State Cybersecurity Governance Case Studies

CROSS SITE REPORT

December 2017

Homeland Security

NASCIO
Representing Chief Information Officers of the States

Executive Summary

This report and supporting case studies identify how five states, identified by the Department of Homeland Security (DHS) and the National Association of State Chief Information Officers (NASCIO), govern cybersecurity as an enterprise-wide, strategic issue across state government and other public and private sector stakeholders in these six areas:[i]

- Strategy and planning
- Budget and acquisition
- Risk identification and mitigation
- Incident response
- Information sharing
- Workforce and education

Specifically, this report identifies trends, with supporting examples, in how Georgia, Michigan, New Jersey, Virginia, and Washington use cross-enterprise governance mechanisms (i.e., laws, policies, structures, and processes) to help prioritize, plan, and make cross-enterprise decisions about cybersecurity in each of the six areas above.

The trends and examples were included either because they were present in a majority of states studied, or because they represented a particularly unique or important mechanism shared by more than one state. The trends are not intended to be statistically generalizable beyond this report. However, they offer a window into how a subset of states that have intentionally focused on cybersecurity governance, have addressed this topic.

The following trends emerged across the states and six areas examined in the case studies.

Strategy & Planning Governance Trends

- *Authority to Set Strategy in State-Level Roles:* Laws and policies locate the authority to set cybersecurity strategy in state-level roles* (e.g., Chief Information Officer [CIO], Chief Technology Officer [CTO], Chief Information Security Officer [CISO], or Chief Security Officer [CSO]).

  *"State-level roles" refer to roles that have purview over the executive branch of state government.

- *Formal Mechanisms to Adapt Strategy:* Though guided by strategic plans, formal mechanisms are in place that allow states to evolve and address changing conditions (e.g., councils through which decision makers adjust key initiatives).

- *Formal Mechanisms for Cross-Organizational Collaboration in Strategy Development:* Formal mechanisms (e.g., commissions or boards) exist to enable collaboration across organizations in the development of strategy across

government, and between the public and private sectors.

Budget & Acquisition Governance Trends

- *Formal Mechanisms Ensure that Cybersecurity Is a Budget Priority Across Agencies:* A range of formal governance mechanisms (e.g., state-level CIO/CISO review and/or approval of agency* budgets, purchasing of centralized services) are used to ensure that cybersecurity is a budget priority across individual agencies.

  *"Agency" refers to executive branch agencies.

- *Authorities for Acquisition Approval in State-Level Roles:* For agencies, laws and policies vest acquisition approval authorities in state-level roles (e.g., CIO, CTO, CSO) to ensure that cybersecurity standards and policies are applied consistently.

Risk Identification & Mitigation Governance Trends

- *Authority for Risk Management Standards in State-Level Roles:* Authority for establishing risk management standards and policies across agencies is located in state-level roles (e.g., CISO, CSO), while risk identification and risk mitigation are shared between state-level roles and individual agencies.
- *Mechanisms Formalize Cross-Organizational Collaboration to Address Risk:* Formal bodies (e.g., committees, working groups) are developed to involve stakeholders across state-level roles, individual agencies, and, in some cases, the private sector in the risk identification and mitigation process.
- *Information Security Officer (ISO) as a Shared Service:* ISOs may be offered as a shared service by the office of the CIO or CISO for small agencies or local governments that cannot support one in-house.

Incident Response Governance Trends

- *Definitions of Incidents, Authorities, and Responsibilities:* What constitutes an incident or event and which organizations or individuals have the authority and responsibility to respond are defined in a formal incident response plan.
- *Escalation Paths Across Organizations:* Based on the nature of the incident, multiple organizations may participate in incident response, and there are clear mechanisms to escalate incident response management between agencies, CISOs/CSOs, and emergency management organizations.
- *Formal Governance Mechanisms to Involve Public and Private Sector Partners:* There are formal structures and mechanisms to include public and private sector organizations outside of state government in incident response management.

Information Sharing Governance Trends

- *Diverse Governance Structures and Mechanisms for Diverse Information Sharing Needs:* Multiple governance structures and mechanisms are used to share different types of cyber information (e.g., cyber threat indicators, cyber risk mitigation strategies) across public and private sectors.
- *Trusted Relationships Enable Information Sharing Mechanisms:* Trusted relationships, built deliberately and over time, are important for formal and informal information sharing.

Workforce & Education Governance Trend

- *Governance Structures Leverage Non-Government Organizations:* Governance structures leverage nongovernment organizations to develop a range of cybersecurity education and training programs for a broad set of users.

Overarching Takeaways

Cybersecurity is a challenge that cuts across many issues and many interdependent stakeholders. The states studied use a range of governance mechanisms to work across different public, private, academic, and nonprofit organizations, instantiating and aligning cybersecurity governance with cybersecurity priorities. These mechanisms were often developed and implemented over many years. They continue to be refined and are the result of ongoing commitment by multiple leaders from across state executive and legislative branches of government, education, and the private and not-for-profit sectors. Across the five states, governors provided leadership and commitment to this issue.

Table of Contents

Background & Methodology

This report was developed as part of a case study 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.[1]

The case studies explore cross-enterprise governance mechanisms used by states 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.

The cross site report and individual case studies are not formal evaluations. Instead, they offer trends, concepts, and approaches that may be useful to other states and organizations that face similar challenges. As this report covers a broad range of areas, each related section provides an overview of states' governance approaches, rather than detailed explorations. Additional details on the states' governance approaches can be found in the individual case studies located in the following appendices:

- Appendix A: Georgia
- Appendix B: Michigan
- Appendix C: New Jersey
- Appendix D: Virginia
- Appendix E: Washington

DHS' Office of Cybersecurity and Communications (CS&C) initiated and led 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."[2] The Homeland Security Systems Engineering and Development Institue (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 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 Governance Trends

The Challenge:

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

State Governance Trends:

- Laws and policies locate the authority to set cybersecurity strategy in state-level roles (e.g., Chief Information Officer [CIO], Chief Technology Officer [CTO], Chief Information Security Officer [CISO], or Chief Security Officer [CSO]).
- Though guided by strategic plans, formal mechanisms are in place that allow states to evolve and address changing conditions (e.g., councils through which decision makers adjust key initiatives).
- Formal mechanisms (e.g., commissions or boards) exist to enable collaboration across organizations in the development of strategy across government, and between the public and private sectors.

Section Orientation

For this and each subsequent section of the cross-site report, bolded text introduces trends. Text following the bolded text discusses the trend in more detail and provides examples from the states in the alphabetical order of the state name.

"Agency" refers to executive branch agencies. "State-level roles" refer to roles that have purview over the executive branch of state government.

States use a variety of governance mechanisms to drive cross-enterprise cybersecurity strategy and policy.

Authority to Set Strategy in State-level Roles

One mechanism common to several states was establishing in law and/or policy that authority to set cybersecurity strategy is held in a state-level role such as a as CIO or CTO. In Georgia, authority to set the cybersecurity strategy across agencies is located, by law, within the Georgia Technology Authority (GTA). GTA is led by a CIO who is also the Executive Director, includes a CTO and CISO, and is guided by a 12-member Board of Directors.[3] Additionally, Georgia created a Cybersecurity Review Board in 2015 to further support the state's development of its cybersecurity strategy and to increase the

visibility of cybersecurity as a cross-government priority. The board is chaired by the State CIO and includes three other Governor-appointed agency heads.

In Michigan, authority for strategy and policy across agencies is located, by law, within the Michigan Department of Technology Management and Budget (DTMB). It is led by a Director, who is also the CIO, and includes a CTO, CSO, and Agency Service Information Technology leads. By law, the DTMB has authority for information technology (IT) for agencies, and is responsible for coordinating and executing a unified executive branch strategic IT plan that addresses cybersecurity and aligns with statewide priorities.[4]

In New Jersey, by law, the CISO sets information security policies and standards for the state, and is charged with developing a statewide cybersecurity strategy. This responsibility is part of the CISO's overall mission to establish and manage "an information security program to ensure the confidentiality, integrity, and availability" of the executive branch's "information resources, systems, and services while promoting and protecting privacy" and "developing, implementing and monitoring the performance of the information security program."[5] The cybersecurity strategy, which was recently completed, is not publicly available as of publication of this report.

In Virginia, the Secretary of Technology, who oversees the Virginia Information Technology Agency (VITA), has the responsibility to develop the Commonwealth's strategy and planning activities, by law. Nearly all IT services from across the Commonwealth were consolidated into the VITA in 2003 through major legislation passed by the Virginia General Assembly.[6] VITA is led by a CIO, who works with a CISO to address cybersecurity issues.

In Washington, by law, the Washington Technology Solutions (WaTech) has the responsibility to create cross-government strategies and policies. In 2015, the state Office of CyberSecurity (OCS) was consolidated into Washington Technology Solutions along with all other state IT services. OCS, led by the state Chief Information Security Officer sets statewide cybersecurity strategies and planning activities.[7] Washington State's cybersecurity strategy and planning activities are led by the state's CIO and informed by the CISO.

Formal Mechanisms to Adapt Strategy

Though it is common for states to have strategic plans in place, it is also common for them to establish governance mechanisms that allow them to evolve their strategies based on shifts in leadership priorities and environmental threats. In Georgia, though the Georgia Enterprise IT Strategic Plan 2025 is a long-term plan, the state distributes an annual questionnaire to agencies, collected and analyzed through its State Technology Annual Report Register tool. The information collected through this tool, such as application inventory and data retention, is presented to the state legislature, used in annual reports, and used to update the strategic plan.[8] The information can inform adjustments to strategy, budget, and execution.

In Michigan, the DTMB is responsible for coordinating a unified executive branch strategic information technology plan.[9] However, this plan is augmented by strategic decisions made in councils that meet regularly, such as the IT Strategy Group, which meets weekly and "oversee[s] and deliver[s] all investment decisions, including the overall strategic direction of the enterprise."[10,11]

In Washington, the law directs the CIO to prepare a state strategic IT plan—the Strategic Roadmap—every two years to identify IT priorities and to enable mission delivery in securing and protecting those technologies.[12] To track progress on the impact of cybersecurity-related initiatives, the CISO publishes a biweekly cyber health report and distributes it to agencies. This health report provides a snapshot of information security measures, such as types

of attacks, and allows for ongoing adjustments to key initiatives.

Formal Mechanisms for Cross-Organizational Collaboration in Strategy Development

Another feature common to the states studied is that they often collaborate both across the government and with the private sector on setting strategy and policy. Georgia created a State Government Systems Cybersecurity Review Board to bolster cybersecurity. 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, and the Commissioner of the Department of Administrative Services.[13] Among other activities, the board provides a forum for the CISO's office and GTA to set cybersecurity priorities, and assesses and provides recommendations regarding the state's cybersecurity preparedness.

In Michigan, a CIO Kitchen Cabinet was created to bring together Michigan-based CIOs from across private industry to discuss cybersecurity topics, engage on a variety of common challenges, and share mitigation strategies. The CIO used these monthly meetings as a sounding board on topics such as the state's cybersecurity strategy and budgeting exercises.[14] The success of this initiative led to the formation of the CSO Kitchen Cabinet, as well as industry-specific councils on healthcare and finance.

To bring a cross-organizational perspective to the development of state cybersecurity strategy, New Jersey established a policy to create the Information Security Governance Committee (ISGC), an intra-governmental body co-chaired by the Director of the Office of Homeland Security and Preparedness (OHSP) and the CTO. The ISGC, which is in the process of being stood up, is intended to play a strategic role in cybersecurity issues within the state and reports to the cabinet. ISGC members include the state CISO, the state Chief Data Officer, representatives from the Department of Treasury, and other state agencies as appropriate.[15]

In Virginia, the law directs the Secretary of Technology to engage with a variety of agencies, councils, and boards in setting strategy and direction, including the Information Technology Advisory Council (ITAC).[16] The ITAC, which advises on the Commonwealth's cybersecurity strategy, includes members from both government and the private sector. The Governor also created, via Executive Order, the Virginia Cyber Security Commission, which is comprised of public and private sector cybersecurity experts.[17] These experts offered a set of recommendations in a report that has become a grounding document in the state, influencing decisions on budget, policy, and the law.[18]

In Washington, the private sector provides perspectives and input regarding strategic planning through involvement in the WaTech Technology Services Board (TSB), an oversight board to the CIO that includes members of state and local government in addition to the private sector.[19] The TSB advises the CIO on issues such as strategic vision, system governance, and quality assurance for IT projects.[20]

II. Budget & Acquisition Governance Trends

The Challenge:

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

State Governance Trends:

- A range of formal governance mechanisms (e.g., state-level CIO/CISO review and/or approval of agency budgets, purchasing of centralized services) are used to ensure that cybersecurity is a budget priority across individual agencies.
- For agencies, laws and policies vest acquisition approval authorities in state-level roles (e.g., CIO, CTO, CSO) to ensure that cybersecurity standards and policies are applied consistently.

The states explored in this study use budget and acquisition governance to drive strategic cybersecurity priorities across state agencies.

Formal Mechanisms Ensure Cybersecurity Is a Budget Priority Across Agencies

States establish formal governance mechanisms to ensure that cybersecurity is a budget priority across individual agencies. Georgia's agencies receive annual budgets. Agencies that obtain infrastructure and managed network services through GTA use a portion of their annual budgets to pay GTA for these IT services, adjusted based on their service consumption. Cybersecurity features and associated costs are built into these service charges, ensuring that security remains a priority. Out-of-cycle cybersecurity funding requests during the rest of the year are reviewed by the Cybersecurity Review Board, which is chaired by the CIO, before going to the Office of Planning and Budget (OPB) and Governor's Office for approval.

In Michigan, all executive branch IT budget requests are submitted annually to the DTMB and State Budget Office (SBO) through a centralized budget process. The DTMB CIO and SBO jointly review, evaluate, and prioritize all IT and cyber-related spending requests from state agencies to ensure that proposals align with the strategic IT plan for the state.[21,22] After evaluating all requests to ensure strategic alignment, the DTMB and SBO submit a consolidated, overall IT budget package to the legislature for funding approval. The process allows the state to operationalize cybersecurity priorities across state agencies.

In New Jersey, agencies receive an annual IT budget. Some of this budget is used to purchase

services provided by the Office of Information Technology (OIT) or OHSP. One example is a web content filtering tool provided by OIT that restricts access to certain sites, which operationalizes the state's internet user agreement policy. Additionally, funding is provided directly to OHSP for enterprise-wide cybersecurity, such as a shared firewall, prioritizing such protections.

Virginia provides state funding through an annual budget process in which agencies each receive their own IT budget, but budget requests for IT projects, including those that may introduce cyber risks to the Commonwealth's enterprise, are overseen by the CIO, with consultation from the CISO. The law directs agencies to provide the CIO with justification for IT projects, and the CIO reviews requests to ensure that the proposed IT projects align with the Commonwealth's IT strategic direction before approving or disapproving them.[23]

In Washington, each agency prepares an annual IT budget as part of the budgeting process. The CIO evaluates current IT spending and prioritizes new IT and cyber-related spending requests against portfolio-based IT management and cyber-related criteria developed by the CIO.[24] The CIO establishes priority ranking categories for the proposals based on several categories of risk and other factors, with no more than one-third of the submitted proposals ranked in the highest priority category.[25] Based on this prioritization, the CIO recommends to the Director of Washington's Office of Financial Management (OFM) to fund all or part of submitted agency IT budgets and additional IT or cyber-related budget proposals.[26] The OFM has final approval authority over the development and submission of the Governor's budget request to the state legislature. In addition, the TSB plays a role in setting the criteria and the weighting for those criteria on IT budget and planning activities.[27]

Authorities for Acquisition Approval in State-Level Roles

Another way the states drive strategic priorities is through acquisition approval authority, ensuring that cybersecurity standards and policies are applied consistently through the acquisition process. Laws and policies typically vest acquisition approval authorities in state-level roles. In Georgia, acquisition approval authority for projects costing more than one million dollars for a five-year total cost of ownership is split between OPB and GTA's Enterprise Portfolio Management Office (EPMO). By law, any technology projects over that dollar threshold must submit a formal business case and/or organizational change management plan and strategy to OPB and EPMO.[28, 29] The EPMO conducts a preliminary review, often in consultation with the CISO and GTA's Sourcing Management Organization (SMO), and shares feedback with OPB, the agency, and GTA's CTO.

In Michigan, the DTMB is responsible for, and has approval authority over, all executive branch IT acquisition activities, and the CSO's office is the lead for managing IT acquisition and implementation through an integrated approach designed to assess and manage cybersecurity risks. Michigan conducts a series of checkpoints throughout the acquisition process and system development life cycle, led by the CSO, to ensure that vendors are meeting security requirements.

In New Jersey, OIT procurement policy established procedures that apply to agency acquisition of IT hardware, software, and subscription-based services. The OIT CTO reviews and approves IT purchases exceeding $50,000, while those exceeding $100,000 must undergo OIT and Office of Management and Budget (OMB) review and approval.[30] OIT review ensures that purchases comply with statewide IT and cybersecurity policies and standards. Purchases under those thresholds do not require advance approval, but must meet

certain criteria specified in policy. OIT has the authority to conduct audits to ensure that agencies operate according to this purchasing policy.[31]

In Virginia, the CIO, in consultation with the CISO, has approval authority for agency IT projects; a process that occurs during the annual budgeting process. All agency procurements must occur through VITA, which allows the CIO to manage cybersecurity risks associated with vendor products and services and ensure strict adherence to cybersecurity standards.[32] The acquisition process is designed around strict adherence to cybersecurity standards. The bulk of IT products and services for state agencies, including cybersecurity services, are provided through a Northrop Grumman contract. The CIO manages the Northrop Grumman contract, as well as requests to purchase any goods or services outside the contract. Any outside vendors must comply with an extensive cybersecurity vetting process and contractual requirements.[33]

In Washington, the CIO reviews and approves all major IT investments.[34] The CIO determines what constitutes a major IT investment, but size of the investment and potential type and severity of risks to the state's network are always considered as part of the evaluation process.[35] In addition, the TSB, of which the CIO is the chair, plays a role in the acquisition process by reviewing major IT policy changes and providing oversight of major IT investments.

III. Risk Identification & Mitigation Governance Trends

The Challenge:

How to identify and mitigate cybersecurity risks across multiple organizations?

State Governance Trends:

- Authority for establishing risk management standards and policies across agencies is located in state-level roles (e.g., CISO, CSO), while risk identification and risk mitigation are shared between state-level roles and individual agencies.
- Formal bodies (e.g., committees, working groups) are developed to involve stakeholders across state-level roles, individual agencies, and, in some cases, the private sector in the risk identification and mitigation process.
- ISOs may be offered as a shared service by the office of the CIO or CISO for small agencies or local governments that cannot support one in-house.

The states in the case studies share several governance features related to cybersecurity risk identification and mitigation.

Authority for Risk Management Standards in State-Level Roles

Authority for establishing common risk management standards and policies is located with state-level roles such as CISOs. The authority for identification and mitigation vary from state to state, and may be shared among multiple entities including state-level roles and individual agencies. In Georgia, executive branch authority for risk management policies and standards is located within GTA. The Office of Information Security (OIS),[36] led by the CISO, is responsible for providing "statewide cyber strategic direction and leadership" and cybersecurity policy, standards, and guidelines.[37] State agencies must operate their own information security program in compliance with these policies, standards, and guidelines.[38] For risk identification and mitigation, GTA developed risk identification and mitigation bodies, including the Critical Projects Review Panel, the Large IT Project Executive Decision-Making Board, and the Cybersecurity Review Panel. These bodies,

respectively, monitor and address risks of IT investments over one million dollars, provide additional oversight to projects over 10 million dollars, and provide oversight to high-impact systems. Georgia further mitigates cybersecurity risk through its consolidated provisioning of infrastructure and managed networked services to agencies through a public-private partnership called the Georgia Enterprise Technology Services (GETS) program. GTA uses GETS 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). GETS consistently applies standards for systems and building processes across the enterprise. GETS vendors 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. GTA's SMO uses a formal sourcing governance structure to oversee the GETS service providers and their associated risks, including cybersecurity.

In Michigan, authority for executive branch risk management activity, including developing strategy and policy as well as cyber and physical risk identification and mitigation, is located within the DTMB by mandate of the Management and Budget Act, with the CSO bearing responsibility.[39] Michigan created the CSO role in 2012 in response to the increasing convergence of cyber and physical risks. Under the CSO's leadership, the DTMB develops, promulgates, and implements standardized risk management policies, practices, and programs across state agencies. The CSO's office scans networks and applications for vulnerabilities, addressing them if found. Other DTMB offices help monitor cybersecurity risks, such as the CTO's Enterprise Solution Design Services Division, which ensures that cyber risk is addressed during high-level design of new applications.[40] The CSO also validates that risks are properly mitigated before an application is deployed on the network.

