Cybersecurity Governance in the State of Georgia

A CASE STUDY

December 2017

Homeland Security

NASCIO
Representing Chief Information Officers of the States

Georgia State Fast Facts[1,2,3]

ELECTED OFFICIALS:

- Governor Nathan Deal
- Georgia House of Representatives: 180 Representatives
- Georgia State Senate: 56 Senators

STATE CYBERSECURITY EXECUTIVES:

- Georgia Technology Authority (GTA) Executive Director and State Chief Information Officer (CIO) Calvin Rhodes
- Chief Information Security Officer (CISO) Stanton Gatewood
- Chief Technology Officer (CTO) Dr. Steve Nichols

STATE DEMOGRAPHICS:

- Population: 9,810,417
- Workforce in "computers and math" occupations: 2.6%

EDUCATION:

- Public with a high school diploma: 49.8%
- Public with an advanced degree: 34.9%

COLLEGES AND UNIVERSITIES:

- 22 technical colleges[4]
- 29 public universities[5]
- 62 private colleges[6]

KEY INDUSTRIES:[7]

- Agriculture
- Film
- Energy
- Automotive
- Tourism

Executive Summary

The Overall Challenge:

How to address a range of cybersecurity challenges that cut across multiple government, public, and private sector organizations?

Overall Lessons Learned from Georgia's Governance Approach:

- **Leadership Matters**. Leaders across multiple government, public, and private organizations make cybersecurity, and cybersecurity governance, a priority.
- **Leadership Is Not Everything**. Laws, policies, structures, and processes instantiate and align cybersecurity governance with cybersecurity priorities so that focus does not change as personalities change.
- **Governance Crosses Organizational Boundaries.** The distributed nature of cybersecurity requires a range of governance mechanisms that connect across multiple organizations and sectors.

This case study describes how Georgia has used laws, policies, structures, and processes to help govern cybersecurity as an enterprise-wide, strategic issue across state government and other public and private sector stakeholders. It explores cross-enterprise governance mechanisms used by Georgia across a range of common cybersecurity areas—strategy and planning, budget and acquisition, risk identification and mitigation, incident response, information sharing, and workforce and education.[*]

This case study is part of a pilot project intended to demonstrate how states have used governance mechanisms to help prioritize, plan, and make cross-enterprise decisions about cybersecurity. It offers concepts and approaches to other states and organizations that face similar challenges. As the case covers a broad range of areas, each related section provides an overview of Georgia's governance approach, rather than a detailed exploration. Individual states and organizations seeking greater detail would likely need to engage directly with Georgia to better understand how to tailor solutions to their specific circumstances.

Since the early 2000s, the state of Georgia's executive branch has taken a series of deliberate steps to enable cybersecurity to be governed as an enterprise-wide strategic issue across the executive branch of state government and has included some other state government and private industry stakeholders. As the Georgia Technology Authority (GTA) Executive Director and Chief Information Officer (CIO) Calvin Rhodes said, "[Governor Deal] is deeply involved

[*] For purposes of this case study, governance refers to the laws, policies, structures, and processes that enable people within and across organizations to address challenges in a coordinated manner through activities such as prioritization, planning, and decision making.

and has made [cybersecurity] a top priority across the government. Having the governor's leadership and continued involvement in this space has been extremely important to get many things accomplished. [Former] Governor Perdue saw the importance of a strong information technology (IT) organization and started the modernization effort, which made way for pursuing [cyber]security."[8] Economic factors have made cybersecurity a priority for the state. For example, Georgia ranks third in the United States for information security, with more than 115 cybersecurity firms in the state,[9] and is a major hub for FinTech and Health IT industries,[10] driving a need for cyber expertise and a workforce pipeline.

The state of Georgia government governs IT through a governance structure that enables a unified and coordinated approach to cybersecurity across the executive branch. Under Georgia law, GTA has authority for technology, including cybersecurity, and its associated enterprise management, policy, and portfolio management. GTA is led by a single individual serving as its Executive Director and CIO. GTA leadership is responsible for coordinating and executing a unified executive branch strategy, which includes cybersecurity and aligns with overall statewide management priorities.

A 2007 state-commissioned study found significant cybersecurity risks due to old IT infrastructure and inadequate processes and governance, which led GTA to a transformation and consolidation initiative, development of a public-private partnership, and a strong sourcing governance structure, all aimed at strengthening the cybersecurity posture of the state. The management of the vendors in the partnership and the governance structure have evolved and advanced over the years, making way for the state to bolster other areas, such as risk identification and mitigation, incident response, and workforce development and education.

GTA uses its mandate of setting cybersecurity policy, standards, and guidelines for executive branch agencies as a way to identify and mitigate cybersecurity risks. (In this case study, "agency" refers to executive branch agencies.[11]) One way GTA accomplishes this mandate is through its Sourcing Management Organization (SMO), which oversees and manages GTA's service providers who are contracted to manage the state's infrastructure and managed network services. The SMO has developed a set of consistently used governance processes to create clear decision points, well-defined escalation paths, and structured meeting forums to identify and mitigate risks (including cybersecurity), receive cross-organizational updates, escalate issues, and collaborate across GTA, the agencies, and vendors.

Georgia has developed a governance approach for managing response to cyber incidents, ranging from minor to severe, across multiple stakeholders. With this approach, agencies assess the scope of the incident in consultation with GTA's Chief Information Security Officer (CISO) to determine whether it can be addressed within the agency itself, requires GTA and private vendor involvement, or needs to be escalated to involve organizations outside of GTA, such as the Georgia Emergency Management & Homeland Security Agency (GEMHSA), Department of Homeland Security (DHS), etc. This approach allows the state to tap into the necessary type and level of subject matter expertise depending on the severity and reach of the incident.

GTA is partnering with a variety of entities, including the Augusta University Cyber Institute, University System of Georgia, the Technical College System of Georgia, local school systems, the Georgia National Guard, Georgia Bureau of Investigation (GBI), federal agencies, and private corporations to narrow the cross-sector cybersecurity workforce gap. The Hull McKnight Georgia Cyber Innovation and Training Center will be managed by Augusta University and is

scheduled to open in the summer of 2018. It will provide a cyber range, a training facility focused on cyber workforce development through real-world practice and education, an incubator for start-up cybersecurity companies and co-location space, facilities cleared for top secret work, space for cybersecurity research and development, and GBI's new Cyber Crime Unit Headquarters.[12] Training will range from information security industry-standard certifications to university degrees from bachelor's degrees through doctorates.[13] The center will also house Georgia's Cybersecurity Workforce Academy,[14] which GTA's Office of Information Security (OIS) uses to deliver cybersecurity awareness, training, and education to agency information security officers (ISOs) in monthly, online virtual instructor-led trainings.

Cybersecurity is a challenge that cuts across many issues and many interdependent stakeholders. Therefore, Georgia uses a range of governance mechanisms to work across different public, academic, and, at times, private, organizations. The approaches described in this case study were the result of many years of intentional effort by many leaders and individuals who made cybersecurity and cybersecurity governance a priority across the state. As Dr. Steve Nichols, Chief Technology (CTO), GTA, pointed out, "[Georgia has] had two two-term governors, so we're going on 16 years of staying the course."[15] State leaders have looked at cross-organizational factors—policies, governance approaches and mechanisms, organizational design and structure, etc.—to make cybersecurity a top priority enterprise-wide. These leaders and the state legislature consider cybersecurity important from both a threat mitigation and economic development perspective. However, leadership was not everything. Georgia has used tangible laws, policies, processes, and forums to elevate the importance of cybersecurity and include it as an essential enterprise IT priority.

