best practice for safety and economic drivers, to extend until 2020.

David Upton provided testimony to the Committee regarding the changes in the cybersecurity environment and how government agencies, specifically, need to be more aware and quicker to respond to cyber threats. Mr. Upton explained how the primary focus of cyber threats have turned to nation-state actors and despite the changing environment, most have not changed their cybersecurity strategies. He further noted that most state and local government IT departments do not have the depth or resources to effectively protect their secure information, but they must focus on the pertinent areas of vulnerability and security to maximize their cybersecurity protection.

Yejin Cooke presented the findings of a cybersecurity study report jointly created by Deloitte and the National Association of State Chief Information Officers (NASCIO). Ms. Cooke provided three major takeaways from the report: (1) Governor-level awareness is on the rise; (2) cybersecurity is becoming part of the fabric of government operations; and (3) a formal strategy can lead to more resources. She also mentioned that some emerging cyber threat trends include phishing and pharming, social engineering, ransomware, viruses, worms, and malware, and exploits of vulnerabilities from unsecured code.

Ms. Cooke also mentioned the shortage in workforce and the foreseeable problems that it will cause in the future. When asked how the State can increase the workforce, Ms. Cooke mentioned Federal programs, such as CyberCorps, could be beneficial.

### **Meeting 4: November 10, 2016**

---

The Committee held its fourth meeting at the Georgia State Capitol with Committee testimony provided by:

- Jeff Collins, Director of Managed Network Services with AT&T;
- James O'Dell, Senior Cyber-Security Strategist with AT&T Business;
- Drew Morefield, Cybersecurity and Risk Executive at Capgemini;
- Wade Damron, Director of Risk Management Services for the Georgia Department of Administrative Services;
- Bill Schaumann, Senior Manager at Ernst & Young (EY);
- Christopher Smoak, Division Chief of the Cyber Technology and Information Security Laboratory at the Georgia Institute of Technology; and
- Wayne Mattadeen, Executive Director of Advisory Services for EY.

Jeff Collins first offered testimony to the Committee on the details and scope of the current State and AT&T network contract. Currently, AT&T provides services to 15 executive branch agencies along with the security overlay services for the Georgia Enterprise Technology Services (GETS) program. Mr. Collins noted that it would be beneficial to both the State and AT&T to combine all agencies to better aggregate all pertinent cybersecurity information.

James O'Dell then presented on the ways that the government can better improve their current cybersecurity posture, specifically in the areas of Managed Security Information and Event Management (SIEM), Security Operations Center (SOC), Security Awareness Training, Data Loss Prevention (DLP), Identity Access Management (IAM), Cloud Security Shadow IT, Advanced Persistent Threat (APT) tools, and Department of Homeland Security Programs. Mr. O'Dell noted that before, security methods were based on preventative-based models, but advanced threats are causing the shift towards direction-based models.

Drew Morefield presented from CapGemini, a technology consulting company, on the current cybersecurity risk landscape along with enhanced and advanced IT solutions. Mr. Morefield stated that there is a need to approach cybersecurity differently, but with that comes increased vulnerabilities such as sophisticated cyber-attacks, ransomware, cross border data exchanges, third party risks, and insider threats. There are five areas of IT and cybersecurity where Mr. Morefield presented enhanced and advanced security strategies included Identity and Access Management (I&AM), Security Operations Center (SOC), Business Continuity and Disaster Relief (BCDR), Application Security Testing, and ongoing Governance Risk and Compliance (eGRC).

Wade Damron provided testimony to the Committee regarding the risks and current coverage options for cybersecurity insurances. Mr. Damron noted that while the market for cyber insurance is increasing the options for government cyber coverage have not. Currently, there are cyber insurance proposals to cover the State; however, they will be vetted by the Georgia Cybersecurity Council.

Bill Schaumann discussed several industry best practices concerning data privacy. Mr. Schaumann identified unremoved permission access as one of the biggest mistakes made concerning cybersecurity – the user has unnecessary access which can be purposefully or accidentally exploited. He also reiterated cybersecurity strategies previously mentioned in earlier testimony, specifically pointing out Data Loss Prevention (DLP) as a very effective tool.



Chris Smoak presented to the Committee on the future of cybersecurity, specifically focusing on people, process, and technology. Regarding people, Mr. Smoak suggests a new multi-discipline approach to solving cybersecurity challenges, with a wide range of expertise. For processes, the developments of process-specific tools are helping to reduce the overall cost of developing, testing, and maintaining strong cybersecurity processes. Lastly, Mr. Smoak promotes observing past trends to better help understand attackers' future technology focus.

Wayne Mattadeen offered a summary of the Data Security and Privacy Senate Study Committee's meetings thus far, along with several policy and legislative recommendations which will be presented in a final report completed by EY (See Appendix).

---

**Meeting 5: November 21, 2016**


The Committee met for a fifth, and final time, at the Georgia State Capitol to discuss its findings and recommendations based on the testimony heard at the previous meetings.

## **FINDINGS AND RECOMMENDATIONS**

The findings and recommendations for the Senate Study Committee on Data Security and Privacy have been provided in detail in a report collaboratively produced by Ernst & Young (EY) and the Georgia Technology Authority (GTA). The report has been provided in the Appendix.

Respectfully Submitted,

**THE SENATE DATA SECURITY AND PRIVACY STUDY COMMITTEE**



---

**Senator Bruce Thompson – Chairman  
District 14**