In New Jersey, state cybersecurity risk identification and mitigation activities are a shared responsibility between the CISO, CTO, and state agencies. The CISO and CTO are primarily responsible for policy setting and review, while agencies are primarily responsible for implementation. The CISO establishes the overarching requirements, standards, and metrics for cybersecurity in agencies. The CISO is also responsible for developing an Information Security Governance, Risk, and Compliance program. The CTO is responsible for reviewing "all plans for any modification and/or new installation to Executive Branch information systems," including hardware, software, and IT architecture "to ensure those modifications are in alignment with the State's [IT] strategy and in compliance with enterprise architecture standards."[41] The CTO uses a System Architecture Review process to ensure that agency systems and services comply with the CISO's guidelines.

In Virginia, authority for risk strategy, identification, and mitigation across government agencies is located within VITA, with the CIO and CISO, though working groups and agencies also share responsibility for identification and mitigation. VITA developed risk management strategies "to strengthen and modernize agencies' cyber security profiles."[42] The Commonwealth Security and Risk Management (CSRM) Directorate, a unit within VITA led by the CISO, executes many CIO-related risk identification and audit activities.[43] The CSRM assesses agency IT security programs through regular security audits. If inadequate security is found, the department or agency is discouraged from beginning new IT investments until the risk is addressed, which ensures prioritization of funds to mitigate risks.

In Washington, governance for cross-organizational risk identification and mitigation is shared by the CISO and the Military

Department. The CISO focuses on risks to state networks, while the Washington Military Department focuses on risks that could impact critical infrastructure and that would require an emergency response. The OCS, which is located within the WaTech Office of the Chief Information Officer and led by the CISO, is charged with identifying and mitigating cyber risks to state government networks. The CISO, who reports to the CIO, sets information security standards for state systems and advises the Governor and state legislators on various cyber issues.[44] OCS also manages the state's Security Operations Center (SOC), conducts risk assessments, implements data controls, and determines appropriate data architectures based on risk profiles of various types of data. OCS also oversees a security design review process required for all agencies prior to adding the product or service into the shared network environment. The Washington Military Department plays a role in identifying and planning for risks that could require a coordinated emergency response.[45] The Military Department maintains the State Threat and Hazard Identification and Risk Assessment, which outlines statewide risks, emergency plans, and emergency response capabilities.

Mechanisms Formalize Cross-Organizational Collaboration to Address Risk

States recognize the need to create formal bodies of stakeholders, such as committees or working groups, with expertise or areas of focus that address various aspects of risk identification and mitigation. In Georgia, GTA's EPMO, in collaboration with state agencies, focuses on addressing risks to IT projects through project, program, and application assessments, governance support, project assurance assessments, project management support, and more.[46] When applications are created, the EPMO is involved throughout the process. The EPMO also engages the CISO's office whenever required by risk management processes, such as during vendor contracting regarding security and privacy protocols. Deployment of an application requires approval by several GTA leaders, including the CISO. Georgia also established a Critical Project Review Panel to monitor large, critical technology investments, address risks, and make decisions. The panel, comprised of state government executives, identifies and address risks early.

Michigan coordinates with stakeholders through IT governance bodies. For example, the Information Security Steering Committee includes representatives from Agency Services and two state agencies and discusses variations from cyber risk policies or processes and possible solutions. Unresolved risks can be elevated to the Enterprise Risk and Control Committee (ERCC), which includes representatives from the Governor's Office, the DTMB, and agencies outside the DTMB. The ERCC examines and resolves macro-level risks and making enterprise-wide decisions.

New Jersey established the ISGC, co-chaired by the CTO and Director of OHSP, to assist the CISO in reviewing reports of major information security incidents and noncompliance cases,[47] as well as a New Jersey Cybersecurity Communication and Integration Cell (NJCCIC) Governance Risk and Compliance Bureau (GRCB), which meets twice weekly with OIT to review all proposed new technology products and services. The GRCB reviews risks at an enterprise level to ensure that cybersecurity standards are being met. Agencies are responsible for implementing and ensuring compliance with security policies and standards on information assets they own, manage, or license. Additionally, in 2001, the legislature passed the New Jersey Domestic Security Preparedness Act, establishing the Domestic Security Preparedness Task Force (DSPTF) and the Infrastructure Advisory Committee (IAC). The DSPTF is comprised of nine public and private sector members. Their duties include identifying and assessing risks to the domestic security and well-being of the citizens of New Jersey, including disruptions to critical

infrastructure and key resources (CIKR), and they liaison with the federal Homeland Security Council.[48] The IAC members include approximately 40 representatives from the private sector, who discuss cybersecurity trends, author best practices, and act as liaison with the public and private sectors regarding domestic preparedness and the respective roles of the public and private sectors.[49]

Virginia created standing intra-governmental working groups to identify cyber risks. The Secure Commonwealth Panel (SCP), for example, is a legislatively created standing advisory group tasked with reviewing and identifying laws and policies that may need to change to address public safety and homeland security issues in the Commonwealth. By statute, the SCP consists of 36 members from the legislative and executive branches, as well as private citizens, and is chaired by the Secretary of Public Safety and Homeland Security. Recognizing the threat cyber poses to public safety, the SCP formed the Cyber Security Sub-Panel to evaluate whether to amend Virginia's laws and policies regarding cybercrime, critical infrastructure, and law enforcement. The Cyber Security Sub-Panel meets quarterly and is comprised of members of the Governor's Cabinet, Virginia's Legislature, representatives from a variety of state agencies, and private citizens. Recommendations are passed to the Secretary of Public Safety and Homeland Security and the SCP, who shares them with the Governor and, where appropriate, the General Assembly.

In Washington, the OCS is the central authority for risk identification and mitigation for state government networks, and the Washington Military Department is the central authority for risks that could impact critical infrastructure and that could require a coordinated emergency response. The Military Department coordinates with private sector owner/operators of CIKR, and developed the State of Washington Infrastructure Protection Plan in collaboration with public agencies and the private sector in 2008.[50]

Information Security Officer as a Shared Service

Another risk identification and mitigation governance mechanism shared by some states relates to meeting the cybersecurity needs of smaller entities. Both Michigan and Virginia offer CISO services to smaller agencies or local government entities through a "CISO-as-a-service" model. For entities that are not large enough to support a full-time CISO, this program offers access to CISO expertise through a shared services model. Local governments in Michigan and agencies in Virginia contract with DTMB or VITA, respectively, to obtain part-time assistance in applying cybersecurity risk management expertise to a variety of technical and operational issues. Georgia is developing a similar program. The CISO's office is creating a program through which smaller agencies can contract through the CISO's office to gain access to an Information Security Officer (ISO).

IV. Incident Response Governance Trends

The Challenge:

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

State Governance Trends:

- What constitutes an incident or event and which organizations or individuals have the authority and responsibility to respond are defined in a formal incident response plan.
- Based on the nature of the incident, multiple organizations may participate in incident response, and there are clear mechanisms to escalate incident response management between agencies, CISOs/CSOs, and emergency management organizations.
- There are formal structures and mechanisms to include public and private sector organizations outside of state government in incident response management.

Since cyber incidents may occur beyond a single network's boundary and require coordinated response, governance mechanisms in states have evolved to ensure cross-organizational engagement in incident response.

Definitions of Incidents, Authorities, and Responsibilities

States define what constitute incidents or events in their states. Once it is clear an event or incident is occurring, response is often a shared responsibility between individuals and organizations, such as the CIO/CISO and state emergency management and public safety organizations. Roles and responsibilities between these organizations are defined in formal incident response plans.

In Georgia, the Computer Security Incident Response and Handling Plan defines an IT security incident as "a violation (breach) or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices..."[51] GTA's OIS's Governance, Risk, and Consulting and Cyber divisions protect the state's infrastructure and network, developing, delivering, and maintaining the state's cybersecurity program.[52] OIS 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).[53] OIS is responsible for cyber incident management within Georgia State's government, and

GEMHSA is responsible for cybersecurity incidents extending beyond state government, such as those impacting private industry and CIKR.

The Michigan Cyber Disruption Response Strategy defines a significant cyber disruption event as "an event that is likely to cause, or is causing, harm to critical functions and services across the public and private sectors by impairing the confidentiality, integrity, or availability, of electronic information, information systems, services, or networks; and/or threaten public safety, undermine public confidence, have a negative effect on the state economy, or diminish the security posture of the state."[54] This definition establishes when incident response processes begin. The Michigan Cyber Disruption Response Plan (CDRP) uses a threat matrix to move cyber incidents along a five-level cyber escalation/de-escalation path, which is detailed in the next trend. The CIO's office manages day-to-day cyber events at levels one and two. At levels three and above, the CDRP triggers emergency processes including an Incident Command System staffed by a Cyber Disruption Response Team (CDRT). The CDRT is comprised of subject matter experts from public and private emergency management and IT fields.

In New Jersey, the newly revised 2017 cyber incident response policy and plan defines a cybersecurity incident as "any adverse event or condition that has the potential to impact the confidentiality, integrity, and availability of agency information assets."[55] The CISO is responsible for developing, maintaining, and executing the incident response plan for the state.[56] Agencies are responsible for forming in-house Cybersecurity Incident Response Teams to coordinate and carry out the department's or agency's response to incidents. The agencies operate under an incident response framework consisting of practices and tools to categorize, prioritize, communicate, track, and document incident response activities.[57] OIT and NJCCIC support the Cybersecurity Incident Response Teams.

In Virginia, VITA defines both incidents and events. An "information security incident refers to an adverse event in an information system, network, and/or workstation, or the threat of the occurrence of such an event" and "an event is any observable occurrence in a system, network, and/or workstation."[58,59] Incidents that occur on the state network and are not emergencies are handled with VITA in the lead role. By law, agency directors must report incidents to VITA within 24 hours of discovery, or from when the incident should have been discovered, where it is then categorized by VITA's Commonwealth Security Incident Response Team.[60] The VITA Computer Incident Response Team, comprised of the agency ISO and CSRM incident management staff, then coordinates response to the reported incident.[61] If the incident is deemed an emergency or impacts local or private critical infrastructure, it is managed through a Unified Command (UC) structure, led by the Virginia Department of Emergency Management (VDEM) Virginia Emergency Support Team (VEST). The cyber-specific response is led by a Cyber Unified Coordination Group (Cyber-UCG), comprised of VITA, VDEM, the Virginia State Police (VSP), the Virginia Fusion Center (VFC), and the affected entity. When the Cyber-UCG is activated, the VITA CISO is responsible for protection of Commonwealth networks, VDEM coordinates resources for response, VSP is the lead for threat response and criminal investigations, the VFC leads information dissemination, and the affected entity provides information regarding the impacted system.

In Washington, a security incident is defined in law as an accidental or intentional event resulting in "an imminent threat of the unauthorized access, loss, disclosure, modification, disruption, or destruction of communication and information resources."[62] The law requires the CIO to develop an incident

response policy to address IT security incidents posing a threat to the state's data architecture and systems.[63] Threats to the state government network are led by the CIO, in coordination with the CISO. If the Governor declares a cyber incident is significant, such as events impacting CIKR, the Washington State Homeland Security Advisor (HSA), who is also the Adjutant General of the Washington Military Department, leads the response. The HSA coordinates response with the support of the Cyber Unified Coordination Group (UCG), organized through the Washington State Emergency Operations Center (SEOC). The Cyber UCG includes members of federal, state, and local governments, academia, private industry, and critical infrastructure owners/operators.

Escalation Paths Across Organizations

The shared responsibility for incident management, where authority shifts between multiple individuals and organizations (such as from the CIO/CISO to state emergency management), is based on the incident severity and stakeholder impact, driven by incident escalation policies. In Georgia, the staff of the vendor-operated GETS help desk are trained to look for trigger words to determine whether an incident can be handled within the agency where it occurred or whether it needs to be escalated. Minor to moderate incidents affecting a small number of computers, systems, and agencies are handled by an Incident Response Team.[64] For more severe incidents, the CIO and Cybersecurity Review Board can decide to elevate response to the Governor's Office, as well as determine a plan of action. This includes GEMHSA and GTA working together to coordinate cross-ecosystem response, and it can include the involvement of the Georgia National Guard for their cybersecurity expertise and/or the use of the state's cybersecurity insurance policy for additional support.

In Michigan, the CDRP uses a threat matrix along a five-level escalation/de-escalation path, in line with the Federal Emergency Management Agency's National Incident Management System structure. At levels one and two, the CIO's office and security operations center manage cyber events. As needed, the Michigan State Police's Michigan Intelligence Operations Center (MIOC), or fusion center, can be involved. At level three, involvement by the Governor's Office, Michigan Cyber Command Center, National Guard, Cyber Civilian Corps, and Michigan SEOC, which can include nongovernment entities, is triggered. At levels three through five, a CDRT staffs an incident command system with subject matter experts from public and private emergency management and IT fields.[65] A CDRT lead is appointed to act as the incident commander once the SEOC is activated.[66] The CDRP further breaks down the roles and responsibilities of the organizations and teams operating within these structures.

The New Jersey plan provides an approach to classify incidents into one of eight categories. The plan also describes a standardized means to track incidents across the enterprise[67] and defined levels of severity. Severity helps determine the priority of an incident and resources required to address it.[68] The agency CIO, the agency ISO, or an authorized designee, acts as Incident Coordinator and, among other duties, escalates incidents to executive management as appropriate. NJCCIC provides incident response assistance for any incident that is too large for a department or agency CIRT to address, and a department or agency is required to notify NJCCIC if a data breach occurs. NJCCIC then notifies the State Police Cyber Crimes Unit and the Office of the Attorney General.[69]

In Virginia, the VITA Commonwealth Security Incident Response Team categorizes security incidents based on the type of activity. If an incident is deemed an emergency or impacts local or private critical infrastructure, the UC structure is initiated, led by the VDEM VEST, with cyber-specific response led by a scalable

Cyber-UCG. To manage an emergency response, the Governor may call on the Secretary of Public Safety and Homeland Security for additional resources, such as Department of Military Affairs and Virginia National Guard cyber expertise, or their VSP High Tech Crimes division for forensic analysis.

In Washington, if the threat is to the state government network, it is led by the CIO, in coordination with the CISO. The OCS, which reports to the CISO, is the central point of contact for security incidents for state government agencies. The OCS operates 24-7 to identify, respond to, and mitigate cyber threats. When an agency notifies the OCS of an IT security incident, the OCS staff and CISO determine corrective actions and can call in additional capabilities to assist in response. The CISO may determine that it is necessary to notify the CIO and Assistant Attorney General for the CIO, to then make determinations about public notice. If the Governor declares a significant cyber incident, it is led by the HSA. The HSA response is organized through the SEOC, where Cyber UCG members from across government and the private sector can address incident prioritization and critical resource allocation. The Governor may also activate the National Guard for incident response related to industrial control systems and supervisory control and data acquisition (SCADA) systems, of which the Washington National Guard has specialized knowledge and training.

Formal Governance Mechanisms to Involve Public and Private Sector Partners

Many states have formal mechanisms to involve public and private sector partners in incident response. These mechanisms are intended to help address incidents with significant consequences to the state overall, but that may not involve state networks. The states recognize that private industry will not only be affected, but can also provide insights into the assets involved and may even be able to lend cyber expertise.

Georgia's incident response plan accounts for incidents impacting CIKR sectors, and these entities are also involved in incident response exercises. Georgia tested its incident response plan with both public and private sector stakeholders during a week-long Cyber Storm exercise in 2016 that simulated widespread system failures and allowed participants to practice response and handoffs, and identify capability gaps.[70]

In Michigan, the CDRP was developed by members of the public and private sectors, including critical infrastructure owners and operators. Therefore, both sectors are considered in the response plan, and both are part of the response team. Michigan performs discussion-based (e.g., tabletop exercises) and operations-based (e.g., drills) exercises throughout the year to prepare for cyber incidents and to identify necessary updates for the CDRP.[71]

In Virginia, the Cyber-UCG can include private critical infrastructure partners. Additionally, the SCP includes private citizens. Agencies are required to develop and maintain IT disaster recovery and continuity plans. VITA reviews and approves these plans, and is responsible for conducting annual incident response tests. The SCP, an advisory body within Public Safety and Homeland Security (PSHS), assesses statewide prevention, response, and recovery initiatives. The SCP, whose members include the Attorney General, Lt. Governor, representatives from legislative, executive, and local government, as well as private citizens, makes recommendations to the Governor about emergency preparedness and submits annual reports on Virginia's preparedness efforts.[72]

In Washington, the Cyber UCG includes academia, private industry, and critical infrastructure owners and operators. Also, representatives from CIKR are integrated physically and virtually into the UCG during significant cyber incidents affecting CIKR sectors. OCS conducts exercises with state

agency leaders to respond to cyber-attacks and hosts training sessions with IT security professionals from across the state to stay current on the latest security tools and best practices. During incidents, if public notification of an IT security incident is required by law, the CIO may convene the Security Incident Communications Team (SICT) and authorize public notification.[73] The SICT can include the CISO, agency heads, legal counsel, law enforcement, and others. Checks and balances are built into the escalation procedures, where, for example, the CISO and Washington State Attorney General make a determination about whether a public notification is warranted and provide that determination to the CIO, who makes that decision.[74] This step ensures that the CIO considers both security and legal expertise in making the decision.

V. Information Sharing Governance Trends

The Challenge:

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

State Governance Trends:

- Multiple governance structures and mechanisms are used to share different types of cyber information (e.g., cyber threat indicators, cyber risk mitigation strategies) across public and private sectors.
- Trusted relationships, built deliberately and over time, are important for formal and informal information sharing.

Information sharing is a priority for each of the states, which recognize that different types of information provided by diverse stakeholder sets can inform changes to cyber defenses. As a result, no state has one single information sharing body or mechanism. Instead, they all have developed multiple forums through which different stakeholders can share different types of information.

Diverse Governance Structures and Mechanisms for Diverse Information Sharing Needs

States have formed different information sharing bodies to address the information needs of their diverse stakeholders in both the public and private sectors. Georgia's State Fusion Center is operated by the GBI, State Police, and GEMHSA, and GTA has several of its employees staffed there as well. The fusion center receives information from local, state, and federal partners, as well as the Multi-State Information Sharing and Analysis Center (MS-ISAC), on cyber threats to the state's critical infrastructure. Georgia also shares information through forums such as MS-ISAC, the Cybersecurity Review Board, and GTA's sourcing governance structure. MS-ISAC shares information on threats across the nation, the Cybersecurity Review Board shares information about the state's cybersecurity risk posture and landscape with state leaders, and GTA's internal sourcing governance structure provides forums for service providers and government personnel to discuss IT project cybersecurity risks and mitigations.