Table of Contents

Background & Methodology

This case study was developed as part of a pilot project to identify how states have used laws, policies, structures, and processes to help better govern cybersecurity as an enterprise-wide, strategic issue across state government and other public and private sector stakeholders. This project emerged as a result of the *Department of Homeland Security (DHS) Advisory Council Final Report of the Cybersecurity Subcommittee, Part II – State, Local, Tribal & Territorial (SLTT*), which recognized the importance of governance in addressing a range of cybersecurity technology and operational challenges.[16]

The case study explores cross-enterprise governance mechanisms used by Georgia across a range of common cybersecurity areas—strategy and planning, budget and acquisition, risk identification and mitigation, incident response, information sharing, and workforce and education. It is not intended to serve as a formal evaluation. Instead, the case offers concepts and approaches that may be useful to other states and organizations that face similar challenges. As this case covers a broad range of areas, each related section provides an overview of Georgia's governance approach, rather than a detailed exploration. Individual states and organizations seeking greater detail would likely need to engage directly with Georgia to better understand how to tailor solutions to their specific circumstances.

DHS' Office of Cybersecurity and Communications (CS&C) initiated and leads the project in partnership with the National Association of State Chief Information Officers (NASCIO). NASCIO is a nonprofit association "representing state chief information officers and information technology executives and managers from the states, territories, and the District of Columbia."[17] The Homeland Security Systems Engineering and Development Institute (HSSEDI), a DHS owned Federally Funded Research and Development Center (FFRDC), developed the case studies.

Candidate states were identified to participate in the pilot project based on:

- analysis of third party sources,
- diversity of geographic region, and
- recommendations from DHS and NASCIO with awareness of SLTT cybersecurity practices.

Candidate states that agreed to participate in the DHS-led pilot project did so on a voluntary basis. Researchers used open source material and conducted a series of interviews to gather the necessary information to develop each state case study.

I. Strategy & Planning

The Challenge:

How to set direction and prioritize cybersecurity initiatives across multiple organizations?

Features of Georgia's Governance Approach:

- The Georgia Technology Authority (GTA) sets the information technology (IT) and cybersecurity strategy and direction for the state.
- GTA uses data from executive branch agencies through its State Technology Annual Report Register (STARR) tool to inform adjustments to strategy, budget, and execution.
- In 2015, the governor established a new governance mechanism, the Cybersecurity Review Board, to support GTA in the development of its cybersecurity strategy and to increase the visibility of cybersecurity as a cross-government priority.

The authority to set cybersecurity strategy for agencies in the state of Georgia is held by GTA. This authority derives from its overall statutory role, "to provide for technology enterprise management and technology portfolio management…in the best interest of the state."[18] GTA is led by an Executive Director and State Chief Information Officer (CIO), Calvin Rhodes, and guided by a 12-member Board of Directors.[19]

GTA's authority includes establishing policies and standards, providing oversight and program management for IT projects exceeding a cumulative investment of over $1 million, establishing architecture for the state technology infrastructure, and managing the delivery of IT infrastructure services (i.e., mainframes, servers, service desk, end user computing, disaster recovery and security) to 85 agencies[20] and managed network services (i.e., wide and local area networks, voice, cable and wiring, and conferencing services) to 1,300 state and local government entities.[21]

As part of its 2025 "Enterprise IT Strategic Plan," GTA established cybersecurity as one of its five strategic goals, which helps guide alignment and prioritization of strategic investments. Sample cybersecurity priorities are to address the cyber workforce gap by bringing together cross-government organizations, private industry, and academia at the Hull McKnight Georgia Cyber Innovation and Training Center (scheduled to open in summer 2018 and described in the Workforce & Education section), use quantitative measures to advance Georgia's enterprise cybersecurity maturity, and establish cyber resilience.[22]

In addition to setting the overall strategy, GTA collects a range of information from agencies to help inform adjustments to its strategy and execution. Since 2000, GTA has had authority to collect IT-related data from agencies to help the state track IT costs and statistics.[23] A March

2008 Executive Order further clarified the security reporting. GTA distributes questionnaires through its STARR tool to collect and analyze self-reported data, including questions on application inventory, IT spend, data retention, and agencies' strategic planning.[24] STARR data is used to update the Enterprise IT Strategic Plan and shared with the agencies and the state legislature. It gives GTA a pulse on the enterprise and enables GTA to make adjustments on IT spending, cybersecurity, etc., from where it started seven years ago.[25] Various GTA offices use the data output from the tool. GTA's Enterprise Project Management Office (EPMO) analyzes results for anomalies, aging systems, vendor consolidation opportunities, and collaboration opportunities. The Office of Information Security (OIS), led by the Chief Information Security Officer (CISO), uses the security data for its security planning. GTA's Enterprise Governance and Planning office uses the data for strategic planning purposes.

In 2015, a new governance mechanism was created, in part, to support GTA in the development of its cybersecurity strategy and to increase the visibility of cybersecurity as a cross-government priority. Through an Executive Order, Governor Nathan Deal reinforced the state's focus on cybersecurity by creating a State Government Systems Cybersecurity Review Board (board) to bolster the cybersecurity of agencies' "networks, systems and data"[26] by:

- Strengthening statewide processes for developing and institutionalizing best practices,
- Developing and retaining a cybersecurity workforce, and
- Working with public and private entities to leverage emerging technology.[27]

The board is chaired by the State CIO and includes three other Governor-appointed agency heads, the Director of the Georgia Emergency Management & Homeland Security Agency (GEMHSA), the Adjutant General of Georgia Department of Defense (DoD)[28], and the Commissioner of the Department of Administrative Services (DOAS).[29] It provides a forum for the CISO's office and GTA to set cybersecurity priorities and a mechanism for state agencies to request funding for urgent cybersecurity needs. In addition to the board, there is an associated working group chaired by the CISO with members from each of the board member's organizations; both entities operate with the same goals and objectives. In December 2016, the board produced its first annual report, which provided an assessment of the state's overall cybersecurity preparedness, observations about agencies' cybersecurity preparedness, and a list of recommendations.

One of the board's recommendations was to create a Cybersecurity Review Panel to work with agencies to rate their system(s) low, medium, or high-impact "depending on the worse-case potential outcome of a security incident"[30] based on National Institute of Standards and Technology (NIST) and Federal Information Processing Standard (FIPS) 199-200 standards.[31] The state used third-party private sector companies to conduct quantitative risk assessments on the high-impact systems, including penetration (pen) testing, vulnerability scans, and tabletop exercises to identify cybersecurity risks.

The OIS has found the assessments to be invaluable. According to Stan Gatewood, CISO, GTA, the board and the third-party risk assessments "have been key turning points in helping state agencies understand cyber risks and the need to build risk identification and mitigation and cyber response plans."[32] These assessments will also be used to inform the premium allocations for Georgia's new cyber insurance policy. For the first year of the policy (FY 2018), the cost of the premium is allocated proportionately across all agencies based on employee headcount. For future fiscal years, GTA will use a maturity model, which will use the

third-party risk assessment findings to establish the maturity and risk level of an agency and give each agency "maturity points." The state will use these maturity points and employee headcount to determine the premium allocation paid by each agency. The more cyber mature an agency is, the less it will pay.

The policy covers all executive branch agencies and some non-executive branch agencies that voluntarily opted in. It provides $100 million in limits and a $1.8 million premium for data breach response and crisis management, and third- and first-party liability coverage. GTA and DOAS's Risk Management Services Division (the insurance policy holder) worked collaboratively on this effort.[33] According to Wade Damron, Director, Risk Management Services, DOAS, the policy demonstrates that Georgia is focused on promoting a "risk culture by awarding maturity points" and "cyber insurance incentivizes agencies to do better."[34]

II. Budget & Acquisition

The Challenge:

How to manage investments in strategic cybersecurity priorities as part of budget and acquisition processes across multiple organizations?