Michigan formed several cross-organizational information sharing platforms to address a variety of cybersecurity challenges. In addition to the Kitchen Cabinets described previously, the Cyber Advisory Council, which includes members across multiple sectors (e.g., critical infrastructure, finance, education), provides a cross-ecosystem forum for sharing information

directly with the Governor. The Council shares insights on cyber-related topics, and the Governor's Office uses this information when setting priorities for the state. Similarly, the Cyber Executive Team brings together members of the public sector (e.g., Michigan State Police, academia) with the CIO and CSO to inform DTMB decisions on budgeting and regional training. The DTMB and Michigan State Police regularly coordinate through the MIOC to share information statewide with local, state, federal, and private sector partners. Also, the state participates in MS-ISAC, which it uses to gather and share information on nationwide cyber threats and incident response training.[75]

In New Jersey, the central cybersecurity Information Sharing and Analysis Organization (ISAO) is the NJCCIC, which is located at the State Police-operated Regional Operations Intelligence Center (ROIC) and serves as the state's fusion center and emergency operations center.[76] The NJCCIC is comprised of the OHSP, Office of the Attorney General, Division of State Police, OIT, and local, county, federal, and private sector partners.[77] Stakeholders receiving and sharing information through the NJCCIC include more than 39 states, 42 federal agencies, state executive agencies, local governments, 13 international countries, private sector companies, and other information sharing groups such as the Financial Services Information Sharing and Analysis Center (FS-ISAC). In addition to the NJCCIC, New Jersey established the DSPTF and IAC to serve as resources for risk mitigation as well as information sharing forums. The DSPTF, comprised of nine public and private sector members, raises issues related to domestic preparedness and cybersecurity matters,[78] and shares information with the federal Homeland Security Council.[79] The IAC, co-chaired by the Director of IAC and a representative from the private sector, and comprised of approximately 40 private sector stakeholders, discusses cybersecurity trends, best practices, and guidelines.[80]

In Virginia, to support information sharing about a broad range of cybersecurity operational issues at the agency levels, the VITA CSRM conducts monthly Information Security Officers Advisory Group meetings, which provide security training and facilitate knowledge exchange. The state shares cyber intelligence information with agencies and state law enforcement, in addition to federal partners, through VITA's Commonwealth Security Incident Response Team. The PSHS VFC collects, analyzes, and shares cyber threat information with state, local, and federal governments, as well as private sector partners. The Virginia Cyber Security Partnership, a partnership between the Federal Bureau of Investigation (FBI), VITA, and private companies, shares a broad range of cybersecurity information with the private sector.[81] Additionally, Virginia is in the process of forming the first state-level ISAO to enhance voluntary sharing of critical cybersecurity threat information across government and industry.[82]

In Washington, the OCS SOC gathers threat information from monitoring state networks and engaging with MS-ISAC, DHS the National Cybersecurity and Integration Center (NCCIC), and the Cyber Incident Response Coalition and Analysis Sharing regional information sharing body. The SOC then communicates this information to SLTT representatives and critical infrastructure partners. The Washington State Fusion Center (WSFC) leverages the Homeland Security Information Network to gather incident-related information and organizes that information into alerts and notifications. Those communications then emanate from the Cyber UCG, NCCIC, and the Seattle FBI Joint Cyber Task Force.[83] The WSFC also engages with the SEOC, cyber stakeholders, and other national homeland security fusion center cyber programs. Finally, Washington is also working on developing a state-level Information Sharing and Analysis Center (ISAC). It would provide actionable threat information to SLTT partners

and focus on the regional Washington environment.[84]

Trusted Relationships Enable Information Sharing Mechanisms

Trusted relationships, which are often built deliberately and over time, are important for information sharing. In Michigan, the Chief of Staff to the CIO noted that information sharing relationships evolve, and that "over time, relationships and trust were built with partners across government, private, academia, etc., to a point where communication and partnership are part of the fabric of how [the state of Michigan approaches cybersecurity]."[85] The value of informal networks was stressed as being of particular importance. According to Michigan's CTO, when information sharing is motivated by personal interest and passion, it frequently becomes the "most sustaining because it's the most authentic."[86] In Washington, the CTO describes the security achieved through information sharing as "all about building trust relationships," and says that those "relationships need to be in place before they are needed."[87]

VI. Workforce & Education Governance Trends

The Challenge:

How do states work across multiple organizations to shape responses to cybersecurity workforce shortages and education needs?

State Governance Trends:

- Governance structures leverage nongovernment organizations to develop a range of cybersecurity education and training programs for a broad set of users.

Cybersecurity education and workforce development is a responsibility shared across government, academia, and industry. These stakeholders recognize that there is a gap between the cyber skills of the population and the cybersecurity workforce needs of the state.

Governance Structures Leverage Non-Government Organizations

Nongovernment organizations can offer a range of cybersecurity education and training programs to fill the cyber skill gap, addressing the needs of a broad set of users ranging from high school through the current workforce. Governance structures leverage these nongovernment organizations to address cybersecurity education and workforce needs within the state. Georgia, through the funding of a facility and formalization of partnerships, established the governance through which a cybersecurity innovation facility could be built. In June 2017, Georgia broke ground on the Hull McKnight Georgia Cyber Innovation and Training Center in Augusta. Georgia partnered, through a memorandum of understanding, with Augusta University to provide day-to-day facility operations.[88] Additional partnerships were formed with a variety of entities to develop the center, including the University System of Georgia, the Technical College System of Georgia, local school systems, the Georgia National Guard, GBI, federal agencies, and private corporations. The center will house a cyber range, training facility, and cybercrime lab.[89] Training will range from industry-standard certifications to university degrees.[90] The facility will also house Georgia's Cybersecurity Workforce Academy, through which GTA's OIS

provides cybersecurity awareness, training, and education to agency ISOs.[91] The Hull McKnight Georgia Cyber Innovation and Training Center is slated to open in summer 2018.

Michigan, through grants and sponsorship, partnered with Merit, a not-for-profit organization governed by Michigan's public universities,[92] to create the Michigan Cyber Range (MCR) in 2012. The MCR was the first unclassified network-accessible range in the United States. It provides a space for product development and testing, as well as online and classroom cybersecurity education and training. Michigan's partnership with Merit and support for the MCR facilitates numerous cybersecurity education programs. Merit partnered directly with Pinckney Community High School to act as one of the MCR's hubs, or extensions, offering college credits for high school students as well as certification opportunities for high school students, college students, and tech professionals.[93] Additionally, Merit operates the "Governor's High School Cyber Challenge," a multi-round online cybersecurity competition for teams of high school students. Teams that make it to the final round receive an expense-paid trip to the North American International Cyber Summit in Detroit for the final round of the competition.[94] Also, MCR's Regional Cybersecurity Education Collaboration, a self-funded collaboration between the higher education community and private sector partners, provides university curriculums via distance learning to train individuals without access to a physical hub.[95]

In 2016, Virginia partnered with higher education institutions and provided funding to create the Virginia Cyber Range, with Virginia Tech serving as the coordinating entity.[96] The Virginia Cyber Range is a virtual, cloud-based environment that offers courses providing teachers from high schools, colleges, and universities with access to standardized lessons and the ability to host cybersecurity labs and exercises for students.[97] The Virginia Cyber Range is designed to support Virginia's high schools, colleges, and universities, and is led by an executive committee comprised of representatives from Virginia's higher education institutions, which are nationally recognized centers of academic excellence in cybersecurity.[98] The Virginia Cyber Range offers courses, labs, and exercises for use in high schools across the state.[99]

In Washington, the government formed a public-private partnership with the Washington Technology Industry Association (WTIA) to launch Apprenti, an apprenticeship program that trains existing workers to quality for IT and cyber-related jobs. The WTIA manages and operates the apprenticeship program. Working closely with private technology and communications companies, which form the membership of the WTIA, the Apprenti program is able to respond quickly to changes in market demands based on the inputs of its members.[100] Applicants accepted into the Apprenti program receive certification in occupations such as database administrator, network security administrator, or IT support professional.[101] Apprentices are hired by a partner company prior to beginning classroom training, receive a salary and benefits, and learn on the job. At the end of the one-year apprenticeship program, the apprentice may retain a position with the employer at an entry-level market wage for that job.

VII. Related Secondary Studies

Overview

The case study development team reviewed secondary studies that addressed the issue of cyber governance.[102] The National Association of State Chief Information Officers (NASCIO), the IBM Center for the Business of Government, and the Pell Center for International Relations and Public Policy published studies over the past few years about a variety of cybersecurity topics, including state cybersecurity governance. This summary identifies findings from these studies that relate to this Department of Homeland Security (DHS)-NASCIO cross site report and the underlying case studies (hereafter referred to as this DHS-NASCIO Report).

- *Deloitte-NASCIO Study*

  In 2016, NASCIO partnered with Deloitte to survey Chief Information Security Officers (CISOs) from 49 states and territories about the status of cybersecurity in their states. Participants "answered 59 questions designed to characterize the enterprise-level strategy, governance, and operation of security programs."[103]

- *IBM Center for the Business of Government Study*

  The 2010 IBM study, which conducted surveys and interviews of CISOs from 25 states, focused on the strategies and activities state CISOs use "to establish their credibility and implement policies."[104]

- *Pell Center for International Relations and Public Policy Study*

  The 2015 Pell study used open source data and interviews to analyze state cybersecurity strategic plans, incident response plans, the role of law enforcement and cybercrime, information sharing and education, and cyber capacity building across eight states (California, Maryland, Michigan, New Jersey, New York, Texas, Virginia, and Washington). The study summarized efforts by all eight states to "improve their cybersecurity posture and promote the development and expansion of their cybersecurity industry and talent pool."[105]

Governance as Priority

The 2016 Deloitte-NASCIO study found responding CISOs focused "on areas where they can take proactive steps to better manage risks,"[106] with 29 percent [of respondents] citing "governance (e.g., roles, reporting structures, and directives)" as a top cybersecurity initiative in 2016.[107] CISOs named, in order of priority, training and awareness, monitoring and security operations centers, strategy development, governance, and operationalizing cybersecurity among the top cybersecurity initiatives.

This finding is supported by this DHS-NASCIO Report, which found that governance was a clear priority in the states studied. However, these states demonstrate that developing cybersecurity governance is not accomplished in a single year, and have taken many steps over

several years to build their governance structures.

Addressing Governance Challenges

The Deloitte-NASCIO study noted governance was a challenge because "most states' security functions use a largely federated model of governance."[108] The term "federated" refers to an information technology (IT) structure whereby government agencies retain some level of autonomy and IT functions are generally partially decentralized in the state. For example, the study found CISOs face "challenges in operationalizing state-wide identity and access management implementations [when operating] in a federated governance model."[109] To overcome these challenges, the study concluded the CISO role needs to be elevated, in part, to exert more authority and influence within the state organizational construct. The study also found CISOs need to clearly articulate and communicate cyber risks "to better inform agency business executives and help promote their agendas."[110]

The 2010 IBM study found "centralization of networks and data centers is particularly helpful with cybersecurity efforts aimed at the protection of hardware, systems, and data."[111]

The findings from the Deloitte-NASCIO and IBM studies are generally supported across the five states explored in this DHS-NASCIO Report. Each state has taken discrete steps to define authorities that allow state-level roles (e.g., Chief Information Officers [CIOs], CISOs) to address a range of cross-agency cybersecurity issues and challenges.

Relationship between Strategy and Resources

The Deloitte-NASCIO study also found a lack of sufficient funding was "the most significant challenge" in 2016.[112] However, CISOs responded that, when they develop cybersecurity strategies and get them approved, they can overcome budget and staff challenges.

This DHS-NASCIO Report did not attempt to correlate the presence of a strategy with changes in resource levels. However, each state has developed a cybersecurity strategy or plan and incorporates cybersecurity funding requests into the state budget process. Additionally, in the states that have finalized their plans, those plans inform cybersecurity-related funding requests. Finally, CISOs, CIOs, Chief Security Officers, and/or Chief Technology Officers often play a formal or informal role in approving and/or reviewing cybersecurity funding requests as part of the annual budget cycle.

Use of Multiple Governance Structures to Connect Across Organizations

The IBM study found state CISOs build "knowledge networks…both internal to their states (intra-organizational) and across levels of government and sectors (inter-organizational)" and "are spending significant time coordinating groups of IT staff from agencies within their states.[113]

Five years later, the Pell study found some states create "formal or informal commissions, committees, task forces, and working groups to promote the exchange of information among key stakeholders; examine gaps in the states' cybersecurity posture; and make important recommendations to improve the states' preparedness, mitigation, response, and resilience capabilities."[114]

The Deloitte-NASCIO study goes further, noting "collaboration across state lines and with federal agencies is also part of respondents' strategies, and it is an important means of sharing practices for addressing cybersecurity challenges."[115] The Deloitte-NASCIO study found nearly all CISOs surveyed are "collaborating with the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the United States Department of Homeland Security (DHS) fusion centers."[116]

These findings are supported across this DHS-NASCIO Report. The states adopted formal

mechanisms (e.g., councils, committees) for cross-organizational collaboration in strategy development and to address changing conditions through which decision makers adjust key initiatives. Also, all the states profiled use multiple governance structures and mechanisms to share different types of cyber information (e.g., cyber threat indicators, cyber risk mitigation strategies) across public and private sectors. Additionally, states use trusted relationships and informal communication channels inside and outside government to share information. Finally, all states are actively involved with MS-ISAC and participate in information sharing with federal (e.g., DHS, Federal Bureau of Investigation), state, and local partners.

Conclusion

Several findings from secondary sources—Deloitte-NASCIO, IBM Center for the Business of Government, and the Pell Center for International Relations and Public Policy—support the concepts discussed across the five states examined in this DHS-NASCIO Report, which adds to the body of knowledge about cybersecurity governance. By detailing the specific mechanisms used by the states, as well as addressing some areas not covered in all the previous reports (e.g., acquisition, workforce development), this DHS-NASCIO Report offers concepts and approaches that may be useful to other states and organizations that face similar challenges.

VIII. Acronyms

Acronym	Definition
CDRP	Cyber Disruption Response Plan
CDRT	Cyber Disruption Response Team
CIKR	Critical Infrastructure and Key Resources
CIO	Chief Information Officer
CIRT	Computer Incident Response Team
CISO	Chief Information Security Officer
CS&C	Cybersecurity and Communications
CSO	Chief Security Officer
CSRM	Commonwealth Security and Risk Management
CTO	Chief Technology Officer
Cyber-UCG	Cyber Unified Coordination Group
DHS	Department of Homeland Security
DSPTF	Domestic Security Preparedness Task Force
DTMB	Department of Technology Management and Budget
EPMO	Enterprise Portfolio Management Office
ERCC	Enterprise Risk and Control Committee
FBI	Federal Bureau of Investigation
FS-ISAC	Financial Services Information Sharing and Analysis Center
GBI	Georgia Bureau of Investigation
GEMHSA	Georgia Emergency Management & Homeland Security Agency
GETS	Georgia Enterprise Technology Services
GRCB	Governance Risk and Compliance Bureau
GTA	Georgia Technology Authority
HSA	Homeland Security Advisor
HSSEDI	Homeland Security Systems Engineering
IAC	Infrastructure Advisory Committee
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
ISGC	Information Security Governance Committee
ISO	Information Security Officer
IT	Information Technology
ITAC	Information Technology Advisory Council
MCR	Michigan Cyber Range
MIOC	Michigan Intelligence Operations Center
MS-ISAC	Multi-State Information Sharing and Analysis Center
NASCIO	National Association of State Chief Information Officers
NCCIC	National Cybersecurity and Integration Center
NJCCIC	New Jersey Cybersecurity Communication and Integration Cell
OCS	Office of CyberSecurity

Acronym	Definition
OFM	Office of Financial Management
OHSP	Office of Homeland Security and Preparedness
OIS	Office of Information Security
OIT	Office of Information Technology
OMB	Office of Management and Budget
OPB	Office of Planning and Budget
PSHS	Public Safety and Homeland Security
ROIC	Regional Operations Intelligence Center
SBO	State Budget Office
SCADA	Supervisory Control and Data Acquisition
SCP	Secure Commonwealth Panel
SEOC	State Emergency Operations Center
SICT	Security Incident Communications Team
SLTT	State, Local, Tribal & Territorial
SMO	Sourcing Management Organization
SOC	Security Operations Center
TSB	Technology Services Board
UC	Unified Command
UCG	Unified Coordination Group
VDEM	Virginia Department of Emergency Management
VEST	Virginia Emergency Support Team
VFC	Virginia Fusion Center
VITA	Virginia Information Technology Agency
VSP	Virginia State Police
WaTech	Washington Technology Solutions
WSFC	Washington State Fusion Center
WTIA	Washington Technology Industry Association

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[117,118,119]

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[120]
- 29 public universities[121]
- 62 private colleges[122]

KEY INDUSTRIES:[123]

- 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.[124]

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 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."[125] 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,[126] and is a major hub for FinTech and Health IT industries,[127] 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.[128]) 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.[129] Training will range from information security industry-standard certifications to university degrees from bachelor's degrees through doctorates.[130] The center will also house Georgia's Cybersecurity Workforce Academy,[131] 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."[132] 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.[133]

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."[134] 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."[135] GTA is led by an Executive Director and State Chief Information Officer (CIO), Calvin Rhodes, and guided by a 12-member Board of Directors.[136]

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[137] 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.[138]

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.[139]

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.[140] 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.[141] 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.[142] 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"[143] 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.[144]

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)[145], and the Commissioner of the Department of Administrative Services (DOAS).[146] 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"[147] based on National Institute of Standards and Technology (NIST) and Federal Information Processing Standard (FIPS) 199-200 standards.[148] 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."[149] 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.[150] 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."[151]

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.[152] 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.[153] 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.[154] 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."[155] 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).[156]

In its role of "assuring that critical enterprise technology initiatives deliver on their promises and objectives,"[157] 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.[158,159] 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[160] 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.[161] 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[162] through IT policies, standards, and guidelines, plus a variety of review mechanisms. Its OIS,[163] 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.[164] OIS operates similarly to a central information security program as defined by NIST, Special Publication 800-12.[165] 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.[166]

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.[167] 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.[168,169] 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.[170] The board has one permanent, voting board member from GTA, OPB, and DOAS, respectively, with two additional members from the agency managing the project.[171] 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.[172]

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.[173] 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."[174]

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;[175] 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."[176] The GETS model of IT-as-a-service is consumption-based,[177] 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"[178] and "security underpins everything that is done in the GETS environment."[179] 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),[180] 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"[181] to state agencies (with approximately 40,000 end users); and serve as a coordination point for the state's security program.[182] 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.[183] All vendors are contractually responsible for complying with GTA's policies, technical requirements, and standards.[184] 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."[185]

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.[186] 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).[187] 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.[188] 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."[189] The IRT is led by the GTA ISO and includes members from the agency encountering the incident, OIS, GETS, law enforcement, legal, communications, etc.[190]

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.[191]

Georgia tested its incident response plan with a variety of government and private entities in the weeklong 2016 Cyber Storm V national cybersecurity exercise[192] 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.[193]

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.[194] Stakeholders include local governments using the Homeland Security

Information Network, local and state law enforcement, federal partners, and private industry.[195]

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.[196]

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."[197]

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."[198] Augusta University will manage the day-to-day operations through a memorandum of understanding with GTA.[199]

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.[200] Training will range from information security industry-standard certifications to university degrees from bachelor's degrees through doctorates.[201] 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,[202] 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.[203] 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."[204]

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

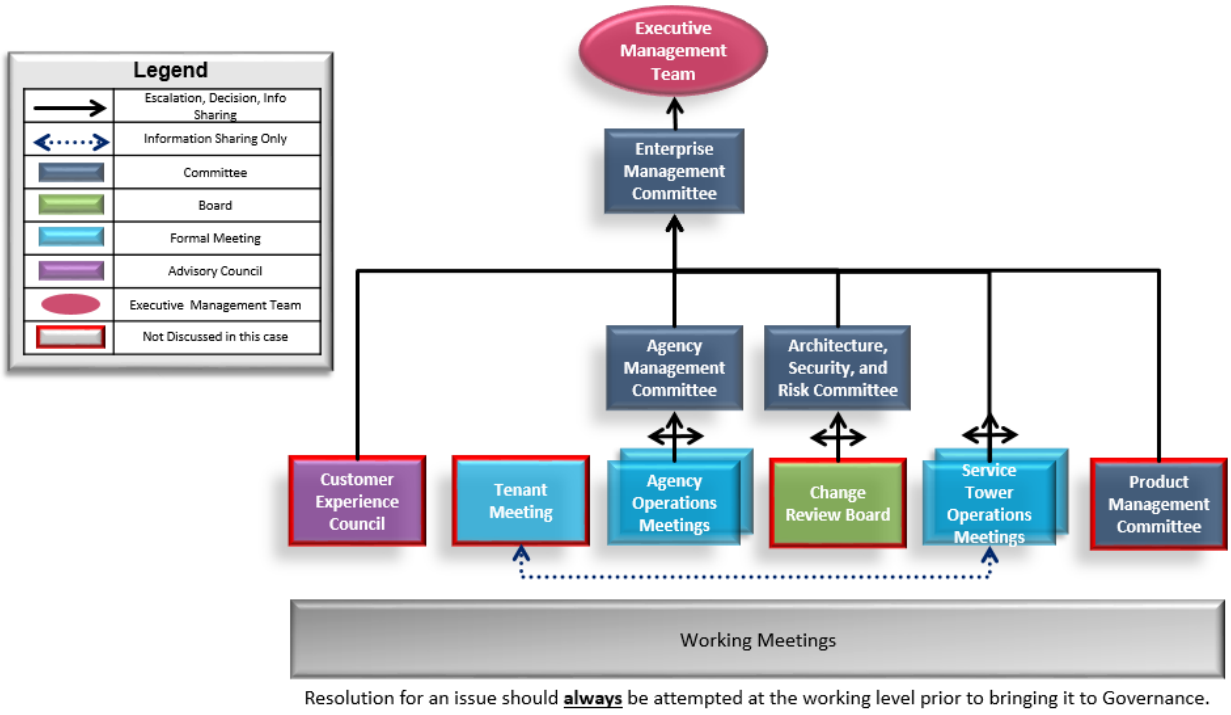
Large organizations with vast IT operations face challenges in managing cybersecurity risk, in part due to confusing decision points, unclear decision-making authority, and undocumented escalation paths. Identifying and mitigating cybersecurity risk happens across the enterprise performance life cycle, 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.[205]

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.[206] 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.207 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."[208]



* 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[209]

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[210] 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.[211] 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.[212] 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.[213] 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.[214] 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.[215]

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."[216]

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

Cybersecurity Governance in the State of Michigan

A CASE STUDY

December 2017

Homeland Security

NASCIO
Representing Chief Information Officers of the States

Michigan State Fast Facts[217,218,219]

ELECTED OFFICIALS:

- Governor Rick Snyder
- Michigan House of Representatives: 110 Representatives
- Michigan State Senate: 38 Senators

STATE CYBERSECURITY EXECUTIVES:

- Chief Information Officer (CIO) David DeVries
- Chief Security Officer (CSO) Rajiv Das
- Chief Technology Officer (CTO) Rod Davenport

STATE DEMOGRAPHICS:

- Population: 9,886,095
- Workforce in "computers and math" occupations: 2.1%

EDUCATION:

- Public with a high school diploma: 54.4%
- Public with an advanced degree: 34.5%

COLLEGES AND UNIVERSITIES:

- 33 community colleges[220]
- 15 public universities[221]
- 54 private colleges[222]

KEY INDUSTRIES:[223]

- Manufacturing
- Agri-business
- Cybersecurity
- Defense
- Information Technology

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 Michigan'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 Michigan 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 Michigan 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.[224]

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 Michigan's governance approach, rather than a detailed exploration. Individual states and organizations seeking greater detail would likely need to engage directly with Michigan to better understand how to tailor solutions to their specific circumstances.