Features of Georgia's Governance Approach:

- GTA uses budget charge-back to provide consistent IT and cybersecurity services to agencies.
- The state's IT acquisition process involves multiple GTA and agency stakeholders early in the acquisition cycle to ensure that cybersecurity risk mitigation is considered in investment decisions.

GTA uses two primary budgetary and acquisition governance mechanisms to drive cybersecurity priorities across agencies. First, it uses budget charge-back to enable GTA to provide consistent IT and cybersecurity services across agencies. Second, it has developed an acquisition governance process that enables regular reviews and input into agency investments.

While GTA does not receive its own annual appropriated budget, the agencies do, and they use a portion of those funds to pay GTA for IT and cybersecurity services, such as infrastructure and managed network services, based on their service consumption. During the annual budgeting process, agencies work with the Office of Planning and Budget (OPB) to create their annual funding request.[35] As a part of this process, GTA provides budget projections based on previous year trend analysis and current projections for what each agency is expected to consume the following year.[36] The services that agencies purchase (e.g., infrastructure and/or managed network services) have cybersecurity features and their associated costs built into these service charges.

The agencies, including GTA, make ad hoc budget requests for unplanned activities (e.g., insurance policy premium, cyber assessments) throughout the year.[37] Out-of-cycle cybersecurity-related requests are first reviewed by the Cybersecurity Review Board and associated working group, then go to OPB and the Governor's office for approval.

GTA has a comprehensive governance methodology that guides its engagement in agency acquisitions and begins with "the initiation and planning phases of new information technology investments."[38] This acquisition governance methodology includes three foundational activities:

- Annual investment strategy sessions between GTA and technical and business leaders to discuss agency IT strategic plans to identify cross-agency collaboration opportunities, gain insight into investment planning, and improve accuracy of the state's technology inventory.

- Collaboration of purchasing, GTA, and agency business experts in conducting procurement revisions and creating development procurement documents with standard language.
- Guidance from state purchasing to agencies interested in alternative strategies for technical services delivery (e.g., cloud).[39]

In its role of "assuring that critical enterprise technology initiatives deliver on their promises and objectives,"[40] GTA's EPMO targets early involvement with large IT budgeting and procurement activities. By law, any technology projects costing over $1 million for a five-year total cost of ownership must submit a formal business case and/or organizational change management plan and strategy to OPB and the EPMO.[41,42] The EPMO conducts a preliminary review, often with consultation from the CISO and GTA's Sourcing Management Organization (SMO), and shares feedback with OPB, the agency, and GTA's Chief Technology Officer (CTO).

III. Risk Identification & Mitigation

The Challenge:

How to identify and mitigate cybersecurity risks across multiple organizations?

Features of Georgia's Governance Approach:

- GTA develops cybersecurity policies and standards that govern agencies in the development, deployment, and maintenance of systems.
- GTA leads several review boards and forums that are used to assessing and managing risk, including cybersecurity risk, for agency projects of over $1 million.
- GTA provides infrastructure and managed network services that agencies use to deliver many IT services, including cybersecurity.

Georgia's governance approach to risk identification and management emerged from a decision to modernize and centralize its IT in GTA. Over time, GTA has developed a cross-enterprise approach to risk management.

In 2007, Georgia commissioned a study by Technology Partners International[43] that found the state had significant cybersecurity risks due to aged infrastructure and lack of processes, procedures, and governance. As a result, Governor Sonny Perdue directed GTA to undergo a transformation and consolidation effort and create a public-private partnership to strengthen security, modernize infrastructure and networks, improve reliability, and increase transparency in the state's IT enterprise.[44] As a part of this, GTA shifted to an enterprise approach to technology intended, in part, to help manage cyber risk. While individual agencies manage the development, deployment, and maintenance of their systems, GTA drives enterprise-wide cybersecurity through three governance mechanisms:

- Development of cybersecurity policies and standards that govern agencies in the development, deployment, and maintenance of systems.
- Leadership of several review boards and forums that are used to assess and manage risk, including cybersecurity risk, for agency projects of over $1 million.
- Provision of infrastructure and managed network services that agencies use to deliver many IT services, including cybersecurity.

GTA has several offices that are focused on identifying and mitigating cybersecurity risks across the state's IT enterprise[45] through IT policies, standards, and guidelines, plus a variety of review mechanisms. Its OIS,[46] led by the CISO, has a particularly significant role in this area

because it "provides statewide cyber strategic direction and leadership" and sets cybersecurity policy, standards, and guidelines.[47] OIS operates similarly to a central information security program as defined by NIST, Special Publication 800-12.[48] It also uses processes, frameworks, and checklists to help the secure the state's data in accordance Federal Information Security Management Act (FISMA) and NIST standards.[49]

One way GTA seeks to mitigate cybersecurity risks is by requiring state agencies to have an Information Security Officer (ISO) or security designee and operate their own information security program that complies with GTA's IT policies, standards, and guidelines.[50] For agencies without a security designee, the CISO's office is creating a program allowing the agency to contract through its office to gain access to one.[51,52] OIS collaborates with agencies by holding a monthly ISO Council meeting with agency ISOs to discuss security activities and news and hear about what the ISOs are seeing. These meetings are intended to help in raising all agencies to the same cybersecurity level, and relevant information is shared with the Cybersecurity Review Board.

With a focus on increasing project success rate, GTA developed three executive-level governance and oversight boards, and associated governance processes, for IT projects over $1 million (see Table 1).

Table 1. Highlighted Cybersecurity Risk Identification and Mitigation Bodies

Cybersecurity Risk Identification & Mitigation Bodies (frequency)	Purpose	Participants
Critical Projects Review Panel (monthly)	Monitor performance of IT projects over $1 M investments, address risks, and make fact-based decisions, etc.	• Chaired by the CIO and co-chaired by the Deputy CIO • State government executives
Large IT Project Executive Decision-Making Board (as needed)	Provide additional level of oversight and governance to projects over $10 M and projects selected due to their significance to the state.	• One permanent, voting board member from GTA, OPB, and DOAS, respectively • Two additional members from the agency managing the project
Cybersecurity Review Board (monthly) and associated Cybersecurity Review Panel (initially every other month and then as needed)	*Board:* Set cybersecurity priorities and a mechanism for state agencies to request funding for urgent cybersecurity needs. *Panel:* Help agencies rate systems as low-, medium-, or high-impact and provide oversight to the high-impact systems. Report findings to the Cybersecurity Review Board.	*Board:* • Chaired by the CIO • Director, GEMHSA • Director, DOAS • Adjutant General, GA DoD *Panel:* • Chaired by the CISO • Participating agencies

For projects over $1 million, the Critical Projects Review Panel, chaired by the CIO and co-chaired by the Deputy CIO, meets monthly to hear directly from agencies about their projects'

performance (i.e., schedule and delivery of services), monitor these investments, address risks early (including cybersecurity), and make fact-based decisions. For these projects, the agencies retain project management responsibilities.