Since the early 2000s, the state of Michigan executive and legislative branches have taken a series of deliberate steps to enable cybersecurity to be governed as an enterprise-wide strategic issue both across state government and across a diverse set of public and private sector stakeholders. As former Michigan Department of Technology Management and Budget (DTMB) Director and Chief Information Officer (CIO) David Behen said, "The focus is state of Michigan cybersecurity, not [just] the state of Michigan government's cybersecurity."[225]

The state of Michigan government governs information technology (IT) through a centralized structure, which enables a unified and coordinated approach to cybersecurity across the executive branch. Under Michigan law, the DTMB has authority for IT, including cybersecurity, management, and budget operations, for all state departments and agencies. (In this case study, "agency" refers to executive branch agencies.) The DTMB is led by a Director who is also the CIO.[226] Under the direction of this single Director and CIO, Chief Technology Officer (CTO), Chief Security Officer (CSO), and Agency Service Information Technology leads, the DTMB is responsible for coordinating and executing a unified executive branch strategic IT plan, which includes cybersecurity and aligns with overall statewide management and budget priorities.

Michigan also utilizes a range of governance structures and processes to address a variety of cybersecurity challenges that require collaboration and coordination across public and private stakeholders. For example, Michigan has established a cross-ecosystem governance approach to managing cyber incident response. Working collaboratively with federal, state, local, and private sector organizations, leaders from the Cyber Security Infrastructure Protection Division of the DTMB and the Emergency Management and Homeland Security Division of the Michigan State Police developed the Cyber Disruption Response Plan (CDRP). The CDRP provides a framework for emergency management and IT agencies to identify cyber threats and coordinate cyber response and recovery operations. The plan uses a threat matrix that considers cyber events along a five-level escalation/de-escalation path and articulates which organization is responsible for the cyber response management at each level. Stakeholders across the ecosystem rely on consistent, informal communications, in combination with formal communication lines, to stay prepared for cyber disruptions.[227]

Information sharing has also played a critical role in connecting a cybersecurity ecosystem of public and private sector stakeholders. This started as a grassroots effort by the Governor's and CIO's offices to reach out across stakeholders and ask for input. The initiative has evolved into an intentional set of formal and informal communication governance mechanisms to solve problems at strategic, operational, and tactical levels. "Over time, relationships and trust were built with partners across government, private, academia, etc., to a point where communication and partnership are part of the fabric of how [the state of Michigan approaches cybersecurity]," Ashley Gelisse, the Chief of Staff to the CIO, said.[228]

To strengthen the cyber workforce, Michigan called on a governance approach developed by Michigan's education community. Specifically, it utilized Merit Network[229] (Merit), a consortium of 300+ members, including Michigan's public universities, K-12 schools, libraries, local government agencies, and not-for-profits. Merit led the effort to build the Michigan Cyber Range (MCR), an unclassified virtual private training cloud that can be used for hands-on adaptive training and certification in cybersecurity and IT as well as product development and testing. The MCR also provides a controlled environment to perform a variety of simulations and testing, including running attack scenarios, applying responses, and analyzing the effect on a network without putting an organization or network at risk. The MCR services can be accessed through a virtual connection or at a physical extension of the MCR called a hub.

Cybersecurity is a challenge that cuts across many issues and many interdependent stakeholders. Therefore, Michigan uses a range of governance mechanisms to work across different public, private, academic and nonprofit 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. Governor Rick Snyder made cybersecurity a top priority. He and others in the executive branch agencies, state legislature, and private organizations addressed cybersecurity as important from both a threat mitigation and economic development perspective. However, leadership was not everything. Protecting data and critical infrastructure across the state, not just in state-run systems, required engagement and partnership across the entire cybersecurity ecosystem. In Michigan, tangible laws, policies, structures, and processes instantiated and aligned cybersecurity governance with broader cybersecurity priorities

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.[230]

The case study explores cross-enterprise governance mechanisms used by Michigan 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 Michigan's governance approach, rather than a detailed exploration. Individual states and organizations seeking greater detail would likely need to engage directly with Michigan 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."[231] 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 Michigan's Governance Approach:

- The Governor developed an overarching strategy to focus and frame how the state would address cyber risks.
- The Department of Technology Management and Budget (DTMB) Director/Chief Information Officer (CIO) develops a statewide strategic information technology (IT) plan that sets direction for how the state government will use and secure technology.
- The state has established a formal governance structure to execute its strategic IT plan.

In 2011, Governor Snyder developed the *2011 Michigan Cyber Initiative*, the state's plan to defend against cyber attacks and position the state to benefit economically from the cybersecurity industry. This Cyber Initiative was an action plan that emphasized Michigan's commitment to cybersecurity and identified actions the state would take to protect Michigan's citizens, infrastructure, and economy. These actions included creating a State Police-run cyber emergency command center, launching a Cyber Defense Response Team, building partnerships with the private sector, and focusing on expanding online and classroom training to target students from preschool through age 20.[232, 233]

Building on this effort, four years later Governor Snyder announced the *2015 Michigan Cyber Initiative*, which articulated Michigan's cybersecurity approach as "…a holistic and continuously evolving concept" that is about more than just technology.[234] This initiative highlighted successes since 2011 (e.g., brought physical security and cybersecurity under one Chief Security Officer [CSO], launched the Michigan Cyber Range, hosted and participated in number of cyber response and recovery exercises). It also laid out a series of next steps to advance cybersecurity over the next four years across areas such as education, workforce development, and incident response. Examples include continuing to evolve the state's approach to cyber incident response by advancing its cyber disruption plan and "transition[ing] from a compliance-centric approach to cybersecurity to a risk-based approach."[235]

Both initiatives served as guiding documents with sets of specific actions emphasizing that cyber work should be approached as a whole-of-state challenge that requires engagement both across state government and across a larger ecosystem of public and private organizations.

Across state government, setting cybersecurity priorities falls to the Department of Technology Management and Budget (DTMB). The DTMB is

responsible for coordinating a "unified executive branch strategic information technology plan" and managing cybersecurity risks to state technology systems.[236] Figure 1 provides an organizational chart for the DTMB.

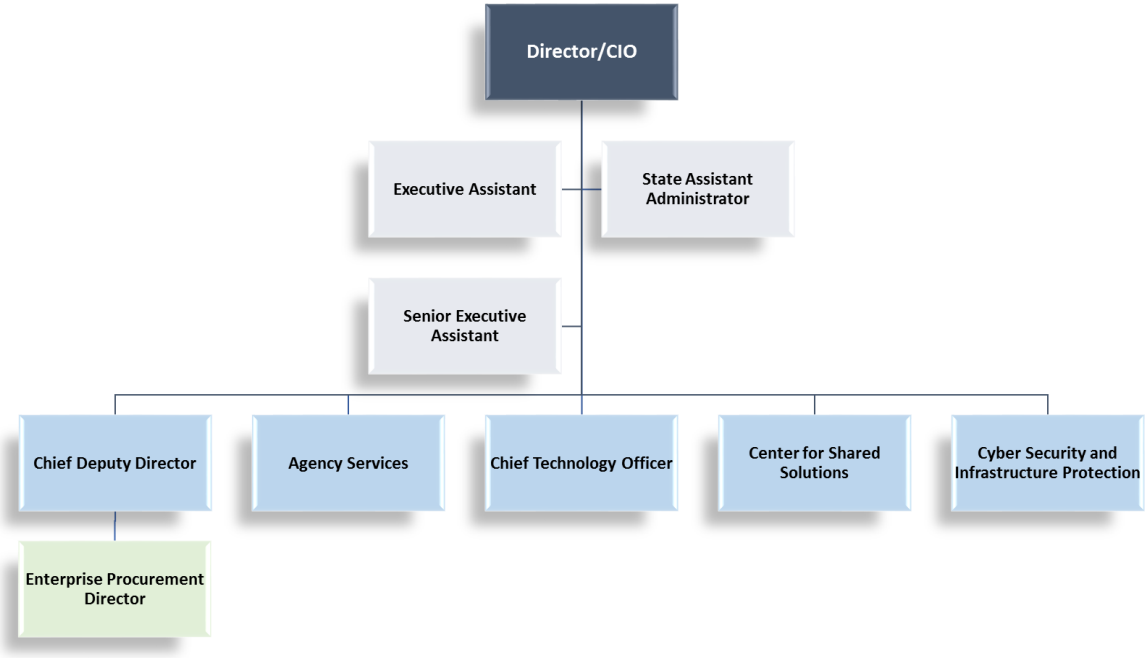


Figure 1. DTMB Organizational Chart

The DTMB utilizes a variety of cross-organizational governance bodies to execute the strategic direction. During 2017, the DTMB rolled out an information technology (IT) governance model informed by industry practices. Figure 2 shows a portion of this model; the remaining elements are shown in Figure 3 in the Risk Identification and Mitigation section.

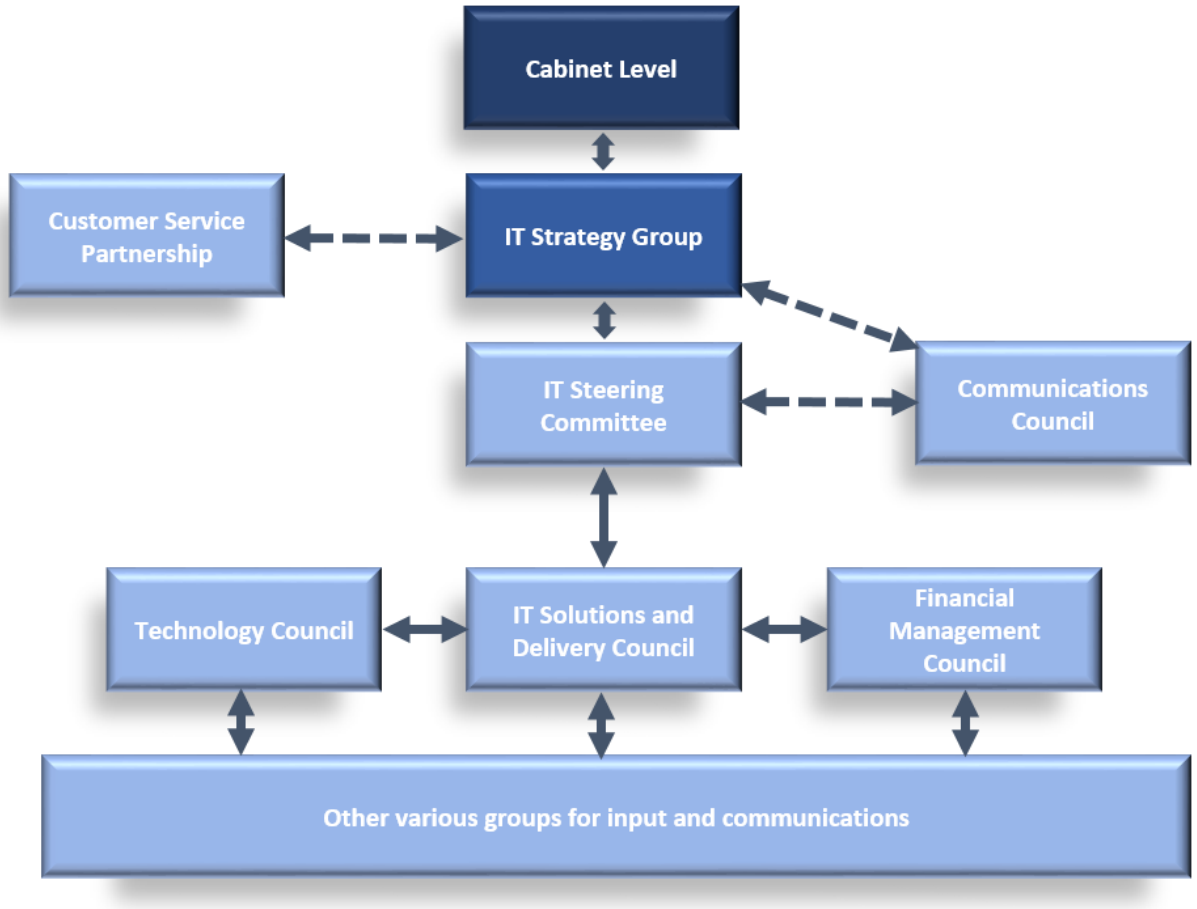


Figure 2. Portion of DTMB Governance Model

(See Figure 3 in the Risk Identification and Mitigation section for the complete DTMB Governance Model. The Customer Service Partnership is not discussed in this case.)

At the top of this model sits the *Cabinet Level* body, which is composed of various cabinet members, members from the Governor's Office, DTMB Director, and Deputy Director. It sets business strategy and vision and ensures that internal decisions are aligned with the direction it sets. These types of enterprise-level governance bodies allow the state to take a systematic view of IT decisions and risks across the state network, better define processes, and create consistent lines of decision making.

Below this body is the *IT Strategy Group*. This group consists of the DTMB leadership (i.e., CIO, CTO, CSO, Director of Agency Services, Chief of Staff, Legislative Liaison and Policy Advisor, Director of the Center for Shared Solutions, and Enterprise Procurement Director). It meets weekly to "oversee and deliver all investment decisions, including the overall strategic direction of the enterprise,"[237] align specific strategies (e.g., cybersecurity, cloud, and mobile) with timelines and metrics, and "[ensure] that technology services deliver business value."[238]

Below the IT Strategy Group are five specialized councils with participation from groups across the DTMB which conduct analysis, provide recommendations, and make decisions for their areas of responsibility. One of these councils, the IT Steering Committee,[239] performs/delegates analysis for the IT Strategy Group, makes policy decisions, approves/decides IT standards, collaborates to develop an annual project plan, and works with

leadership to establish metrics for the enterprise-wide IT budget, among other responsibilities.[240] The other four specialized councils share information up to and receive direction and information from the IT Steering Committee:

- The *Technology Council*[241] reviews new technology requests from the DTMB and the agencies by assessing total cost of operation and associated risks, including cybersecurity risks, from an enterprise perspective.[242]
- The *IT Solutions and Delivery Council*[243] makes recommendations to the IT Steering Committee based on group feedback, receives directives from the IT Steering Committee, serves as an entry point for operational governance, reviews hardware/software life cycle management, maintenance, and updates,[244] and has authority to decide how agencies implement IT solutions.
- The *Financial Management Council*[245] "work[s] with the IT Steering Committee to ensure effective and efficient use of [Michigan] financial resources and that submitted proposals are consistent with enterprise financial and technological strategy."[246]
- The *Communications Council*[247] keeps governance functioning within Michigan by providing administration guidance across the governance bodies to ensure operational consistency and gives advice and the tools necessary to effectively communicate information among the bodies.[248] It meets weekly.

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 Michigan's Governance Approach:

- The CIO and State Budget Office evaluate IT and cyber-related spending requests across state agencies and make recommendations to the legislature for approval.
- The CSO is responsible for the IT acquisition approach used to evaluate and manage risks associated with proposed IT acquisitions across state agencies.

State law creates a centralized budget process through which IT budget requests for the executive branch are submitted annually to the DTMB and State Budget Office (SBO). This process serves as one way the state operationalizes cybersecurity priorities across state agencies.[249] The DTMB CIO and SBO jointly evaluate all IT and cyber-related spending requests from state agencies to ensure proposals put forth for funding consideration "… fit into the overall strategic information technology management plan of the state and that provide a reasonable return on investment."[250] An agency's annual budget includes money to put toward a shared service model in which the CIO's office provides IT services, including cybersecurity, to the agencies, and those agencies pay for the services with funds allocated to them from the annual IT budget or a discretionary budget line available for IT and non-IT related expenses. The DTMB and SBO consolidate requests and submit an overall IT budget package to the legislature for ultimate funding approval.

Consistent with its role in the centralized budget process, the DTMB is also responsible for all IT acquisition activities. Michigan's IT acquisition is managed through an integrated acquisition and delivery framework focused on minimizing cybersecurity risks and keeping the overall system as secure as possible. The acquisition process is supported by policy stating that the "DTMB will adopt, acquire, develop and/or implement all [State of Michigan] IT products. The DTMB will also be responsible for managing all IT activities of agency projects that involve IT Resources."[251]

Led by the CSO's office, the state manages IT acquisition and implementation through an integrated approach designed to assess and manage cybersecurity risks. To assist with this, one of the three directors within the CSO's office is focused on risk assessments, compliance, and security awareness. For acquisitions, after determining that a need exists, Central Procurement conducts a market scan to identify qualified vendors. After a vendor is selected, the CSO's office begins running a series of checkpoints throughout the process to confirm

that the vendor is meeting security requirements. For more information on risk management during design and development of new systems, see the Risk Identification & Mitigation section below.

III. Risk Identification & Mitigation

The Challenge:

How to identify and mitigate cybersecurity risks across multiple organizations?

Features of Michigan's Governance Approach:

- The state merged its cyber and physical security teams under a single role, the CSO.
- The CSO sets policies and standards to govern information security that apply to all state government systems and conducts security assessments.
- The CSO's office actively works with state agencies to assess and manage cybersecurity risks in system development, from acquisition through implementation.
- The state is using a shared service model to provide CISO services to local municipalities that cannot fully fund their own.

The Management and Budget Act grants responsibility to the DTMB for the development, acquisition, and implementation of standardized risk management policies, practices, and programs across state agencies.[252] This responsibility is executed by a single CSO who manages Michigan's cyber and physical security teams. As the state saw cyber and physical risks converging, it created the CSO role in 2012 to manage all cyber and physical risks to the state government network. The CSO's office uses National Institute of Standards and Technology (NIST) guidance to inform its policy development for cyber risk management, provides risk assessment and management services across the DTMB and state agencies, and ensures that the DTMB and agencies comply with the policies.

Regardless of whether a new IT application is purchased or in-house development work is being completed, the CSO's office identifies risks that need to be mitigated throughout the system development life cycle.[253] As Rajiv Das, CSO and Deputy Director, said, "We want to deliver applications where we know the vulnerabilities are low. This approach also allows us to move to a risk-based model rather than a compliance-based model. The risk assessments point us to gaps and then we address the gaps through initiatives."[254] Using information from an application's initial risk assessment, the CSO's office conducts reviews to identify risks at design, coding, and testing checkpoints. Agency Services, a division within the DTMB, works with the agencies to remediate any identified risks. The CSO validates that the risks were properly mitigated before an application is deployed.

After the system integration work is done, the CSO's office regularly conducts application and network scans to detect vulnerabilities and corrects them if found. The CSO also helps remove communication gaps by maintaining at least one monthly meeting with each agency's Security and Privacy Officer to discuss upcoming DTMB projects, agency needs, etc.[255] Other offices within the DTMB have responsibilities associated with assessing and managing the risk of new applications. For example, within the software development life cycle, the CTO's Enterprise Solution Design Services division works to ensure that cyber risk is addressed during high-level design.[256]

To help govern this risk management approach, the DTMB also uses its overall DTMB Governance Model. In addition to the governance bodies introduced in the Strategy and Planning section (see Figure 2), Figure 3 introduces two other governance bodies that play important roles in decision making and risk resolution for the enterprise.