For projects over $10 million or of particular significance to the state, GTA developed the Large IT Project Executive Decision-Making Board in January 2017.[53] The board has one permanent, voting board member from GTA, OPB, and DOAS, respectively, with two additional members from the agency managing the project.[54] This board has ultimate decision-making authority over the project's entire life cycle, including pre-solicitation activities, vendor award, organizational change management plan reviews, and transition to agency program management, etc.[55]

For all projects over $1 million, GTA supplements these formal boards with a set of governance processes related to the system development life cycle (SDLC) to help mitigate project risks. The EPMO, the organization within GTA that manages these processes, uses a formal governance process to mitigate all project risks, including cybersecurity risks. It consults with state agencies during plan, build, and execution phases to reduce project risks and failures, increase project deliveries on budget and schedule, and meet business needs. It provides support through assessments, governance, investment management, professional development, project assurance assessment, and project management.[56] By monitoring IT projects, EPMO's governance framework ensures that policies, standards, and guidelines are followed in the SDLC and gives decision makers a view of "the full range of projects to ensure that the right projects are executed at the right time with the minimum amount of risk."[57]

GTA has embedded several checks in the SDLC of over $1 million projects specifically to reduce cybersecurity risks. This begins early when the EPMO, the project's agency(ies), and others are in the planning and contracting phases, and the EPMO brings the CISO's office into the process to provide analysis on security and privacy protocols, hardware/software features, etc. The EPMO remains engaged throughout the project's life cycle through full implementation and continues to involve the CISO for security input. Prior to deploying an application or system, the agency is required to perform its own validation;[58] however, the final decision to deploy must be approved by a group that includes several GTA leaders, including the CISO. These decision makers determine whether the application or system meets all technical and security requirements, including an associated security plan, required for deployment. The CISO monitors this process carefully and reviews claims raised by the vendor to ensure that proofs of assurance are verified.

In 2007, GTA began consolidating the provision of infrastructure and managed networked services to agencies through a public-private partnership called the Georgia Enterprise Technology Services (GETS) program, which GTA uses to deliver two types of services: infrastructure (e.g., mainframes, servers, service desk) and managed network services (e.g., wide and local area networks, voice). Prior to GETS, agencies ran separate networks and firewalls with different security standards, creating untenable vulnerabilities. Dean Johnson, Chief Operating Officer (COO), SMO, said, "hundreds of firewalls and thousands of rules was a nightmare to manage and consolidating [through GETS] in a centrally managed way improved [GTA's] security profile."[59] The GETS model of IT-as-a-service is consumption-based,[60] giving agencies insight into costs and allowing them to quickly introduce new and innovative IT services, thereby decreasing the risk associated with maintaining cybersecurity features of aging IT.

According to Chris McClendon, Technology Services Officer, SMO, "GETS is the anchor for

[GTA's] security work"[61] and "security underpins everything that is done in the GETS environment."[62] One of the first steps in standing up the GETS program was to consistently apply standards for systems and building processes across the enterprise. GETS started in 2008 with two prime contractors to manage the infrastructure and managed services contracts. These vendors, called service tower providers (STPs),[63] are contractually responsible for applying GTA technical and security standards consistently to the network and all systems and applications and conducting their own patching, currency, quarterly health checks, etc., to ensure that systems are within specification. A contract for a multisourcing service integrator (MSI) was added in 2015 to tie the STPs together; integrate, coordinate, and oversee the delivery of "multiple technology providers and [standardize] processes and systems"[64] to state agencies (with approximately 40,000 end users); and serve as a coordination point for the state's security program.[65] The SMO oversees these service providers and their associated risks, including cybersecurity, through a separate sourcing governance structure that is described in the Deep Dive section.

Agencies on the GETS network request IT services from GETS STPs to develop, test, and operate applications.[66] All vendors are contractually responsible for complying with GTA's policies, technical requirements, and standards.[67] As Dr. Steve Nichols, CTO, GTA, said, "Outsourcing was the best thing that ever happened to [GTA]. We have real transparency; contracts slice up the liability…and people disclose problems and fix them."[68]

IV. Incident Response

The Challenge:

How to prepare for and respond to cyber incidents that require coordinated action across multiple organizations?

Features of Georgia's Governance Approach:

- Georgia has an incident response governance approach that allows it to escalate incidents based on severity from GTA to GEMHSA.
- During the incident response process, GTA forms an Incident Response Team (IRT) of cross-government representatives who are collectively authorized to facilitate the response process.

Georgia has developed a response approach for managing cyber incident responses, from minor incidents to severe attacks across organizations. Its approach defines when incidents can be managed by an agency itself; when they require GTA, MSI, and STP support; when they are escalated to involve other state government entities; and when the incident requires participation, engagement, and leadership from outside state government by entities such as DHS, critical infrastructure, and private industry.

GTA's Governance, Risk, and Consulting and Cyber divisions of OIS are focused on protecting the state's infrastructure and network. OIS develops, delivers, and maintains the state's cybersecurity program.[69] As a part of its responsibilities, it has created standards that require agencies to implement a formal information security program, designate an ISO to run the program, and have an incident response plan that has been approved by the CISO with review by the Georgia Bureau of Investigation (GBI).[70] GEMHSA is responsible for cybersecurity incidents that require more resources than GTA has or that extend beyond state government and include critical infrastructure, private industry, etc.

The response to cybersecurity incidents varies based on the breadth of the incident. A minor incident (e.g., malware within a single agency) affecting a small number of computers, systems, and agencies is handled by the agency in accordance with its own incident response plan. If a more significant incident happens (e.g., denial of service attack, incident that impacts a critical business application) to an agency utilizing GETS services, GTA and the MSI manage the response process in coordination with the agency and the infrastructure services STP. When incidents are reported into the MSI's help desk, the staff is trained to look for trigger words to know if the incident can be handled within the agency or if it needs to be escalated. If an incident occurs within a non-GETS agency or if more response capacity is needed, the agency can contract with MSI and other vendors to support the response.[71] For these types of minor to moderate incidents, Georgia forms an Incident Response Team (IRT) to handle the incident "so that investigation and recovery can

quickly occur."[72] The IRT is led by the GTA ISO and includes members from the agency encountering the incident, OIS, GETS, law enforcement, legal, communications, etc.[73]

If the incident is more severe, the CIO and Cybersecurity Review Board, which includes the GEMHSA Director and Adjutant General of Georgia DoD, can decide to elevate the response to the Governor's office. At this point, these entities determine a plan of action, which can include mobilizing GEMHSA and Georgia National Guard cyber teams. The Georgia National Guard provides an important level of cybersecurity expertise and is the sponsoring entity that allows the state to receive controlled information (i.e., classified briefings). In the event of this level of incident management, GEMHSA and GTA work together to coordinate the cross-ecosystem response. The state can also choose to utilize its cybersecurity insurance policy (described in the Strategy & Planning section) for additional support and resources.[74]

Georgia tested its incident response plan with a variety of government and private entities in the weeklong 2016 Cyber Storm V national cybersecurity exercise[75] that simulated widespread system failures and outages in a safe environment. The exercise allowed participants to practice their response and identify gaps in cybersecurity communication, handoffs, and capabilities.[76]

The Hull McKnight Georgia Cyber Innovation and Training Center (described in the Workforce & Education section) is expected to further enhance incident response collaboration through partnerships with critical state, federal, academic, research, and private industry cyber resources and the creation of new offices, such as GBI's new Cyber Crimes Unit

V. Information Sharing

The Challenge:

How to engage across multiple organizations to share cybersecurity-related information?

Features of Georgia's Governance Approach:

- Georgia uses different governance mechanisms to share a variety of information with a range of stakeholders.
- The Georgia Information Sharing and Analysis Center (GISAC) and Multi-State Information Sharing and Analysis Center (MS-ISAC) are used to share cybersecurity threat information across a range of public and private stakeholders.
- The Cybersecurity Review Board and sourcing governance structure are used to share cybersecurity risk information across government stakeholders.

Georgia uses different governance mechanisms to share different kinds of information with a range of stakeholders (see Table 2).

Table 2. Georgia Information Sharing Entities

Information Sharing Entities	Type of Information Shared	Target Audience
GISAC	Cybersecurity operational and intelligence information	Agencies; state, local, and federal governments; private sector entities
MS-ISAC	Cyber threat information	Agencies, state and local governments, private sector entities
Cybersecurity Review Board	Cybersecurity statewide risk information	State leadership, GTA, agencies
Sourcing Governance Structure	Cybersecurity-related risks associated with SDLC	GTA, agencies, vendors

Several GTA employees are staffed at the State Fusion Center, formally known as GISAC, run by GBI, State Police, and GEMHSA. GISAC receives cyber threat information related to the state's critical infrastructure (e.g., the state's IT assets, networks, and constituent data and information) from local, state, and federal partners and MS-ISAC. GISAC assesses the information for relevancy and processes it into communications to inform stakeholders of possible threats.[77] Stakeholders include local governments using the Homeland Security

Information Network, local and state law enforcement, federal partners, and private industry.[78]

Georgia also participates in the MS-ISAC to gather information on cyber threats across the nation and the state. The MS-ISAC provides the state with two-way information sharing channels and incident response training and awareness.[79]

Another internal information sharing mechanism is the Cybersecurity Review Board (described in the Strategy & Planning section). This forum analyzes and shares information about the state cybersecurity risk posture and landscape from a cross-government perspective and shares this information with the Governor and other state leaders to inform strategic cybersecurity decision making.

A related information sharing mechanism is the sourcing governance structure (introduced in the Risk Identification & Mitigation section and described in detail in the Deep Dive section). This structure provides regular forums in which service providers, agency and GTA representatives, and other government personnel share information. These forums give the participants opportunities to communicate about cybersecurity risks found in projects' SDLC and discuss remediation approaches.

The state is also working to develop relationships across state- and local-level entities to leverage knowledge and resources. For example, GTA is now working closely with a state senator, rural and metropolitan hospitals, and the Georgia Hospital Association to bring together healthcare IT professionals to talk about cybersecurity issues they are facing and what resources are needed to address those issues. According to Jeff McCord, Director, Intergovernmental Relations, GTA, "GTA is proactively figuring out this first-of-its-kind state/private partnership, and it could be a model for engaging other industries in the state."[80]

VI. Workforce & Education

The Challenge:

How does Georgia work across multiple organizations to shape responses to cybersecurity workforce shortages and education needs?

Features of Georgia's Governance Approach:

- The Hull McKnight Georgia Cyber Innovation and Training Center will bring together federal, state, and local government entities with academia, research, and private industry to address workforce development and education gaps.
- The center's construction was funded with state funds, and will be managed by a university; ongoing operational costs will be funded by tenants.

Workforce development and education have emerged as priority areas of investment for Georgia. The state government is focused on narrowing the cybersecurity workforce gap that cuts across multiple organizations and sectors.

The state is developing a new public-private mechanism, the Hull McKnight Georgia Cyber Innovation and Training Center (center) in Augusta, to address this gap by bringing together cross-government organizations, private industry, and academia. The center, slated to open in the summer of 2018, will be a state-owned, 167,000-square-foot facility for cross-ecosystem collaboration and interdisciplinary research supporting cybersecurity innovation "to stay a step ahead of emerging threats by aligning training and technology."[81] Augusta University will manage the day-to-day operations through a memorandum of understanding with GTA.[82]

The center will house a cyber range, a training facility focused on cyber workforce development through real-world practice and education, an incubator for start-up cybersecurity companies and co-location space, facilities cleared for top secret work, space for cybersecurity research and development, and GBI's new Cyber Crime Unit Headquarters.[83] Training will range from information security industry-standard certifications to university degrees from bachelor's degrees through doctorates.[84] These types of training will help to increase the cybersecurity workforce pipeline across the state that will benefit all sectors. The center will also house Georgia's Cybersecurity Workforce Academy,[85] which GTA's OIS uses to deliver cybersecurity awareness, training, and education to agency ISOs in monthly, online virtual instructor-led trainings.

GTA is partnering with a variety of entities, including the Augusta University Cyber Institute,

University System of Georgia, the Technical College System of Georgia, local school systems, the Georgia National Guard, GBI, federal agencies, and private corporations to develop the center. The facility will leverage Georgia's research institutions to focus on research and development.[86] The initial funding for the building's construction came from a state government budget appropriation. Once the center is functional, operating and maintenance costs will be covered by the tenants who are leasing the space. The existing Augusta University Cyber Institute will move to the new facility, which will have a strong focus on research and development and will tap into the assets of the University System of Georgia's research institutions. Other partners include Augusta Technical College, the City of Augusta, the GBI, U.S. Army Cyber Command, U.S. Army Cyber Center of Excellence, National Security Agency (NSA), and private entities, including both established and start-up cybersecurity companies. According to the NSA, "The Georgia Cyber Innovation and Training Center will allow our best and brightest, from both the public and private sector, to develop critical relationships in an innovative and collaborative training environment."[87]

VII. Deep Dive: GTA Sourcing Governance Forums

Introduction

The purpose of the "Deep Dive" is to provide a more in-depth look at how Georgia applied a formal sourcing governance solution to address a specific cyber governance challenge.

The Challenge

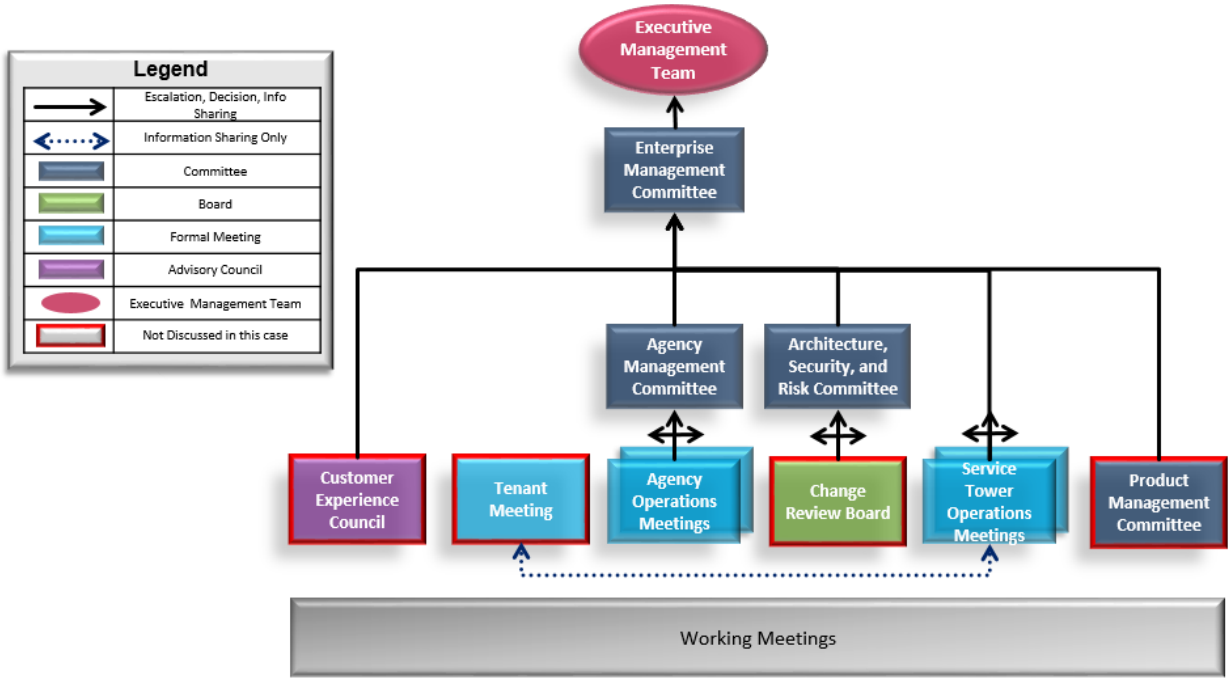
Large organizations with vast IT operations face challenges in managing cybersecurity risk, in part due to confusing decision points, unclear decision-making authority, and undocumented escalation paths. Identifying and mitigating cybersecurity risk happens across the enterprise performance life cycle, from procurement through maintenance. Developing and following a clear governance framework with cross-organizational participation can help organizations identify and mitigate risk and operate effectively and efficiently.