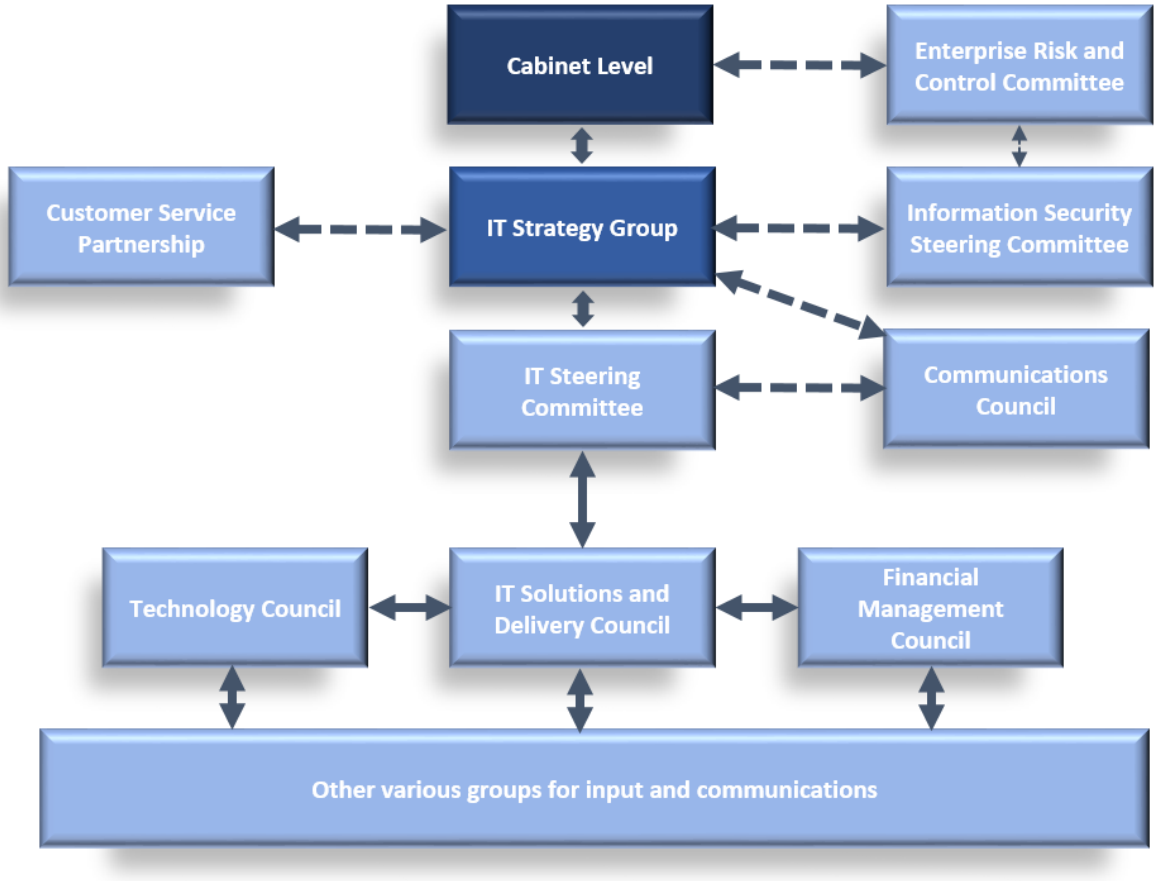


Figure 3. Complete DTMB Governance Model

(Detail on the bodies not discussed in this section was provided in the Strategy and Planning section. The Customer Service Partnership is not discussed in this case.)

The Information Security Steering Committee reports to the CSO, with representatives from Agency Services and two state agencies who rotate on an annual basis. It meets monthly to discuss variations from cyber risk policies or processes (i.e., exception requests) and propose solutions to resolve the issues from an enterprise perspective.[257] If needed, this group escalates unresolved risks to the Enterprise Risk and Control Committee (ERCC). The ERCC, which

reports to the Governor's office, has representatives from the Governor's office, the DTMB, and agencies outside the DTMB. It meets quarterly and is focused on examining and resolving macro-level risks and making enterprise-wide decisions.

In addition to managing risk in its own network, the state is addressing risk for local government entities through a new capability called "CISO as a service."[258] Under this model, local governments can opt via a memorandum of understanding to pay for a portion of a Chief Information Security Officer's (CISO) time. This initiative allows local governments, which may not be able to pay for a full-time CISO, to take advantage of an affordable shared service and apply cybersecurity risk management expertise across the state.[259]

Michigan also has formal governance structures and approaches to manage risks associated with preparation for and response to cyber incidents that cut across the government and private organizations. These are discussed in the Incident Response section below.

IV. Incident Response

The Challenge:

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

Features of Michigan's Governance Approach:

- The state worked with federal and state government, private industry, and others to create a Cyber Disruption Response Plan (CDRP) that guides preparation for and response to cyber incidents across public and private organizations.
- The state tailors existing emergency management response and recovery approaches and structures to cyber incidents.
- The CDRP uses a five-level threat matrix to move cyber incidents through escalation and de-escalation of the incident across the DTMB and the Emergency Management and Homeland Security Division.

Michigan has worked across multiple public and private organizations to develop and articulate its approach for managing cyber incident responses, from minor incidents to severe attacks. Michigan's approach to incident response has evolved through a series of efforts, beginning with Governor Snyder's 2011 and 2015 Cyber Initiatives (described in the Strategy & Planning section), which included incident response-related actions.

As part of this overall priority, in 2013 the state developed a Michigan Cyber Disruption Response Strategy that outlined "a framework for the prevention of, protection from, response to, and recovery from a significant cyber incident."[260] This strategy provided the foundation for the Cyber Disruption Response Plan (CDRP), a cross-ecosystem approach to addressing cyber incidents.[261] To develop the CDRP, leaders from the DTMB and emergency response agencies brought together members of the cyber ecosystem from state government, federal government, private industry, and others to understand requirements, collaborate, and come to consensus on a plan that would work for all stakeholders.[262]

The CDRP "provides a common framework for identifying and responding to technological threats with corresponding responses to address threats of increasing scope and severity."[263] The plan uses the Federal Emergency Management Agency's National Incident Management System structure for its cyber response, and outlines roles and responsibilities, communication procedures, training and exercises, and a risk assessment process by providing "guidelines to partner organizations to best protect Michigan's critical cyber infrastructure."[264]

The state's overall approach was intended to tailor emergency management response and recovery concepts to cyber incidents, not reinvent emergency response. As Captain Chris Kelenske, Commander of the Emergency

Management and Homeland Security Division, Michigan State Police, said, "Cyber incident response in Michigan is not a different emergency management process; the process just starts differently."[265]

To this point, the CDRP uses a threat matrix to move cyber incidents along a five-level cyber escalation/de-escalation path. At levels 1 and 2, the CIO's office and the security operations center manage day-to-day cyber events, including the Michigan State Police's Michigan Intelligence Operations Center (MIOC), or fusion center, as needed. At level 3, the CDRP begins to trigger emergency management processes and the involvement of other organizations, such as the Governor's office, Michigan Cyber Command Center, State Emergency Operations Center (SEOC), National Guard, and Cyber Civilian Corps. Depending on the incident's size, impact, and level of severity, other organizations, including non-government entities, are brought into the SEOC.

For level 3 through 5 cyber incidents, Michigan uses an Incident Command System (ICS), through which a Cyber Disruption Response Team (CDRT) helps staff the ICS and provides domain and cyber expertise from across the ecosystem (see Figure 4). The CDRT is a group of subject matter experts from public and private emergency management and IT fields whose role is to support federal, state, local, and private organizations in the preparation for, response to, and recovery from cyber events.[266] It is led by the CSO as the Chairman and the Deputy State Director of Emergency Management and Homeland Security as the Vice Chairman when the SEOC is not activated. Once the SEOC is activated, the Chair and Co-Chairs appoint a CDRT lead to act as the incident commander.[267] Figure 4 illustrates the ICS structure when a SEOC is activated.

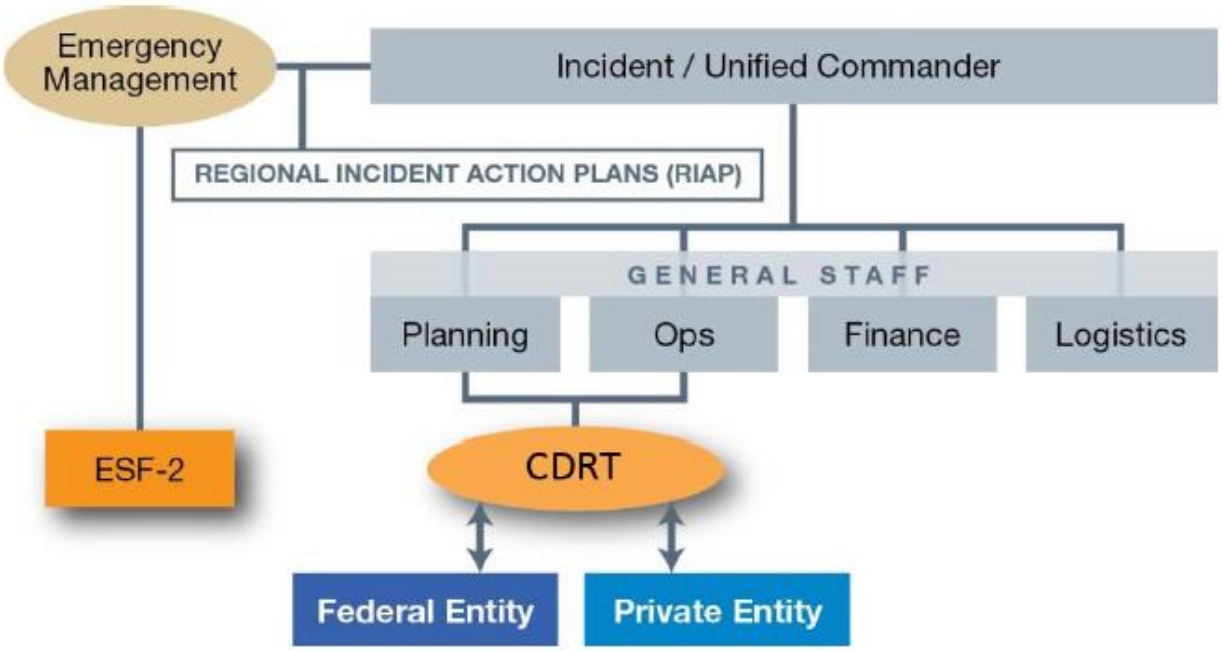


Figure 4. Incident Command System Organization Chart[268]

(This organization chart is from Michigan's CDRP.)

The CDRP and its supporting documentation (workbook and job aids) provided to responders outline how events are managed along the escalation path. To prepare for cyber incidents and update the CDRP, the state conducts discussion-based (e.g., tabletop exercises) and

operations-based (e.g., drills) exercises throughout the year, using post-exercise feedback loops and after-action reports.[269]

Members of the CDRT also regularly use informal communication channels to notify their peers and partners about cyber events before those peers are formally involved.[270] Consistent formal and informal communications help keep the CDRT prepared for cyber events and are key underpinnings of the CDRP's and Michigan's approach to cybersecurity incident response.

V. Information Sharing

The Challenge:

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

Features of Michigan's Governance Approach:

- The state is intentional in its formal and informal information sharing mechanisms at strategic, operational, and tactical levels.
- The state participates in cross-state information sharing bodies (e.g., the Multi-State Information Sharing and Analysis Center [MS-ISAC] and NASCIO).

One of Michigan's most defining features of cybersecurity governance is its interconnected ecosystem, which reaches across state, federal, private, academic, and not-for-profit organizations. According to David Behen, former DTMB Director and CIO, "The focus is state of Michigan cybersecurity, not [just] the state of Michigan government's cybersecurity."[271] To accomplish this, the state uses a combination of formal and informal information sharing mechanisms to help solve problems at the strategic, operational, and tactical levels.

From a strategic perspective, Governor Snyder has promoted information sharing by engaging with individuals and organizations across the ecosystem to provide input into the 2011 and 2015 Cyber Initiatives. The governor stays connected with private sector organizations on cyber-related topics through the quarterly Cyber Advisory Council, which provides an opportunity for sectors (e.g., critical infrastructure, finance, education, and health) to share with the Governor what they are seeing and how the ecosystem is responding.[272] These connections help the Governor's Office set priorities for the state.

The DTMB uses a variety of groups, councils, and committees to share strategic and operational cyber information across the ecosystem. For example, the CIO chairs and the CSO leads the Cyber Executive Team, which brings together public sector members of the ecosystem, such as National Guard, Michigan State Police, academia, and Michigan Economic Development Corporation, on a quarterly basis and helps the DTMB focus on topics such as the budgeting process and regional training.[273]

The DTMB has also created structures to share information with the private sector. When David Behen became Michigan's DTMB Director and CIO, one of his first initiatives was to develop the CIO Kitchen Cabinet. This forum brings together nearly two dozen Michigan-based CIOs from across industries and different-sized organizations on a regular basis. The group is formally chartered, meets monthly, and provides an opportunity for CIOs to discuss cybersecurity topics. Even though direct economic competitors are represented in the cabinet, the group has found ways to actively engage on a range of common challenges, including sharing strategies for mitigating risks

and addressing workforce concerns. Behen used the cabinet as a sounding board on topics such as the state's cybersecurity strategy and budgeting exercises.[274]

Inspired by success of this Kitchen Cabinet, the CSO Kitchen Cabinet and two industry-specific sub-councils focused on the healthcare and finance industries were created.[275] The CSO Kitchen Cabinet and councils operate similarly to CIO Kitchen Cabinet. The Michigan Healthcare Cybersecurity Council, which includes 20 major and minor healthcare providers, is pursuing 501c3 status to secure grant funding and sustained support to accomplish common needs, such as emergency response training. The council is also creating a standardized approach for all Michigan healthcare organizations to work with vendors on cybersecurity issues. This will help provide a consistent approach for healthcare organizations and vendors, which will ultimately help to better secure healthcare data.[276]

From operational and tactical perspectives, both the DTMB and the Michigan State Police require ongoing coordination to execute their important roles in cybersecurity response. They use the formal platform of the MIOC, which provides 24-hours-a-day statewide information sharing among local, state, and federal organizations and private sector partners. Outside of this formal communication channel, the entities err on the side of overinforming each other through informal networks.[277] In addition, the state 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.[278] The DTMB and Michigan cybersecurity ecosystem also routinely collaborate and share information with federal government partners.

While there are now many formal channels for information sharing, according to CTO Rod Davenport, informal information sharing is still very important. When informal, ad hoc information sharing between groups is motivated by personal interest and passion, it frequently becomes the "most sustaining because it's the most authentic," Davenport said.[279]

VI. Workforce & Education

The Challenge:

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

Features of Michigan's Governance Approach:

- The state uses Merit Network (Merit), a nonprofit organization, to help address the cyber workforce gaps across state government, private industry, and other partners.
- The Michigan Cyber Range (MCR), operated by Merit, provides an unclassified physical range for education, training, and product development for organizations across multiple sectors.
- Merit works across and serves diverse institutions, industries, and age groups to offer several other programs to develop cybersecurity skills for a broad range of geographic and demographic populations.

Workforce development and education are areas of critical need for Michigan, because the state government and its private and public sector partners face a common cyber workforce gap. The state government recognized that the cybersecurity workforce gap cuts across multiple organizations and sectors and that creating a sustainable model to help grow the workforce would benefit the entire state. The state is addressing this gap through Merit, a "…non-profit, Member-owned organization governed by Michigan's public universities,"[280] with many links across the education and research fields.

One of the ways that Merit prepares the cybersecurity workforce to address real-world cyber events is through the creation of the first unclassified network-accessible range in the United States. The Michigan Cyber Range (MCR) provides a space for cybersecurity education, training, and product development and testing to its clients across the United States and the world. Training courses, available online or in a classroom, focus on certifying students so that they have professional credentials and certifications necessary to work in the cybersecurity field.[281]

Governor Snyder first proposed the MCR in his Cyber Security Vision Statement in 2011, and it was initially made possible through grants and sponsorship. Now a self-sustaining organization through contracts with its various users, the MCR is operated by Merit. The MCR's resources are available to public and private entities; users include city, county, and state emergency managers, the National Guard, other states,

international organizations, academic institutions, and private organizations and businesses. Its Executive Director works with an Advisory Council to ensure that the MCR's training is aligned with skill demand and the five-year strategic plan is developed to keep it self-sufficient. As a nonprofit, the MCR is well positioned to act quickly and flexibly to meet changing demands.[282]

The MCR has 10 hubs, or physical extensions, that offer more than 40 industry-recognized certifications designed to qualify individuals for cybersecurity positions.[283] With the understanding that developing a strong cyber workforce should begin prior to college, the MCR partnered with the Pinckney Community High School in southeast Michigan in 2016 to serve as one of these hubs. It will expand IT and cybersecurity education and training for its students and surrounding communities in areas such as computer forensics and network security. This hub, or cyber training institute, is the first effort of its kind in the United States, providing "educational and certification opportunities for high school and college students, as well as tech professionals."[284] Through this program, "students can earn college credits and gain access to internship opportunities."[285] Over time, the institute is looking to expand services, including hands-on training, and to "grow the program through partnerships and higher educational institutions."[286]

Merit and the state have developed two other mechanisms to "address the widening gap between the supply of skilled cybersecurity professionals and the demand for those skills."[287] As a part of the MCR, the Regional Cybersecurity Education Collaboration (RCEC) was developed as a self-funded "collaborative between the higher education community[288] and key private sector partners to [grow the cybersecurity workforce and prepare key industries for evolving cybersecurity challenges]."[289] The collaboration encompasses a collection of university curriculums that is accessed through an ecosystem of participating institutions via distance learning over Merit's network. The RCEC leverages Merit's technical infrastructure and bandwidth[290] and the MCR's courses to provide training to individuals who do not have access to a physical hub.[291]

The Governor's second annual High School Cyber Challenge is another Merit-run initiative intended to grow the cybersecurity workforce by developing interest and talent in cybersecurity prior to postsecondary education. Merit works with high schools to conduct a multi-round online competition for small teams of high school students to use their knowledge of IT and cybersecurity, culminating in a head-to-head competition at the North American International Cyber Summit in Detroit.[292] There is no cost to participate, and the trip to Detroit is all expenses paid, which allows the initiative to reach unserved and underserved areas and eliminate economic and geographic constraints.[293]

Faced with a cybersecurity workforce challenge that stretches across the ecosystem, Michigan developed a governance mechanism, using Merit, to address it from a cross-ecosystem perspective. Through mechanisms like the Governor's High School Cyber Challenge, the MCR and its hubs, and the RCEC, Merit builds the cyber workforce from early education through employment while also filling the pipeline by retraining and educating Veterans. By marketing some of its services (e.g., the MCR) to the private sector and entities outside the state, Merit has diversified its funding streams, making it a self-sustaining organization.

VII. Deep Dive: Michigan Cyber Range

Introduction

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

The Challenge

The demand for a trained, diverse cybersecurity workforce outstrips supply in public and private sectors. Traditional models (e.g., recruit graduates from select undergraduate and graduate schools) have not kept up with the demand. Workforce development must start prior to postsecondary education and continue throughout an individual's professional development.

The Solution

Create a virtual environment for cybersecurity education, training, and testing through a not-for-profit organization—Merit—to address the cybersecurity workforce challenge that affects institutions and industries across the state. The education opportunities, including certification courses, are available to high school and college students and working professionals as individuals and groups. Businesses and other organizations may use the secure environment for product development and testing.

Background

In his 2011 Cyber Security Vision Statement, Governor Rick Snyder noted the need for an environment to help build a cybersecurity workforce to both address cyber threats and attract businesses to Michigan. From this, the MCR was created in 2012 and is operated by Merit, a nonprofit, member-owned[294] organization serving research, education, and public sector communities. The MCR "prepares cybersecurity professionals to detect, prevent and mitigate cyber-attacks" through a variety of services:[295]

- Access to an unclassified private cloud.
- A secure environment in which to test attack and defense strategies on small or large networks without introducing actual risk to an organization's network.
- Training courses (for certification)[296] and exercises using a virtual training environment called Alphaville to test cybersecurity skills. Alphaville provides real-world situations that show how information systems across communities are connected, therefore increasing risk and vulnerabilities. This environment includes "virtual machines that act as web servers, mail servers, and other types of machines."[297]
- Research in areas such as new internet protocols, network security, and the development of tools to monitor and secure networks.[298]

Founded in 1966, Merit owns and operates the longest running regional research and education network in the United States and is governed by Michigan's public universities. Its membership includes 300+ members, including Michigan's public universities, K-12 schools, libraries, local government agencies, and not-for-profits. The MCR leverages Merit's experience and resources.