The Solution

Create a formal sourcing governance structure that stretches across organizations and includes the MSI as a co-chair in every meeting to ensure clear lines of communication. Develop the program in a way that creates consistent, streamlined forums with measurable activities, increases agency involvement in the forums, establishes clear, simplified escalation paths with correct decision makers present, and leverages knowledge sharing by using tools to manage governance and defining information flows clearly.[88]

Background

Agencies are responsible for managing the development of their own applications and systems. Since GTA provides the infrastructure, transport layers, operating system, etc., agencies must adhere to GTA policies, standards, and guidelines and work with GTA to put the application or system onto the GETS network.[89] GTA's SMO uses its sourcing governance forums (see Figure 1) to manage this process, identify and mitigate risks (including cybersecurity), receive updates, and identify points of collaboration. The number and types of forums vary from roughly 10 to 15, depending on the need and type of work occurring across the GETS program. This flexibility allows the SMO and GTA to quickly adapt to shifting needs. While the number of forums might change, the structure and formality within them are key, and the SMO emphasizes the use of consistent governance processes.90 As Dean Johnson, COO, SMO, GTA, said, "We [GTA] don't just treat governance with lip service; we perform governance every day. Before, we looked at governance as an impediment, but we've found we are more efficient when we have our governance in order. Governance in and of itself is why we have been successful, and [heavily involving] the agencies pays dividends every day."[91]



* The Sourcing Governance Forum structure is flexible and adjusts based on the enterprise's need at the time. This reflects its structure as of October 2017.

Figure 1. GTA Sourcing Governance Forums[92]

At the top of its sourcing governance forums structure is the *Executive Management Team*, consisting of the CIO and Deputy CIO, who are available to resolve unsolved issues from lower forums. This team participates formally by attending the *Enterprise Management Committee* on a quarterly basis to stay up-to-date on activities and serve as decision makers as needed. The *Enterprise Management Committee* meets monthly and is chaired by the SMO COO and co-chaired by the MSI. Participants include a project executive from each STP, their direct reports, and GTA leadership, with the purpose of providing enterprise oversight of the program, services, MSI, vendors, and customer experience[93] and discussing high-level status. This meeting can serve as an escalation point for topics coming out of two forums occurring below it:

- The monthly *Architecture, Security, and Risk Board* is chaired by the SMO Technology Services Officer and co-chaired by the MSI. It serves as the primary governance mechanism for cybersecurity risk management.[94] This board reviews the GETS Risk Register and conducts a review of the month's activities (e.g., where intrusion prevention systems are deployed, how complete patching is, what anti-virus software is reporting, etc.). The GETS Risk Register is maintained by the MSI and contains GETS-related risks; risk inputs come from various sources (e.g., MSI, STPs, GETS ISO, agency ISO). It includes items such as exceptions to standards and other information coming out of the working-level governance meetings.[95] Participants include the MSI, relevant STPs, GTA, and agencies.
- The monthly *Agency Management Committee* is chaired by the GETS Integration Officer and co-chaired by the MSI. It provides oversight of the overall program, services, and customer (i.e.,

agency) experience.[96] Participants include the MSI, agencies, and GTA.

There are more forums (including some not discussed in this case) and working meetings below these bodies. For example, the weekly *Agency Operations Meetings* (one for each agency on the GETS network), which are chaired by the agency CIO. These meetings are focused on the general management of day-to-day program operations at the agency level.[97] There are also every-other-week *Service Tower Operations Meetings* to discuss activities for the individual forums (i.e., MSI, infrastructure services STP, managed network services STP). Participants include the MSI, relevant service tower, and GTA. Topics from these two meetings can be shared with each other or rolled up to other meetings as needed.[98]

Throughout this regular cadence of governance forums, the SMO has documented escalation points that are strictly followed for decision making and risk management, including a communication chain to the Governor's office through the Cybersecurity Review Board, if needed. According to Dean Johnson, COO, SMO, GTA, this diverse set of forums and meetings is designed to look at the GETS enterprise from both a service and agency perspective and help GTA to maintain a "very secure, reliable, recoverable infrastructure."[99]

VIII. Acronyms

Acronym	Definition
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COO	Chief Operating Officer
CS&C	Office of Cybersecurity and Communications
CTO	Chief Technology Officer
DoD	Department of Defense
DHS	Department of Homeland Security
DOAS	Department of Administrative Services
EPMO	Enterprise Portfolio Management Office
FFRDC	Federally Funded Research and Development Center
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
GBI	Georgia Bureau of Investigation
GEMHSA	Georgia Emergency Management & Homeland Security Agency
GETS	Georgia Enterprise Technology Services
GISAC	Georgia Information Sharing and Analysis Center
GTA	Georgia Technology Authority
HSSEDI	Homeland Security Systems Engineering and Development Institute
IRT	Incident Response Team
ISO	Information Security Officer
IT	Information Technology
MS-ISAC	Multi-State Information Sharing and Analysis Center
MSI	Multisourcing Service Integrator
NASCIO	National Association of State Chief Information Officers
NSA	National Security Agency
NIST	National Institute of Standards and Technologies
OIS	Office of Information Security
OPB	Office of Planning and Budget
SDLC	System Development Life Cycle
SLTT	State, Local, Tribal & Territorial
SMO	Sourcing Management Organization
STARR	State Technology Annual Report Register
STP	Service Tower Provider

[1] Georgia.gov, "Elected Officials." Available: https://georgia.gov/elected-officials.
[2] Statistical Atlas, "Overview of Georgia." Data based on US Census Bureau 2010 census. Available: https://statisticalatlas.com/state/Georgia/Overview.
[3] Information regarding elected officials and state cybersecurity executives was validated in November 2017. "Fast Fact" details were collected in October 2017.
[4] Technical College System of Georgia, "About TCSG." Available: https://tcsg.edu/about-tcsg/.
[5] University System of Georgia, "Prospective Students." Available: http://www.usg.edu/information/prospective_students/.
[6] CollgeCalc, "Private Colleges in Georgia." Available: http://www.collegecalc.org/colleges/georgia/private/.
[7] Newsmax, "Top 5 Industries in Georgia: Which Parts of the Economy Are Strongest?" Available: http://www.newsmax.com/FastFeatures/georgia-industries-top-5-strongest/2015/03/06/id/628277/.
[8] Interview with Calvin Rhodes, Executive Director and Chief Information Officer, Georgia Technology Authority. (2017, August 28).
[9] Georgia.org, "Industries in Georgia/Information Technology/Cybersecurity." Available: http://www.georgia.org/industries/information-technology/cybersecurity/.
[10] Ibid.
[11] "'Agency' means every state department, agency, board, bureau, commission, and authority but shall not include any agency within the judicial or legislative branch of state government, the Georgia Department of Defense, departments headed by elected constitutional officers of the state, or the University System of Georgia and shall also not include any authority statutorily required to effectuate the provisions of Part 4 of Article 9 of Title 11." O.C.G.A. § 50-25-1. GTA works with the non-executive branch entities in a variety of ways, depending on the needs of those entities.
[12] Georgia.gov, "Cyber center groundbreaking underscores state's leading role in cybersecurity." Available: https://gta.georgia.gov/press-releases/2017-06-20/cyber-center-groundbreaking-underscores-states-leading-role-cybersecurity.
[13] Trubey, J. Scott. "New Georgia training center in Augusta to counter cyber threats." The Atlanta Journal-Constitution, 19 June 2017. Available: http://www.myajc.com/news/local-govt--politics/new-georgia-training-center-augusta-counter-cyber-threats/rEs9KmrDuvKjdR7SFqw9hO/.
[14] Sample classes include Introduction and Basic Cybersecurity, Cybersecurity Policy Management, Cybersecurity Incident Management, and Cybersecurity Maturity. Available: https://gta.georgia.gov/georgia-cybersecurity-workforce-academy.
[15] Interview with Dr. Steve Nichols, Chief Technology Officer, Georgia Technology Authority. (2017, August 22).
[16] Department of Homeland Security Advisory Council, "Final Report of the Cybersecurity Subcommittee, Part II – State, Local, Tribal & Territorial (SLTT)." (2016, June). Available: https://www.dhs.gov/sites/default/files/publications/HSAC_Cybersecurity_SLTT_FINAL_Report.pdf.
[17] About NASCIO. Available: https://www.nascio.org/AboutNASCIO.
[18] O.C.G.A. § 50-25-1.
[19] Membership of the Board of Directors includes "seven members appointed by the Governor, two appointed by the Lieutenant Governor, two appointed by the Speaker of the House of Representatives, and one non-voting member appointed by the Chief Justice of the Georgia Supreme Court." Available: https://gta.georgia.gov/board-directors.
[20] Fourteen executive branch agencies receive these services through GTA, while the remaining agencies may receive two or three of these services. Source: https://gta.georgia.gov/about-gta.
[21] O.C.G.A. § 50-25-4.
[22] Georgia Enterprise IT Strategic Plan, p. 8. (2017, May). Available: https://gta.georgia.gov/sites/gta.georgia.gov/files/related_files/site_page/Georgia-Enterprise-IT-Strategic-Plan-2025.pdf.
[23] From Dr. Steve Nichols, Chief Technology Officer, Georgia Technology Authority. Email communication. (2017, October 28).
[24] Strategic planning questionnaire focused on the following areas: providing mobile devices, using Office 365, adopting an agency teleworking policy, encouraging remote meeting participation, improving citizen access to services, and using mobile-enabled service delivery. Available: http://gta.georgia.gov/annualreport/sites/gta.georgia.gov.annualreport/files/related_files/site_page/Annual%20State%20IT%20Report%202016.pdf.
[25] Interview with Mike Curtis, Director, Enterprise Governance and Planning, Georgia Technology Authority; Teresa Reilly, Director, Enterprise Portfolio Management Office, Georgia Technology Authority; and Nicol Bell, Information Security Analyst, Office of Information Services, Georgia Technology Authority. (2017, September 5).
[26] Annual State IT Report FY 2016, p. 23. (2017, January). Available: http://gta.georgia.gov/annualreport/sites/gta.georgia.gov.annualreport/files/related_files/site_page/Annual%20State%20IT%20Report%202016.pdf.
[27] Ibid.
[28] Use of "Georgia Department of Defense" refers to Georgia's National Guard.
[29] State of Georgia Executive Order. (2015, June 25). Available: https://gov.georgia.gov/sites/gov.georgia.gov/files/related_files/document/06.25.15.01.pdf.
[30] Annual State IT Report FY 2016, p. 23. (2017, January). Available: http://gta.georgia.gov/annualreport/sites/gta.georgia.gov.annualreport/files/related_files/site_page/Annual%20State%20IT%20Report%

202016.pdf.

[31] Seventeen agencies participated in the panel's first meeting. Annual State IT Report FY 2016, p. 23. (2017, January). Available: http://gta.georgia.gov/annualreport/sites/gta.georgia.gov.annualreport/files/related_files/site_page/Annual%20State%20IT%20Report%202016.pdf.

[32] Interview with Stanton Gatewood, Chief Information Security Officer, Office of Information Security, Georgia Technology Authority. (2017, September 7).

[33] Obtaining the insurance policy took two years of market research and meetings with insurers. Interview with Wade Damron, Director, Risk Management Services, Department of Administrative Services, Georgia Technology Authority. (2017, August 31).

[34] Interview with Wade Damron, Director, Risk Management Services, Department of Administrative Services, Georgia Technology Authority. (2017, August 31).

[35] Some of the agencies' state budgets are supplemented with federal funds (e.g., grants).

[36] Interview with Dean Johnson, Chief Operating Officer, Sourcing Management Organization, Georgia Technology Authority and Chris McClendon, Technology Services Officer, Sourcing Management Organization, Georgia Technology Authority. (2017, September 5).

[37] Interview with Jeff McCord, Director, Intergovernmental Relations, Georgia Technology Authority. (2017, September 1).

[38] Annual State IT Report FY 2016, p. 23. (2017, January). Available: http://gta.georgia.gov/annualreport/sites/gta.georgia.gov.annualreport/files/related_files/site_page/Annual%20State%20IT%20Report%202016.pdf.

[39] Ibid.

[40] Georgia.gov, "Enterprise Portfolio Management." Available: https://gta.georgia.gov/epmo-main-page-0.

[41] Georgia.gov, "Accountability, Change Management and Process Improvement Act of 2016 (HB676)." Available: https://gta.georgia.gov/psg/article/accountability-change-management-and-process-improvement-act-2016-hb676-0.

[42] The business cases must include an assessment of the initiative's impact of change and how the agency will manage the change. Available: http://gta.georgia.gov/annualreport/sites/gta.georgia.gov.annualreport/files/related_files/site_page/Annual%20State%20IT%20Report%202016.pdf.

[43] From Dr. Steve Nichols, Chief Technology Officer, Georgia Technology Authority. Email communication. (2017, November 17).

[44] Georgia.gov, "Calvin Rhodes." Available: https://gta.georgia.gov/calvin-rhodes.

[45] Georgia.gov, "Governance, Risk and Consulting." Available: https://gta.georgia.gov/governance-risk-and-consulting.

[46] A complete list of OIS functions: 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. Available: https://gta.georgia.gov/cybersecurity.

[47] Georgia.gov, "Cybersecurity." Available: https://gta.georgia.gov/cybersecurity.

[48] Ibid.

[49] Some groups use the 20 Center for Internet Security controls (CIS 20) for a more digestible way to identify and mitigate risks. Interview with Stanton Gatewood, Chief Information Security Officer, Office of Information Security, Georgia Technology Authority. (2017, September 7).

[50] Georgia.gov, "Cybersecurity." Available: https://gta.georgia.gov/cybersecurity.

[51] Interview with Stanton Gatewood, Chief Information Security Officer, Office of Information Security, Georgia Technology Authority. (2017, September 7).

[52] Approximately 80 to 85 agencies have one full-time IT person designated as the agency's ISO. Smaller agencies might assign ISO responsibilities to a network administrator, and some bigger agencies might have a dedicated ISO office. Interview with Dr. Steve Nichols, Chief Technology Officer, Georgia Technology Authority. (2017, August 22).

[53] Georgia.gov, "Large IT Project Executive Decision-Making Board." Available: https://gta.georgia.gov/psg/article/large-it-project-executive-decision-making-board.

[54] "If the project involves more than two agencies, the permanent members will select the agencies to participate as members of this council." Available: https://gta.georgia.gov/psg/article/large-it-project-executive-decision-making-board.

[55] Georgia.gov, "Large IT Project Executive Decision-Making Board." Available: https://gta.georgia.gov/psg/article/large-it-project-executive-decision-making-board.

[56] Read more about the activities involved in these areas of support here: https://gta.georgia.gov/enterprise-portfolio-management-services.

[57] Annual State IT Report FY 2016, p. 23. (2017, January). Available: http://gta.georgia.gov/annualreport/sites/gta.georgia.gov.annualreport/files/related_files/site_page/Annual%20State%20IT%20Report%202016.pdf.