The MCR was funded by grants from NIST, the Michigan State Police, and DHS. Initial sponsorship was also provided by three private sector companies.[299] Since the MCR is operated by Merit, it leverages Merit's 4,000 miles of fiber-optic infrastructure throughout Michigan and neighboring states and use a "national high-speed backbone network" that makes the MCR available nationwide.[300]

The MCR provides training under contract to U.S. and worldwide organizations, such as the National Guard; city, county, and state emergency managers; other state governments; various private sector organizations; and academia. These training courses and other services allow the MCR to be financially self-sufficient; its independence from government allows it to be flexible. Dr. Joe Adams, Vice President for Research and Cyber Security and Executive Director of the MCR, meets with a Board of Advisors every quarter to discuss direction and financial solvency. He also meets with an Advisory Council that is focused on aligning the MCR's training with the demand for certain skills and helps create a strategic five-year plan to guide training programs.[301]

In addition to its eight existing physical hubs,[302] in 2016 the MCR announced two new Cyber Range Hubs at Wayne State University and Pinckney Community High School to expand training and certification offerings. The new facilities will provide trainees with access to computing infrastructure testing labs, cybersecurity training exercises, and product testing and offer certification courses in over 20 cybersecurity disciplines.[303] Both hubs offer courses to college students and cybersecurity professionals, and the Pinckney Community High School hub will be the only program in the state to offer cybersecurity courses to high school students.

Adding to the MCR's physical hubs, in 2017 Merit launched the RCEC as a virtual hub, or extension, of the MCR to reach high schools, colleges, Veterans, and others who cannot reach a physical hub. The RCEC is another mechanism for growing the cybersecurity workforce through seminars, classes, and exercises by leveraging capabilities such as Merit's fiber-optic network and the MCR's intellectual property, including Alphaville. The RCEC is structured as a partnership with three higher education institutions[304] and key private sector partners to become a lasting, financially self-sufficient organization. The RCEC incentivizes participation by students and industry through the solicitation of scholarships for students from private sector organizations.[305] Scholarships will range from $3,000 to $5,000, depending on the course and certification, with the goal of complete coverage for the student.[306] In the initial offerings through the RCEC, the MCR is seeing demand from students and organizations like the Michigan Municipal Services Agency that want to get involved early. As it grows, the RCEC will provide "a platform for instructors to share curriculum throughout the state," and will help it to add more two- and four-year colleges to the collaborative.[307]

Faced with a cybersecurity workforce challenge that stretches across the ecosystem, Michigan developed a governance mechanism, using Merit, to address it from a cross-ecosystem perspective. Through mechanisms like the Governor's High School Cyber Challenge, the MCR and its hubs, and the RCEC, Merit builds the cyber workforce from early education through employment while also filling the pipeline by retraining and educating Veterans. By marketing some of its services (e.g., the MCR) to the private sector and entities outside the state, Merit has diversified its funding streams, making it a self-sustaining organization.

VIII. Acronyms

Acronym	Definition
CDRP	Cyber Disruption Response Plan
CDRT	Cyber Disruption Response Team
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CS&C	Office of Cybersecurity and Communications
CSO	Chief Security Officer
CTO	Chief Technology Officer
DHS	Department of Homeland Security
DTMB	Department of Technology Management and Budget
ERCC	Enterprise Risk and Control Committee
FFRDC	Federally Funded Research and Development Center
HSSEDI	Homeland Security Systems Engineering
ICS	Incident Command System
IT	Information Technology
MCR	Michigan Cyber Range
MIOC	Michigan Intelligence Operations Center
MS-ISAC	Multi-State Information Sharing and Analysis Center
NASCIO	National Association of State Chief Information Officers
NIST	National Institute of Standards and Technology
RCEC	Regional Cybersecurity Education Collaboration
SBO	State Budget Office
SEOC	State Emergency Operations Center
SLTT	State, Local, Tribal & Territorial

Cybersecurity Governance in the State of New Jersey

A CASE STUDY

December 2017

Homeland Security

NASCIO
Representing Chief Information Officers of the States

New Jersey State Fast Facts[308,309]

ELECTED OFFICIALS:

- Governor Chris Christie
- New Jersey General Assembly: 80 Members of the Assembly
- New Jersey State Senate: 40 Senators[310]

STATE CYBERSECURITY EXECUTIVES:

- Chief Information Security Officer (CISO) Michael Geraghty
- Chief Technology Officer (CTO) David Weinstein

STATE DEMOGRAPHICS:

- Population: 8,832,406
- Workforce in "computers and math" occupations: 3.6%[311]

EDUCATION:

- Public with a high school diploma: 46.1%
- Public with an advanced degree: 42.1%

COLLEGES AND UNIVERSITIES:

- 19 community colleges[312]
- 15 private colleges
- 10 public research universities and state colleges[313]

KEY INDUSTRIES:[314]

- Agriculture
- Finance
- Healthcare
- Life sciences
- Logistics
- Manufacturing
- Technology

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 New Jersey'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 New Jersey 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 New Jersey 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.[315]

This case study is part of a pilot project intended to demonstrate how states use 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 New Jersey's governance approach, rather than a detailed exploration. Individual states and organizations seeking greater detail would likely need to engage directly with New Jersey to better understand how to tailor solutions to their specific circumstances.

A law passed in 2007 helped lay the foundation for New Jersey's current cybersecurity initiatives by consolidating information technology (IT) services from across executive branch agencies into one agency—the Office of Information Technology (OIT).[316] This change allowed the state to coordinate IT "planning, budgeting, and spending throughout the Executive Branch to advance cost savings, improve the quality of services, and retain operating efficiencies."[317] (In this case study, "agency" refers to executive branch agencies.) This, in turn, provided a foundation for executive leaders to launch a series of deliberate steps beginning in 2015 to

strengthen cross-organizational cybersecurity governance. This case, therefore, will focus primarily on changes made since approximately 2015 and recognizes that the state is still in the process of developing and implementing its cross-ecosystem cybersecurity governance.

In 2015, Governor Chris Christie signed an executive order establishing the New Jersey Cybersecurity & Communications Integration Cell (NJCCIC), a central civilian body designed to "coordinate cybersecurity information sharing, perform cybersecurity threat analysis, and promote shared and situational awareness between and among the public and private sectors."[318]

The NJCCIC is part of the New Jersey Office of Homeland Security and Preparedness (OHSP), a reflection of the state's view of cyber as a security issue rather than strictly an IT issue.[319] As state Chief Information Security Officer (CISO) Mike Geraghty said, "By moving the CISO under the homeland security function within the state, risks are reported within an environment with a lot of the right assets in place, such as state police, intelligence analysts and information sharing resources."[320]

The Director of OHSP is responsible for "the strategic development, execution, and management of an effective and efficient information security program to manage cyber risks and ensure the confidentiality, integrity, and availability of the Executive Branch's information assets."[321] The CISO, who reports to the Director of OHSP, serves as the head of the OHSP Division of Cybersecurity and leads the state's cybersecurity strategic planning, information sharing, and incident response efforts.[322]

The CISO collaborates with the Chief Technology Officer (CTO), who leads OIT and issues policies designed to protect the state's assets and networks, and ensures that state departments and agencies follow the CISO and CTO policies.[323] The CTO, who is a member of the cabinet and reports directly to the Governor, is responsible for supporting the state information security program. This is accomplished by designing, acquiring, and implementing an enterprise IT system—in compliance with information security policies and standards set by the state CISO—and operating the IT systems in compliance with CISO-approved security procedures, such as malware protection, data encryption, and software patch management. As part of this responsibility, the CTO ensures that policies are implemented by the individual departments and agencies.

In 2017, OIT and NJCCIC leaders collaborated and issued a series of new information security policies to provide foundational direction to state departments and agencies. Among the first policies to be drafted and issued were the state's cyber incident response policy and plan; cybersecurity organizational roles and responsibilities; and state department and agency IT acquisition policy.

In addition to the priorities outlined above, New Jersey has developed information sharing structures and mechanisms to disseminate threat information with the government and private sector. For example, the NJCCIC shares information with more than 39 states, 42 federal agencies, state executive departments and agencies, local governments, 13 international countries (such as the UK, Australia, and Germany), and many companies. Also, reflective of the importance of the financial industry to the economy, the NJCCIC formed a partnership with the Financial Services Information Sharing and Analysis Center (FS-ISAC) to share and analyze cyber threats to the financial industry. In addition, there are two formal information sharing bodies—the Domestic Security Preparedness Task Force (DSPTF) and the Infrastructure Advisory Committee (IAC)—that include private sector membership. The DSPTF and IAC raise cybersecurity issues facing private industry to the attention of executive branch leaders.

New Jersey demonstrates cybersecurity is a challenge that cuts across many issues and many interdependent stakeholders. Therefore, New Jersey uses a range of governance mechanisms to work across organizations. As New Jersey is in the process of strengthening and expanding cross-ecosystem cybersecurity governance, much of the initial focus has been on strengthening cross-government cybersecurity, filling some of the most important cybersecurity roles in the state, such as the CTO, CISO and Director of OHSP, and building on New Jersey's public/private information sharing mechanisms.

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.[324]

The case study explores cross-enterprise governance mechanisms used by New Jersey 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 New Jersey's governance approach, rather than a detailed exploration. Individual states and organizations seeking greater detail would likely need to engage directly with New Jersey 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."[325] 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 New Jersey's Governance Approach:

- The CISO is charged with developing a statewide cybersecurity strategy.
- A cross-enterprise information security program is operationalized via policies and standards developed by the OHSP and OIT.
- An intra-governmental committee brings a cross-organizational perspective to the development of state cybersecurity strategy.

The CISO, who was hired in 2016 and reports to the Director of the OHSP (see Figure 1 below), is charged with developing a statewide cybersecurity strategy. This responsibility is part of the CISO's overall mission to establish and manage "an information security program to ensure the confidentiality, integrity, and availability" of the executive branch's "information resources, systems, and services while promoting and protecting privacy" and "developing, implementing and monitoring the performance of the information security program."[326] The CISO:

- Sets strategic information security plans across the executive branch,
- Publishes and maintains the statewide Information Security Policies and Standards,
- Develops, maintains, and interprets the Information Security Policies and Standards, and
- Provides cybersecurity subject matter expertise to state agencies.[327]

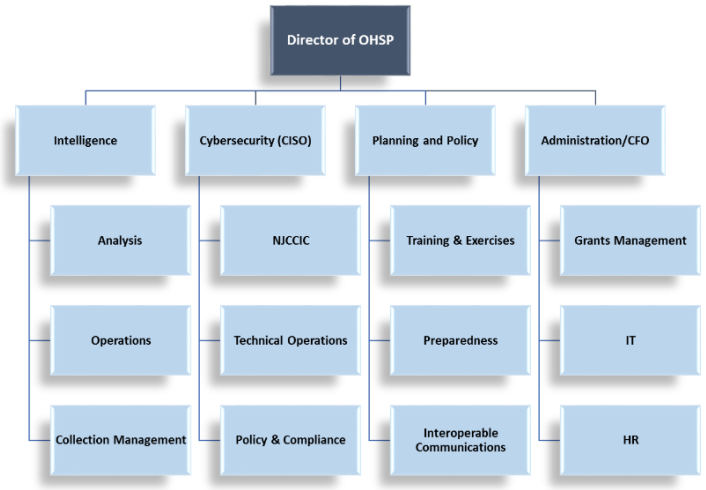


Figure 1. New Jersey Office of Homeland Security and Preparedness[328]

When this case was being developed, the CISO was in the final stages of completing a formal cybersecurity strategic plan guided by several government and industry-authored frameworks.[329] However, the Director of OHSP, the CTO, and CISO shared a common strategic perspective about the need for a cross-enterprise information security program. They have taken several steps in the last year to instantiate this program via policies and standards that address cyber risk identification and mitigation, cyber incident response, and information sharing (see Section II, Budget & Acquisition; Section III, Risk Identification & Mitigation; and Section V, Information Sharing).[330]

To bring a cross-organizational perspective to the development of state cybersecurity strategy, in January 2017 OIT policy created the Information Security Governance Committee (ISGC), an intra-governmental body co-chaired by the Director of the OHSP and the CTO. The ISGC, which is in the process of being stood up, is intended to play a strategic role in cybersecurity issues within the state and reports to the cabinet. ISGC members include the state CISO, the state Chief Data Officer (CDO), representatives from the Department of Treasury, and other state agencies as appropriate.[331] The ISGC is responsible for:[332]

- Assisting the CISO in overseeing and executing the state's information security management program,
- Reviewing the Enterprise Information Security Policies and Standards—and subsequent amendments—to ensure their alignment with the executive branch business objectives and goals, risk tolerances, and statutory, regulatory, and contractual requirements,
- Providing direction and counsel regarding the assessment and management of information security risks and cyber threats to the state of New Jersey,
- Reviewing reports on major information security incidents and cases of noncompliance,
- Overseeing the response to information security incidents,
- Reviewing security metrics and trends regarding the overall performance of the information security program, and
- Staying abreast of cybersecurity threats to the executive branch of state government through briefings and reports.

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 New Jersey's Governance Approach:

- Agencies use annual IT budget to reimburse OHSP and/or OIT for some enterprise-wide cyber-related services.
- Acquisition policy is designed to reduce cyber risks by centralizing authorization for certain services and products with the CTO.

The OHSP and OIT use a variety of budget and acquisition governance mechanisms to drive and influence cybersecurity practices throughout state departments and agencies.

While each agency receives an annual IT budget, some of this budget is used to reimburse OHSP and OIT for enterprise-wide cyber-related services. Reimbursement levels are set according to agency headcount or workstation count, with the larger organizations paying more than smaller organizations. For example, OIT provides a vendor solution called "Websense" to all executive agencies to help filter internet content available to users on the state's network.[333] Access to certain sites is restricted in keeping with the state's internet user agreement and risk profile, and Websense provides a mechanism to operationalize this policy. The OIT purchased a global license to Websense and charges agencies a fee based on usage to cover the cost of the license.[334] Websense is one of many information security tools the CTO uses to ensure user safety on the state's network. NJCCIC also provides some enterprise-wide cybersecurity protections, such as next generation firewalls, intrusion prevention systems, and a security information and event management system.[335]

In addition to budget, New Jersey uses acquisition policy to drive cybersecurity. In September 2017, a new procurement policy established procedures that apply to department and agency acquisition of IT hardware, software, and subscription-based services. The purpose of the policy is, in part, to reduce the risk of cybersecurity threats to the state's network by centralizing IT acquisition with the OIT CTO to ensure that any new technology or service introduced into the state's network receives proper vetting to comply with information security standards set by the CISO.

The policy expressly prohibits agencies from purchasing "any information technology infrastructure, regardless of dollar value, unless granted approval due to exceptional circumstances by OIT."[336] IT infrastructure is defined as "computing, storage, network and data center assets (e.g. servers, routers, racks)."[337] In addition, the new policy requires

CTO approval for upgrades to IT infrastructure that may impact information security.[338]

The OIT CTO reviews and approves IT purchases exceeding $50,000, while those exceeding $100,000 must undergo OIT and Office of Management and Budget (OMB) review and approval.[339]

III. Risk Identification & Mitigation

The Challenge:

How to identify and mitigate cybersecurity risks across multiple organizations?

Features of New Jersey's Governance Approach:

- Cybersecurity risk identification and mitigation activities are a shared responsibility between the CISO, CTO, and state agencies.
- The CISO and CTO are primarily responsible for policy setting and review, while agencies are primarily responsible for implementation.
- The CTO uses a Systems Architecture Review (SAR) process to ensure agency systems and services comply with the CISO's guidelines.
- The CTO also has execution responsibilities, including the day-to-day security management of enterprise information, systems, and solutions.

The state's cybersecurity risk identification and mitigation activities are a shared responsibility between the CISO, CTO, and state departments and agencies. The CISO and CTO are primarily responsible for policy setting and review, while agencies are primarily responsible for implementation.

The CISO establishes the overarching requirements, standards, and metrics for cybersecurity in departments and agencies. Based on 2017 policy, the CISO is responsible for:[340]

- Identifying security requirements to limit risks associated with executive business objectives, and
- Providing security metrics to track the performance of the information security program.

The CISO is also responsible for developing an Information Security Governance, Risk, and Compliance program, including, but not limited to:

- Coordinating and conducting compliance and risk assessments of agencies and their information assets,
- Conducting and managing vulnerability assessments of agency networks, applications, databases, and systems,

- Conducting penetration tests of agency networks, applications, databases, and systems, and
- Conducting information security risk assessments of third parties with access to state of New Jersey information assets.

The program, for example, is on track to conduct 50 risk assessments, 1,500 system vulnerability assessments, and 1,500 application vulnerability assessments in FY2018.[341]

As described above in Section I, Strategy & Planning, the ISGC, which is co-chaired by the Director of OHSP and the CTO, is in the process of being stood up. It is intended to help the CISO identify potential risks. The ISGC reports to the cabinet and can assist the CISO by reviewing reports of major information security incidents and cases of noncompliance, staying abreast of cybersecurity threats to the executive branch, and providing "direction and counsel regarding the assessment and management of information security risks and cyber threats to the State of New Jersey."[342]

The CTO is responsible for reviewing "all plans for any modification and/or new installation to Executive Branch information systems," including hardware, software, and IT architecture "to ensure those modifications are in alignment with the State's [IT] strategy and in compliance with enterprise architecture standards."[343] The CTO uses a SAR process to ensure that department and agency systems and services comply with the CISO's guidelines (see Figure 2).

The SAR includes representation from across the executive branch: the CTO, the department/agency Chief Information Officer (CIO), the OHSP, and the CDO. The purpose of the SAR is to ensure compliance with NJCCIC cybersecurity and IT architecture standards and ensure that a vulnerability and/or risk assessment is performed. The results from the assessment as well as other data collected during the review inform: (1) New Jersey cybersecurity and privacy requirements; (2) potential impacts on existing technology infrastructure and operations; (3) prioritization of resources; and (4) disaster recovery and business continuity requirements.[344]

To identify potential risks, the SAR process entails five steps:

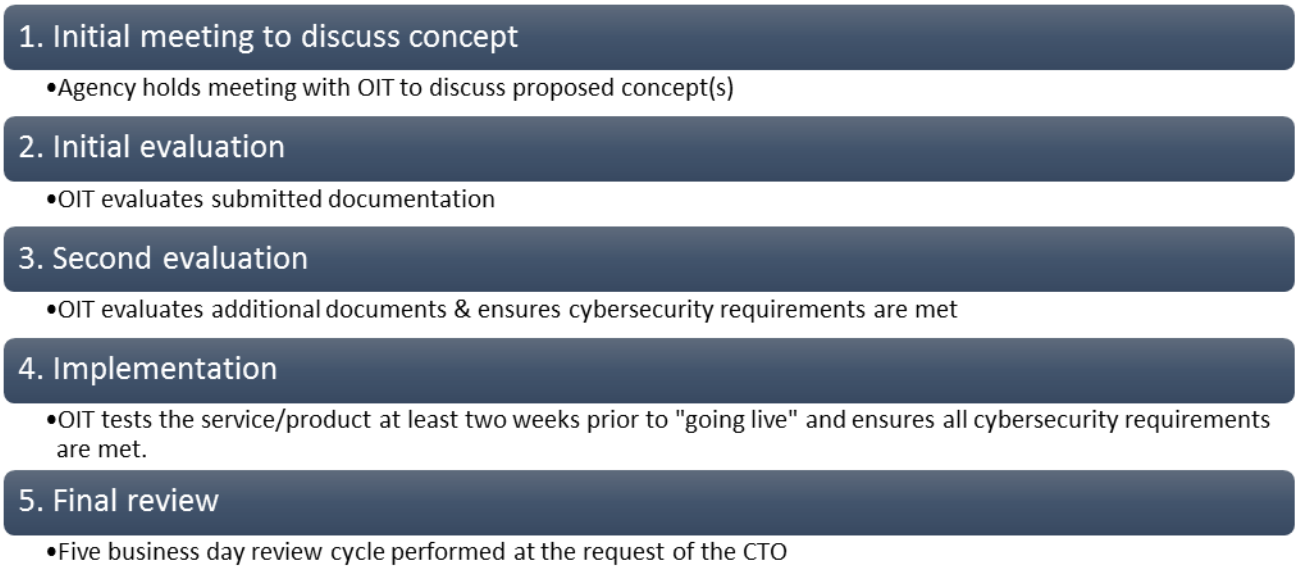


Figure 2. OIT SAR Process[345]

The CTO also has execution responsibilities, including the day-to-day security management of enterprise information, systems, and solutions. For example, an Executive Order signed in June 2017 authorizes the CTO to identify and consolidate state IT assets, such as servers and data centers, and modernize the "hundreds of legacy applications," in part to ensure information security across the enterprise.[346]

To ensure coordination between the CISO and CTO, which has its own risk management responsibilities, the OHSP's Division of Cybersecurity's Governance, Risk and Compliance Bureau (GRCB) meets twice a week with OIT to review all proposed new technology products and services. The GRCB reviews potential risks to ensure that cybersecurity standards are met. An assessment is performed to ensure that a product or service can be integrated into the network without introducing vulnerabilities into the enterprise architecture. The GRCB also ensures that adequate funds are identified within OIT, OHSP, and/or the requesting department or agency.

Agencies are responsible for implementing CISO and OIT policies and "protecting and maintaining the confidentiality, integrity, and availability of information assets" within the department or agency.[347] Agency CIOs also manage third-party vendors under contract to provide information services to the department or agency.[348] Departments/agencies must:[349]

- Identify security requirements to limit cyber risks associated with the agency's business goals and objectives,
- Implement and promote information security awareness within their respective agency,
- Ensure compliance with the CISO-created policies and standards such as:
    - Coordination of risk assessments and compliance audits with the NJCCIC
    - Coordination of vulnerability assessments of agency networks, applications, databases, and systems
    - Coordination of risk assessments of third parties having access to agency information assets
- Assist in the implementation of the Cybersecurity Incident Response Plan, and
- Report all information security incidents to the NJCCIC.

IV. Incident Response

The Challenge:

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

Features of New Jersey's Governance Approach:

- The CISO is responsible for establishing the state's overall cyber incident response policy and plan.
- Agencies are responsible for implementing the plan.
- Policy directs agency heads to form in-house Cybersecurity Incident Response Teams (CSIRTs), which are responsible for incident response.

The CISO is responsible for establishing the state's overall cyber incident response policy and plan, while departments and agencies are responsible for implementing the plan. The Director of OHSP is responsible for "overseeing the response to information security incidents."[350]

In 2017, Michael Geraghty, Director of the NJCCIC and the state CISO, rewrote the state's cyber incident response policy and plan. The policy applies to all executive branch agencies, contractors, and third-party vendors, and all "cybersecurity incidents that affect the confidentiality, integrity and availability of agency networks, systems, applications, databases, data and other information assets owned or controlled by the agencies or maintained on their behalf."[351]

The policy describes cyber incident reporting scope, authorities, communication, training, enforcement, and compliance. The cyber response plan ("the plan") describes the roles and responsibilities of incident response team participants, an approach to characterize the incidents, and reporting requirements, and contains sample communications and notification guidance and documentation.[352] Department and agency leaders are responsible for implementing the plan within their respective organizations.[353] The plan, which applies to all executive departments, agencies, commissions, boards, and bodies, focuses on preparation and response to cyber threats that could impact state assets, such as the state network. In the future, the plan is expected to expand and contemplate incidents emanating from external sources, such as private owners/operators of critical infrastructure, that could impact state assets, and/or large-scale incidents that could simultaneously impact multiple state departments and agencies.

The plan incorporates a Cybersecurity Incident Lifecycle ("Lifecycle") and a Cybersecurity Incident Framework ("Framework") (see Figure 3 below).[354] A cybersecurity incident is defined as "any adverse event or condition that has the potential to impact the confidentiality, integrity, and availability of agency information assets."[355]

"The Lifecycle [which consists of four phases] characterizes the continuous efforts agencies makes to handle incidents, while at the same time ensuring continuous improvements in the overall security posture of the Executive Branch of State Government or an agency thereof."[356]

Phase	Description
Preparation	Includes activities that enable agencies to respond to an incident, such as development and implementation of policies and procedures, security technologies and tools, training, governance, and communication plans.
Detection & Analysis	Includes the identification and investigation of an incident. During the detection and analysis phase, the incident receives an initial categorization and prioritization. An investigation into the incident with corresponding activities, including evidence collection, documentation of the incident response activities, etc., is initiated during this phase.
Containment, Eradication, & Recovery	Includes all activities involved in the containment of the incident, the eradication of its cause, the restoration of the impacted information assets and the return to normal operations. This phase also involves determining the root cause of the incident.
Post Incident Activity	Includes developing the incident report and disseminating it to appropriate stakeholders; identifying lessons learned from the incident handling process, including the successful and unsuccessful actions taken by an agency in response to the incident; and developing recommendations to prevent future incidents and to improve enterprise security implementation.

Figure 3. New Jersey Cybersecurity Incident Lifecycle

The Framework "consists of a collection of practices and tools that provide agencies with the ability to categorize, prioritize, communicate, track and document incident response activities."[357]

Agencies play a central role in implementing the policy and plan. For example, the incident response policy directs agency heads to form in-house CSIRTs, which are responsible for coordinating and carrying out the agency's response to incidents.[358] CSIRTs are generally comprised of members from the agency: IT team, information security office (ISO), legal, public information office, human resources department, and auxiliary agencies, as necessary (see Figure 4 below). CSIRT members are responsible for carrying out the agency's response to information security incidents, including classifying the incident (by severity, type, etc.). Agency leaders must designate an individual with responsibility to act as the CSIRT Coordinator (typically the agency CIO or ISO). The NJCCIC and OIT support the CSIRTs as necessary to effectively respond to an incident.

Figure 4. Agency CSIRT

The policy directs agencies to report all incidents to the NJCCIC and describes the process for reporting, managing, and escalating to the appropriate stakeholders.[359] All reports of incidents are collected by NJCCIC and entered into a centralized reporting system for analysis "to identify trends or outbreaks that may require changes to security controls and/or policies to reduce the risk of future occurrences."[360]

The agency CSIRT is responsible for classifying incidents according to the below categories. This approach to classifying cyber incidents provides a standardized means to track incidents across the enterprise, as well as measure frequency and types of incidents.[361]

Table 1. New Jersey Cyber Incident Classification Categories

Category	Name	Description
Cat 0	Security Testing	This category is used during agency-approved vulnerability testing.
Cat 1	Unauthorized Access	Individual gains logical or physical access without authorization to an agency network, system, application, private or restricted data, or other information asset.
Cat 2	Denial of Service (DoS)	An attack that prevents or impairs the normal authorized functionality of agency networks, systems, or applications by exhausting resources. This activity includes being the victim or participating in the DoS.
Cat 3	Malicious Code	Installation of malicious software (e.g., virus, worm, Trojan horse, ransomware, or other code-based malicious entity) that infects an agency operating system or application.
Cat 4	Improper Usage	A user violates the Acceptable Use Policy or other agency or state policies.[362]
Cat 5	Scans, Probes, Attempted Access	Any activity that seeks to access or identify an agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or DoS.
Cat 6	Investigation	Unconfirmed incidents that are potentially malicious, or anomalous activity, deemed by the reporting entity to warrant further review.
Cat 7	Data Breach	A data breach is: • The compromise of the confidentiality of personally identifiable information (PII) • Loss of data that results in, or there is a reasonable basis to conclude has resulted in, the unauthorized acquisition of PII • Access to PII for an unauthorized purpose • Access to PII that is in excess of authorization

In addition to the classification of incidents listed above, incidents are also described in terms of levels of severity (low, medium, or high), with associated reporting requirements (see Figure 5 below). "The severity of an information security incident determines the priority and resources necessary to handle the incident" as well as "the timing and extent of the response, the documentation and communications."[363] Assigning a level of severity to an incident is a subjective process, but agencies consider such factors as threat to human safety, scope of the impact (e.g., number of critical systems, services), sensitivity of the information (e.g., PII), and legal obligations and risks, among others.[364]

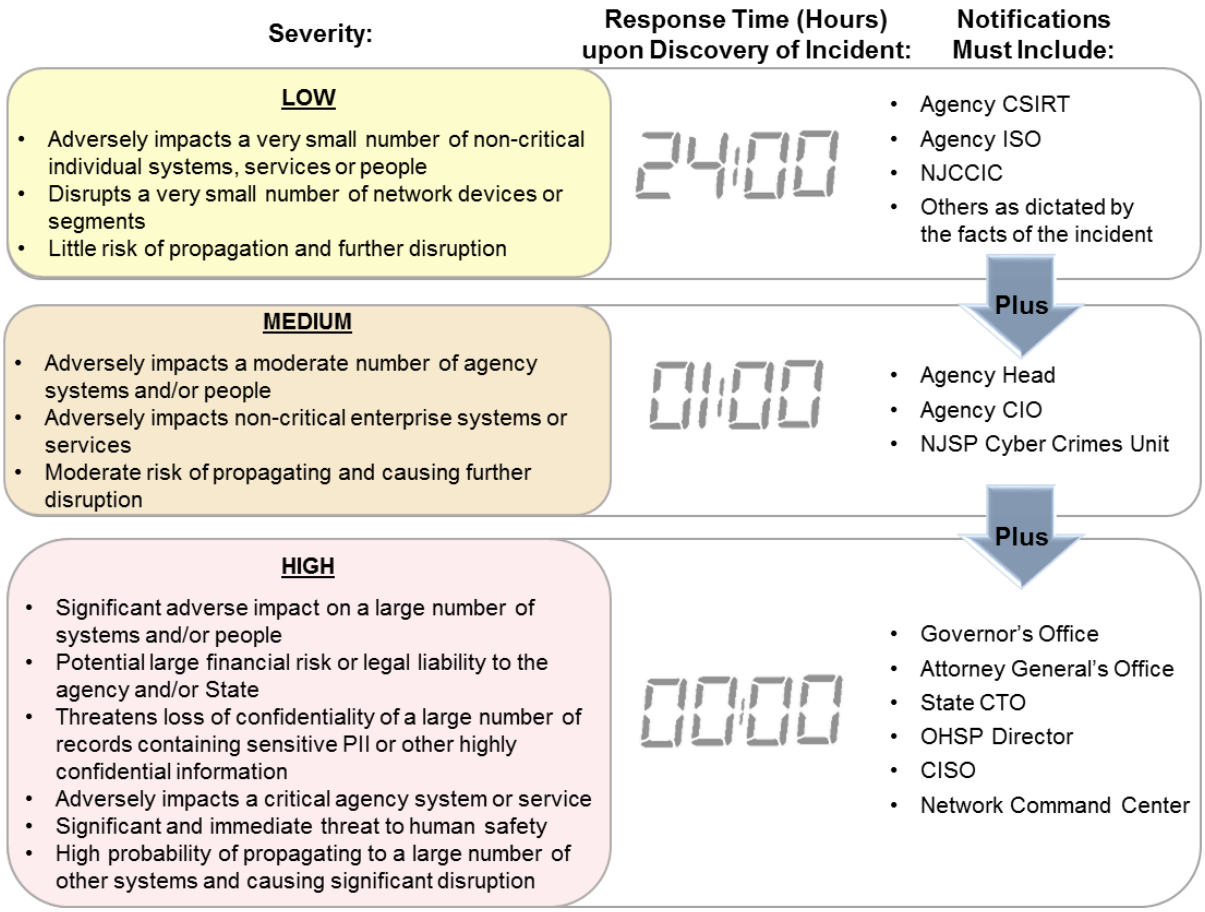


Figure 5. Levels of Severity and Notification Requirements

Once an incident is reported to the CSIRT, members act to:

- Validate the reported incident,
- Determine the type, severity, and priority of the incident, and
- Notify the CSIRT coordinator or an authorized designee of the incident.

The agency CIO, ISO, or an authorized designee will act as the Incident Coordinator, determine which CSIRT members play an active role in the investigation and:

- Coordinates the agency's response efforts,
- Engages auxiliary agencies and resources as necessary,
- Escalates incidents to executive management as appropriate,
- Monitors progress of the response,
- Ensures evidence gathering, chain of custody, and preservation is appropriate, and
- Prepares a written summary of the incident and corrective action taken.[365]

If an incident is too large for the agency CSIRT to address, the NJCCIC provides incident response assistance. However, if the CSIRT determines the agency has experienced a data breach, the agency is required to notify the NJCCIC in accordance with the New Jersey Identity Theft Prevention Act.[366] The agency leader, ISO, and CIO should also be notified. The NJCCIC, in turn, notifies the State Police Cyber Crimes Unit and the Office of the Attorney General "for legal counsel and guidance in determining the agency's notification responsibilities and response process."[367]

V. Information Sharing

The Challenge:

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

Features of New Jersey's Governance Approach:

- An array of governance mechanisms enables different types of information sharing across government, public, and private organizations.
- NJCCIC is the central information sharing body in the state.
- Two formal bodies, created by law, include private sector stakeholders to raise cybersecurity issues to the attention of executive branch leaders.

New Jersey utilizes an array of governance mechanisms to share different types of information across government, public, and private organizations (see Table 2 below for a summary of various information sharing entities).

Table 2. Summary of Information Sharing Entities

Information Sharing Entities	Type of Information Shared	Target Audience
NJCCIC	Cybersecurity operational and intelligence information	State, local, and federal governments; private sector entities
FS-ISAC	Cyber threats and intelligence information related to financial services industry	Private sector financial institutions and state government (police, attorney general)
DSPTF	Cyber risks to essential state/local services (such as healthcare, transportation, telecommunication services)	State government and the public
IAC	Cybersecurity trends and best practices related to critical infrastructure	Private sector critical infrastructure owner/operators

The NJCCIC is the central cybersecurity information sharing and analysis organization in the state, as well as the hub for cyber operations and resources. The NJCCIC is located at the Regional Operations Intelligence Center (ROIC), which is operated by the Division of State Police and serves as the state's fusion center and emergency operations center.[368] The NJCCIC

monitors the state's network for possible cyber-attacks and identifies and analyzes data to determine type of threat, level of severity of threat, threat sources, and potential impacts to stakeholders. The NJCCIC then shares that data and analysis with various stakeholders. In addition to the NJCCIC, New Jersey utilizes a task force and committee to incorporate private sector perspectives on information sharing.

The state's CISO leads the NJCCIC, which is comprised of "appropriate representatives of State entities, including the [OHSP], Office of the Attorney General, Division of State Police, and [OIT] as well as local, county and federal partners and private sector entities as deemed appropriate by the Director of [OHSP]."[369] The NJCCIC includes stakeholders from the public and private sectors, including more than 39 states, 42 federal agencies, state executive departments and agencies, local governments, 13 countries (such as the United Kingdom, Australia, and Germany), and many companies.[370]

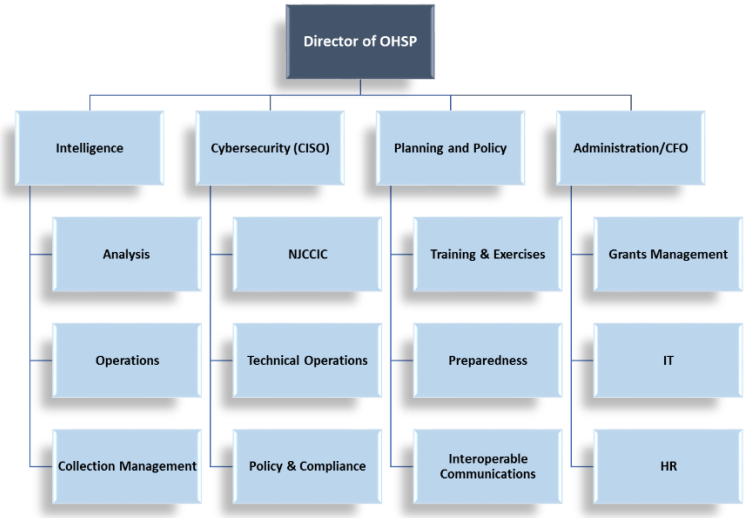


Figure 6. New Jersey Office of Homeland Security and Preparedness[371]

The NJCCIC was intentionally designed as an information sharing body to quickly pass information along to a variety of public and private stakeholders (see Figure 7 below). Within the NJCCIC, the Security Engineering and Cyber Operations (SECOPS) monitors the state's network for attacks. The SECOPS assesses the attacks, vetting them to determine if they are important enough to pass along to NJCCIC stakeholders. The partnerships bureau pushes information out to NJCCIC stakeholders.

Figure 7. NJCCIC Organizational Chart (as of September 2017)

One way the NJCCIC engages with private sector partners is though the FS-ISAC. Reflective of the large financial services industry in New Jersey, which grew in size and scale following the 9/11 attacks in New York City, the NJCCIC formed a partnership with the FS-ISAC "to share and analyze cyber threat information on behalf of New Jersey's banking institutions."[372] The terms of the NJCCIC/FS-ISAC agreement call for NJCCIC cyber threat analysts to "correlate data from various global financial institutions to identify trends, adversary tactics and vulnerabilities." [373]

In addition, there are two formal bodies with information sharing responsibilities—a task force and a committee—created by law that include private sector participants. The task force and committee provide an opportunity for private/public discussion and information sharing between state officials and private sector stakeholders. In 2001, the legislature passed the New Jersey Domestic Security Preparedness Act, which established the DSPTF.

DSPTF duties include identifying and assessing "potential risks to the domestic security and well-being of New Jersey's citizens, including risks to, and disruptions of, essential State and local infrastructures, transportation networks, public and private telecommunications and and the IAC. The law is significant because it offers two formal mechanisms for private sector stakeholders to raise cybersecurity issues to the attention of executive branch leaders.

The DSPTF was originally created to coordinate and supervise all activities related to domestic preparedness for a terrorist attack. In 2015, the former OHSP Director Chris Rodriguez expanded the DSPTF's mission to include cybersecurity.[374] The DSPTF resides within the OHSP, meets monthly, and liaisons with the federal Homeland Security Council.[375] The DSPTF is comprised of nine members: the Superintendent of State Police or designee, the Attorney General or designee, the Adjutant General of Military and Veterans' Affairs or designee, the Commissioner of Transportation or designee, the Commissioner of Health and Senior Services or designee, the Coordinator of the Office of Recovery and Victim Assistance, and three public members appointed by the Governor, with the advice and consent of the Senate.

information networks, financial systems and networks, the delivery and availability of essential health care services, and the potential impact of terroristic chemical, biological and nuclear attacks or sabotage."[376]

In addition to the DSPTF, the law established the IAC to act as a liaison to private industry and state and local officials "regarding domestic preparedness and the respective roles and responsibilities of the public and private sectors…"[377] IAC members include representatives from "gas, water, electric and utilities, nuclear facilities, and the telecommunications, transportation, health care, chemical, and pharmaceutical industries…among others."[378]

The Director of OHSP is co-chair of the IAC, along with a representative from the private sector. The IAC meets once a quarter and includes approximately 40 private sector stakeholders (e.g., Jersey Central Power and Light, Johnson & Johnson, Prudential).[379] The IAC discusses cybersecurity trends and, working with private sector members, authors best practices and guidelines. The IAC is of value to private sector members, in part, because the state of New Jersey can offer security clearances to qualifying businesses, enabling them to read classified information on a need-to-know basis.[380]

VI. Workforce & Education

The Challenge:

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

Features of New Jersey's Governance Approach:

- New Jersey has begun to address some cybersecurity workforce and education issues and the forthcoming Cybersecurity Strategic Plan prioritizes those issues.
- In 2017, New Jersey partnered with the SANS Institute, a nonprofit organization offering online access to free courses.
- OIT policy directs department or agency CISOs to implement and promote information security awareness within their respective organizations.

New Jersey has begun to address some cybersecurity workforce and education issues through discrete initiatives. The forthcoming NJ State Cybersecurity Strategic Plan intends to address workforce development and cybersecurity education issues in a more comprehensive manner. The plan includes, for example, the development of a capable cybersecurity workforce, a cybersecurity curriculum, and a statewide cybersecurity alliance, among other initiatives.[381]

In August 2017, Governor Christie partnered with the SANS Institute, a nonprofit cooperative research and education organization, to establish SANS Cyber Aces Online, an open, free, comprehensive program of online courses. The partnership was formed to address the skills gap in cybersecurity. The coursework was created by the SANS Institute for:

- High school students
- High school teachers and administrators
- College students
- Military veterans
- Active military
- Job seekers
- Career changers

Although the courses are open to anyone, registration is required to participate in the quizzes. SANS donated the courses to the Cyber Centers (called the SANS Cyber Aces Online), and the program provides an overview of the "core concepts needed to assess, and protect information security systems."[382] Example online courses include network fundamentals, operating systems, and system administration.