[58] Interview with Dean Johnson, Chief Operating Officer, Sourcing Management Organization, Georgia Technology Authority and Chris McClendon, Technology Services Officer, Sourcing Management Organization, Georgia Technology Authority. (2017, September 5).

[59] Ibid.

[60] Overview of the Georgia Enterprise Technology Services (GETS) Environment for Request for Proposal Respondents, p. 3. (2017, May). Available: https://gta.georgia.gov/sites/gta.georgia.gov/files/related_files/site_page/Overview%20of%20GETS%20Environment%20for%20RFP%20Respondents%2C%20May%202017.pdf.

[61] About 70 percent of executive branch agencies have been consolidated, and the remaining 30 percent that are working independently are guided and held accountable by GTA policy and standards. Interview with Dr. Steve Nichols, Chief Technology Officer, Georgia Technology Authority. (2017, August 22).
[62] Interview with Dean Johnson, Chief Operating Officer, Sourcing Management Organization, Georgia Technology Authority and Chris McClendon, Technology Services Officer, Sourcing Management Organization, Georgia Technology Authority. (2017, September 5).
[63] As of May 2017, there are four STPs: the MSI, one for managed network services, one for infrastructure services, and one for email services. Available: https://gta.georgia.gov/sites/gta.georgia.gov/files/related_files/site_page/Overview%20of%20GETS%20Environment%20for%20RFP%20Respondents%2C%20May%202017.pdf.
[64] Annual State IT Report FY 2016, p. 23. (2017, January). Available: http://gta.georgia.gov/annualreport/sites/gta.georgia.gov.annualreport/files/related_files/site_page/Annual%20State%20IT%20Report%202016.pdf.
[65] The MSI also runs the help desk and ticketing system, rolls up event management, manages the disaster recovery program, and ensures that the STPs report up in a coordinated way. Interview with Dr. Steve Nichols, Chief Technology Officer, Georgia Technology Authority. (2017, August 22).
[66] Agencies may also work with the CISO and DOAS to use non-pre-approved IT vendors. Interview with Mike Curtis, Director, Enterprise Governance and Planning, Georgia Technology Authority; Teresa Reilly, Director, Enterprise Portfolio Management Office, Georgia Technology Authority; and Nicol Bell, Information Security Analyst, Office of Information Services, Georgia Technology Authority. (2017, September 5).
[67] Sixty to 70 percent of agencies are under one or more federal regulations to protect data. The agencies are also responsible for adhering to these regulations. Interview with Dean Johnson, Chief Operating Officer, Sourcing Management Organization, Georgia Technology Authority, and Chris McClendon, Technology Services Officer, Sourcing Management Organization, Georgia Technology Authority. (2017, September 5).
[68] Interview with Dr. Steve Nichols, Chief Technology Officer, Georgia Technology Authority. (2017, August 22).
[69] The program includes "information security implementation, monitoring, threat and vulnerability management, cyber incident management, and enterprise business continuity management." Available: https://gta.georgia.gov/cyber-fusion-and-threat-information.
[70] Georgia.gov, "Incident Response and Reporting." Available: https://gta.georgia.gov/psg/article/incident-response-and-reporting.
[71] Interview with Stanton Gatewood, Chief Information Security Officer, Office of Information Security, Georgia Technology Authority. (2017, September 7).
[72] From redacted version of "State of Georgia, Georgia Technology Authority, Computer Security Incident Response & Handling Plan." Made available by GTA (2017, October 20).
[73] Ibid.
[74] Interview with Walter Tong, Director, Cyber Intelligence, Office of Information Security, Georgia Technology Authority. (2017, October 17).
[75] Cyber Storm V is coordinated by the U.S. Department of Homeland Security.
[76] Annual State IT Report FY 2016, p. 23. (2017, January). Available: http://gta.georgia.gov/annualreport/sites/gta.georgia.gov.annualreport/files/related_files/site_page/Annual%20State%20IT%20Report%202016.pdf.
[77] Georgia.gov, "Cyber Fusion and Threat Information." Available: https://gta.georgia.gov/cyber-fusion-and-threat-information.
[78] Ibid.
[79] Interview with Stanton Gatewood, Chief Information Security Officer, Office of Information Security, Georgia Technology Authority. (2017, September 7).
[80] Interview with Jeff McCord, Director, Intergovernmental Relations, Georgia Technology Authority. (2017, September 1).
[81] Georgia.gov, "A Look Ahead: Governor Deal Leads in Cyber." Available: https://gta.georgia.gov/annualreport/look-ahead-governor-deal-leads-cyber.
[82] Georgia.gov, "Georgia Cyber Innovation and Training Center." Available: http://gov.georgia.gov/sites/gov.georgia.gov/files/related_files/press_release/Georgia%20Cyber%20Innovation%20and%20Training%20Center.pdf.
[83] Georgia.gov, "Cyber center groundbreaking underscores state's leading role in cybersecurity." Available: https://gta.georgia.gov/press-releases/2017-06-20/cyber-center-groundbreaking-underscores-states-leading-role-cybersecurity.
[84] Trubey, J. Scott. "New Georgia training center in Augusta to counter cyber threats." The Atlanta Journal-Constitution, 19 June 2017. Available: http://www.myajc.com/news/local-govt--politics/new-georgia-training-center-augusta-counter-cyber-threats/rEs9KmrDuvKjdR7SFqw9hO/.
[85] Sample classes include Introduction and Basic Cybersecurity, Cybersecurity Policy Management, Cybersecurity Incident Management, and Cybersecurity Maturity. Available: https://gta.georgia.gov/georgia-cybersecurity-workforce-academy.
[86] Georgia.gov, "Cyber center groundbreaking underscores state's leading role in cybersecurity." Available: https://gta.georgia.gov/press-releases/2017-06-20/cyber-center-groundbreaking-underscores-states-leading-role-cybersecurity.
[87] Georgia.gov, "Deal announces new Georgia Cyber Innovation and Training Center." Available: https://gov.georgia.gov/press-releases/2017-01-11/deal-announces-new-georgia-cyber-innovation-and-training-center.
[88] From "GETS Sourcing Governance Overview." Made available by GTA (2017, September 6).
[89] Interview with Dean Johnson, Chief Operating Officer, Sourcing Management Organization, Georgia Technology Authority, and Chris

McClendon, Technology Services Officer, Sourcing Management Organization, Georgia Technology Authority. (2017, September 5).
[90] Ibid.
[91] Ibid.
[92] From "GETS Sourcing Governance Overview." Made available by GTA (2017, October 26).
[93] From "GETS Sourcing Governance Overview." Made available by GTA (2017, September 6).
[94] Interview with Dean Johnson, Chief Operating Officer, Sourcing Management Organization, Georgia Technology Authority, and Chris McClendon, Technology Services Officer, Sourcing Management Organization, Georgia Technology Authority. (2017, September 5).
[95] There is also an Enterprise Cybersecurity Risk Register maintained by GTA's CISO. This risk register is a log of non-GETS-related cybersecurity risks and provides a reliable picture of the state's cybersecurity posture to GTA leadership. The CISO and MSI keep in close contact about the two risk registers. Interview with Stanton Gatewood, Chief Information Security Officer, Office of Information Security, Georgia Technology Authority. (2017, September 7).
[96] "GETS Sourcing Governance Overview." Made available by GTA (2017, September 6).
[97] Ibid.
[98] Interview with Dean Johnson, Chief Operating Officer, Sourcing Management Organization, Georgia Technology Authority, and Chris McClendon, Technology Services Officer, Sourcing Management Organization, Georgia Technology Authority. (2017, September 5).
[99] Ibid.