To address cybersecurity education among state employees, OIT policy directs department or agency CISOs to implement and promote "information security awareness within their respective agency." [383] In addition, the Director of NJCCIC is directed under OIT policy to draft and implement "an information security awareness and training program to be used by all State agencies."[384]

VII. Acronyms

Acronym	Definition
CDO	Chief Data Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CS&C	Office of Cybersecurity and Communications
CTO	Chief Technology Officer
CSIRT	Cybersecurity Incident Response Team
DoS	Denial of Service
DHS	Department of Homeland Security
DSPTF	Domestic Security Preparedness Task Force
FFRDC	Federally Funded Research and Development Center
FS-ISAC	Financial Services Information Sharing and Analysis Center
GRCB	Governance Risk and Compliance Bureau
HSSEDI	Homeland Security Systems Engineering and Development Institute
IAC	Infrastructure Advisory Committee
ISO	Information Security Office
IT	Information Technology
NASCIO	National Association of State Chief Information Officers
NJCCIC	New Jersey Cybersecurity & Communications Integration Cell
OHSP	Office of Homeland Security and Preparedness
OIT	Office of Information Technology
OMB	Office of Management and Budget
ROIC	Regional Operations Intelligence Center
SECOPS	Security Engineering and Cyber Operations
SLTT	State, Local, Tribal & Territorial
SAR	Systems Architecture Review

Cybersecurity Governance in the Commonwealth of Virginia

A CASE STUDY

December 2017

Homeland Security

NASCIO
Representing Chief Information Officers of the States

Virginia Fast Facts[385,386]

ELECTED OFFICIALS:

- Governor Terry McAuliffe
- Virginia House of Delegates: 100 Delegates
- Senate of Virginia: 40 Senators

STATE CYBERSECURITY EXECUTIVES:

- Secretary of Technology Karen Jackson
- Chief Information Officer (CIO) Nelson Moe
- Chief Information Security Officer (CISO) Mike Watson[387]

STATE DEMOGRAPHICS:

- Population: 8,100,653
- Workforce in "computers and math" occupations: 4.8%

EDUCATION:

- Public with a high school diploma: 45.3%
- Public with an advanced degree: 42.2%

COLLEGES AND UNIVERSITIES:

- 23 community colleges
- 16 public universities
- 96 private or out-of-state institutions certified to operate in Virginia

KEY INDUSTRIES:

- Food Processing
- Aerospace
- Plastics and Advanced Materials
- Data Centers
- Information Technology
- Cybersecurity
- Life Sciences
- Automotive
- Energy

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 Virginia'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 the cybersecurity priority 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 the Commonwealth of Virginia (the Commonwealth) 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 Virginia 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.[388]

This case study is part of a pilot project intended to demonstrate how states use 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 this case covers a broad range of areas, each related section provides an overview of the Commonwealth's governance approach, rather than a detailed exploration. Individual states and organizations seeking greater detail would likely need to engage directly with the Commonwealth to better understand how to tailor solutions to their specific circumstances.

In recent years, the Virginia executive and legislative branches have taken a series of deliberate steps to govern cybersecurity as an enterprise-wide strategic issue across both state government and a diverse set of private and public sector organizations. (In this case study, "agency" refers to executive branch agencies.)

In 2003, the General Assembly passed major legislation consolidating information technology (IT) services from across the Commonwealth into one agency—the Virginia Information Technology Agency (VITA).[389] VITA is led by the Chief Information Officer (CIO), who works with

a Chief Information Security Officer (CISO) to address cybersecurity issues.[390] VITA is charged with overseeing the Commonwealth's IT infrastructure, including establishing information security programs, for the executive branch departments and agencies. VITA also oversees IT investments and acquisitions on behalf of state departments, agencies, and institutions of higher learning.

The Commonwealth also utilizes a range of governance structures and processes to address a variety of cybersecurity challenges that require collaboration and coordination across public and private stakeholders. For example, the Commonwealth approached cybersecurity strategic planning in a collaborative manner, inviting public and private stakeholders together in two different structures created by law. In 2014, Governor Terry McAuliffe created the first structure, called the Virginia Cyber Security Commission (the Commission), via Executive Order 8.[391] The Commission, co-chaired by Richard Clarke and Secretary of Technology Karen Jackson, was comprised of public and private sector experts, including the Secretaries of Commerce and Trade, Public Safety and Homeland Security, Education, Health and Human Resources, Veterans and Defense Affairs, and 11 citizens appointed by the Governor. The citizens represented private industries such as a global credit card company, a large law firm, and defense and aerospace companies. The Commission members developed a set of 29 recommendations: to improve the resilience and protection of the Commonwealth's information systems; invest in cyber education and workforce development; increase public awareness of cybersecurity as an issue worthy of prioritization and investment; sustain and expand economic development of cyber-related industries; and modernize state laws to address cybercrimes (see Section VII for more details).[392] These policy recommendations have influenced a range of investment and programmatic priorities for the state.

The Commonwealth also utilizes several intra-governmental, cross-agency advisory groups, councils, and working groups to identify laws and policies that may need to change to align with the Commonwealth's cybersecurity risk management approach. For example, the Cyber Response Working Group (CRWG) is a cross-agency working group focused on planning and preparation for cyber incidents that could negatively impact the public's safety. Originally formed by the Virginia National Guard (VANG) to examine how the Guard could support Virginia's cybersecurity efforts, the CRWG has since expanded in scope to oversee initiatives such as the creation of Virginia's first Cyber Incident Response Plan. Members of the CRWG include the Office of Public Safety and Homeland Security, VANG, Virginia Department of Emergency Management (VDEM), VITA, the Virginia State Police (VSP), and the Virginia Fusion Center (VFC).

To facilitate information sharing with the private sector, the Virginia Cyber Security Partnership (VCSP), a partnership between VITA and the Federal Bureau of Investigation (FBI) with approximately 220 private sector entities (such as major critical infrastructure owner/operators, retailers, and healthcare providers, among others), and the public sector (see Figure 3 in Section V for an overview of membership).[393] The purpose of the VCSP, created in March 2012, is to establish a trusted environment where public and private entities can share cyber threat information. The VCSP gathers cyber professionals from across industries in a trusted environment to share information and lessons learned about topics such as threat intelligence, credential management, and supply chain security. [394] The VCSP includes three advisors/liaisons: the FBI, the VITA CISO, and a representative from a large power company.[395]

To address the need for a skilled, cyber-ready workforce, the Commonwealth initiated a partnership between the state, academia, and the private sector to develop the Virginia Cyber

Range (Cyber Range). The Cyber Range is a virtual, cloud-based environment designed to enhance cybersecurity education in Virginia's high schools, colleges, and universities.[396] The Cyber Range is operated within Virginia Polytechnic Institute and State University (Virginia Tech) and is "led by an executive committee representing public institutions that are nationally recognized centers of academic excellence in cybersecurity within the Commonwealth of Virginia."[397]

Cybersecurity is a challenge that cuts across many issues and many interdependent stakeholders. The Commonwealth uses a range of governance mechanisms to work across different public, private, academic, and nonprofit organizations. Leadership on the part of individuals, including the Governor and the legislature, who made cybersecurity and cybersecurity governance a priority across government, public, and private organizations was very important. However, leadership was not everything. As the Commonwealth illustrates, the priority was translated into tangible laws, policies, structures, and processes that aligned cybersecurity governance with broader cybersecurity priorities.

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.[398]

The case study explores cross-enterprise governance mechanisms used by Virginia 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 Virginia's governance approach, rather than a detailed exploration. Individual states and organizations seeking greater detail would likely need to engage directly with Virginia to better understand how to tailor solutions to their specific circumstances.

DHS' Office of (CS&C) Cybersecurity and Communications 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."[399] The Homeland Security Systems Engineering and Development Institute (HSSEDI), a DHS owned Federally Funded Research and Development Center (FFRDC), developed the report and 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 Virginia's Governance Approach:

- The Commonwealth centralizes cybersecurity strategy and planning activities under the Secretary of Technology and the state Chief Information Officer (CIO).
- The Commonwealth uses intra-agency working groups and councils as well as private sector advisory groups to help prioritize actions to address cybersecurity risks.
- The Governor created a temporary structure via executive order—the Virginia Cyber Security Commission—comprised of public and private stakeholders to study and make recommendations to improve the Commonwealth's overall cybersecurity posture.

The Commonwealth uses several governance mechanisms to bring multiple public and private stakeholders into the strategy and planning process and drive cross-enterprise strategy. Commonwealth government cybersecurity strategy and planning activities are centralized by law under the Secretary of Technology, who oversees VITA, and to whom the state's CIO reports.[400] The law directs the Secretary of Technology to "review and approve the Commonwealth strategic plan for information technology," which is developed and recommended by the CIO and includes cybersecurity activities.[401] The CIO collaborates with and collects inputs from the CIO Council's Customer Advisory Council, "a workgroup of agency technology representatives, and IT subject matter experts," to draft the strategic plan.[402]

The 2014-2016 strategic plan sets the overall direction and "establishes the basis for the scoring, ranking and evaluation process to ensure alignment of proposed IT investments to the Commonwealth vision" which, in turn, "determines whether the commonwealth CIO approves or disapproves the IT investments."[403] The Commonwealth's vision is to leverage technology to enable "far-reaching business solutions that benefit all constituents."[404] In the CY2017 update to the 2014-2016 strategic plan, cybersecurity is reflected in two of the six priorities:

1. Move to cloud application hosting,
2. Provide secure wireless access within state office buildings for employees and the public,
3. Provide greater internet access and bandwidth to meet demand,
4. Support delivery of critical digital services to agencies and constituents,

5. Implement IT infrastructure transition successfully, and
6. Implement shared security services (assist agencies with identifying and managing security needs via shared services such as Centralized Information Security Officer, Centralized IT Security Audit, and the Security Incident Management).[405]

The CIO considers these six priorities when evaluating IT investment requests from the Commonwealth's agencies and departments. Investment proposals need to align with the strategic plan's vision and stated IT priorities to obtain CIO approval.

The Commonwealth also uses advisory councils and commissions to inform cybersecurity priorities. The law directs the Secretary of Technology to engage with a variety of agencies, councils, and boards in setting strategy and direction. They include the Information Technology Advisory Council (ITAC).[406] The ITAC is an advisory council within the executive branch of state government and is "responsible for advising the CIO and the Secretary of Technology on the planning, budgeting, acquiring, using, disposing, managing, and administering of information technology in the Commonwealth."[407] The ITAC, which includes membership from across government and the private sector, advises and influences the Commonwealth's strategy to address cybersecurity issues.

In 2014, the Commonwealth approached cybersecurity strategic planning in a collaborative manner, inviting public and private stakeholders together in two different structures created by law. The Governor created the Virginia Cyber Security Commission (the Commission), via Executive Order 8.[408] The Commission, co-chaired by Richard Clarke and Secretary of Technology Karen Jackson, was comprised of public and private sector experts, including the Secretaries of Commerce and Trade, Public Safety and Homeland Security, Education, Health and Human Resources, Veterans and Defense Affairs, and 11 citizens appointed by the Governor. The citizens represented private industries such as a global credit card company, a large law firm, and defense and aerospace companies.

The Commission members developed a set of recommendations to improve the resilience and protection of the Commonwealth's information systems; invest in cyber education and workforce development; increase public awareness of cybersecurity as an issue worthy of prioritization and investment; sustain and expand economic development of cyber-related industries; and modernize state laws to address cyber crimes.[409] Secretary of Technology Karen Jackson characterized the Commission's recommendations and report as a "game changer" for those advocating for changes in law to support cybersecurity-related investments, describing it as a "grounding document" that influenced decisions on budget, policy, and the law.[410] For example, recommendations related to education and workforce development led directly to the creation of the Cyber Range and the Virginia Cybersecurity Public Service Scholarship Program, which awards $20,000 per year, for up to two years, to eligible Virginia students studying cybersecurity.[411] The Commission has seen many of its recommendations implemented since 2016 and continues to influence executive and legislative actions today.

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 Virginia's Governance Approach:

- IT budget requests from state departments and agencies are reviewed and approved by the CIO and Chief Information Security Officer (CISO) to ensure adherence to cybersecurity priorities, policies, and standards.
- Central acquisition processes are used to manage cybersecurity risks and ensure that cybersecurity requirements are adopted across government agencies.
- Standard vendor contract language is used to ensure adherence to information security standards.

The Commonwealth uses its budget and acquisition governance processes to drive cross-government implementation of cybersecurity standards and priorities. The Commonwealth provides state funding through the annual budget process (called the Governor's budget bill). While departments and agencies each receive their own IT budget on an annual basis, budget requests for IT projects, including those that may introduce cyber risks to the Commonwealth's enterprise, are overseen by the CIO, with consultation from the CISO. The CIO ensures that budget requests and acquisitions are aligned with the Commonwealth's IT strategic direction and with cybersecurity policies and standards developed by the CISO.

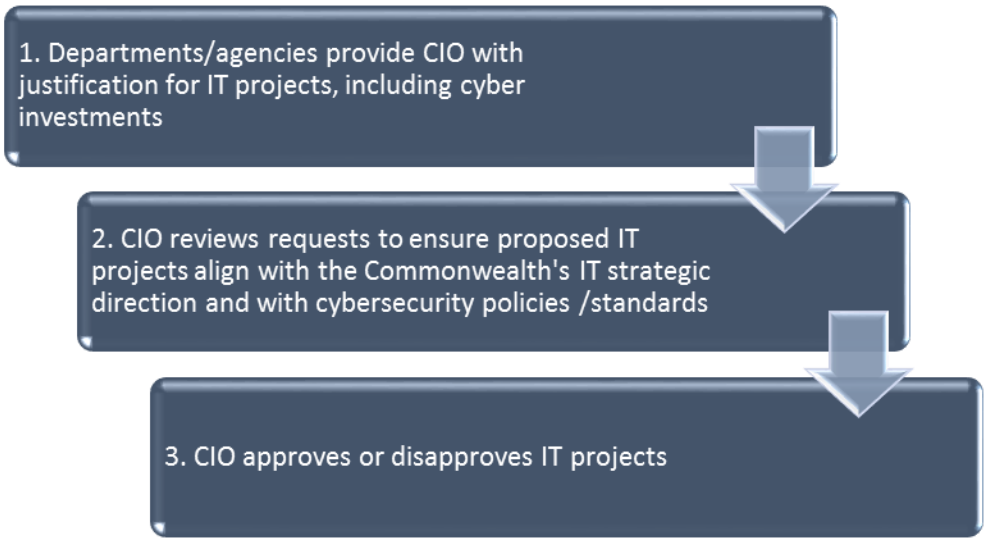


Figure 1. High-Level Overview of Annual Commonwealth Budget Processes Related to Cybersecurity Funding

As shown in Figure 1, the law directs departments and agencies to provide the CIO with justification for IT projects, including cyber investments, as part of the Governor's budget bill.[412] The CIO reviews agency requests for cyber investments as part of the annual budget process and has the authority to approve or disapprove them. This means that agency and department requests for IT projects, including proposed acquisitions for products/services from outside vendors, must adhere to IT security standards set by the CISO. And the CIO reviews proposed projects to ensure adherence to current IT policies and standards. According to CIO Nelson Moe, "the advantage in Virginia is that the state is consolidated"—all agency procurement comes through VITA, which, in turn, allows the CIO to manage cybersecurity risks associated with vendor products and services.[413]

The Commonwealth intentionally designed the acquisition process to ensure that all outside vendors adhere to cybersecurity standards. First, the Commonwealth has a single vendor contract in place with Northrop Grumman to provide the bulk of IT products and services, including cybersecurity services, for all state departments and agencies. Most IT services and products for the Commonwealth's IT infrastructure are provided through this contract, allowing the CIO to enforce and manage cybersecurity standards across the Commonwealth's enterprise. The CIO manages the vendor contract and requests to purchase goods and services outside of the contract. If a department or agency requests a product or service outside of the contract, there is an extensive process to vet vendors to ensure that cybersecurity standards are met. Before an IT product or service is acquired, "we have a list of 150–200 questions we ask vendors to respond to," said Commonwealth CISO Mike Watson.[414] All acquisition exception requests must meet cybersecurity protocols and be approved by the CIO.

Second, standard information security contract language is included in the terms and conditions of all vendor contracts, including the single vendor contract. This contract feature ensures that the Commonwealth works only with vendors that can provide products and services that meet the cybersecurity policies and standards put forth by VITA. The acquisition process "works well and is flexible to meet emerging demands for new products or services, such as cloud services," Watson said.[415]

III. Risk Identification & Mitigation

The Challenge:

How to identify and mitigate cybersecurity risks across multiple public and private organizations?

Features of Virginia's Governance Approach:

- Risk identification and mitigation functions are centralized in the Commonwealth through the CIO and CISO, who develop policies, standards, and guidelines to identify and address cyber risks in state departments and agencies.
- Smaller departments and agencies can access CISO expertise through a shared services model offered by VITA.
- Standing advisory councils that include public and private representation identify and address cyber risks that go beyond the state government.

The VITA CIO and CISO lead cyber risk identification and mitigation functions across Commonwealth government departments and agencies. The Commonwealth also utilizes intra-governmental, cross-agency advisory groups, councils, and working groups to evaluate laws and policies that may need to change to align with the Commonwealth's risk management posture.

In 2003, the General Assembly passed major legislation reorganizing nearly all IT infrastructure and telecommunications services across the Commonwealth into one agency—VITA. The Commonwealth Security and Risk Management (CSRM) Directorate, a unit within VITA, is led by the Commonwealth's CISO.[416] The CSRM executes many CIO-related risk identification and audit activities.[417] For example, the CSRM assesses the strength of Commonwealth agency and department IT security programs through regular security audits. Results of the audits are compiled and published in an annual Commonwealth of Virginia Information Security Report. If an information security audit finds inadequate security, the CISO discourages the agency/department from beginning new IT investments until the information security issues and risks are remedied.[418] This process helps ensure that agencies prioritize funds to mitigate risks prior to receiving additional resources.

In 2014, the Commonwealth adopted the National Institute of Standards and Technology Cybersecurity Framework to "enhance the systematic process for identifying, assessing, prioritizing and communicating cybersecurity risks, efforts to address risks, and, steps needed to reduce risks as part of the state's broader priorities."[419] The Commission (described in Sections I and V) called on VITA to "evaluate the

maturity level of state agencies cyber security programs and practices by leveraging the Framework as a means of assessment" on an annual basis.[420]

As part of VITA's ongoing risk identification and mitigation responsibilities, the CIO must "identify annually those agencies that have not implemented acceptable policies, procedures, and standards to control unauthorized uses, intrusions or other security threats."[421] Noncompliant agencies are identified by evaluating information security audit, risk, and threat management programs.[422] CISO Mike Watson noted, "We have a risk database of all our findings" detailing the agencies/departments that fail to meet security standards.[423] The CISO performs a mid-year preliminary assessment before the end-of-year audit, which allows agencies that may not be in compliance mid-year approximately six months to address security issues. Lee Tinsley, CIO of the Department of Veterans Services, said, "Agencies get on the wall of shame because they fall out of compliance."[424] The CISO, agency head, and agency Information Security Officer (ISO) then work together to address the issues.[425] The risk database helps the CISO and CIO track the risks and ensure that they are remediated over time. This, in turn, provides the CIO and CISO situational awareness to ensure compliance across the state government enterprise.

In addition to ongoing risk management activities, VITA has undertaken some important one-time actions. In August 2015, the Governor signed Executive Directive 6 furthering the Commonwealth's risk management of protected, sensitive data from potential data breach. The Directive was intended to "strengthen the Commonwealth's cybersecurity measures to protect personal information and sensitive data" and decrease the risk of data breach.[426] Per the Directive, VITA conducted an inventory of Commonwealth data and computer systems to determine their sensitivity and criticality and recommended "strategies to strengthen and modernize agencies' cyber security profiles."[427] The VITA data inventory revealed that the Commonwealth processes billions of records each year that contain sensitive data, such as personally identifiable information, federal tax information, and payment card industry data. Moreover, VITA found that more than 1,000 IT systems across the Commonwealth's agencies and departments store sensitive data. The results of the VITA data inventory led to several risk management recommendations to strengthen controls to protect sensitive data stored on Commonwealth IT systems and networks. Many of the recommendations have been, or are in the process of being, adopted.

Recognizing that not all departments and agencies are large enough to support a full-time CISO, VITA offers smaller agencies and departments access to CISO expertise through a shared services model. Agencies and departments can contract with VITA as needed to obtain assistance with cyber-related administrative, technical, and/or operational matters. This service provides needed assistance without the cost of keeping a full-time CISO on staff. The shared CISO services model was a recommendation from the Commission and was implemented by the VITA.

Standing intra-governmental working groups are also used to identify cyber risks. The Secure Commonwealth Panel (SCP), for example, is a legislatively created standing advisory group tasked with reviewing and identifying laws and policies that may need to change to address public safety and homeland security issues in the Commonwealth. By statute, the SCP consists of 36 members from the legislative and executive branches as well as private citizens and is chaired by the Secretary of Public Safety and Homeland Security.[428] Recognizing the threat cyber poses to public safety, the SCP formed the Cyber Security Sub-Panel to evaluate whether to amend Virginia's laws and policies regarding

cyber crime, critical infrastructure, and law enforcement. The Cyber Security Sub-Panel meets quarterly and is comprised of members of the Governor's Cabinet, Virginia's Legislature, representatives from a variety of state agencies, and private citizens.[429] Recommendations are passed to the Secretary of Public Safety and Homeland Security and the SCP, who shares them with the Governor and, where appropriate, the General Assembly.

As mentioned earlier, the CRWG is a multi-agency working group focused on planning and preparation for cyber incidents that could negatively impact the public's safety. Originally formed by the Virginia National Guard (VANG) to examine how the Guard could support Virginia's cybersecurity efforts, the CRWG has since expanded in scope to oversee initiatives such as the creation of Virginia's first Cyber Incident Response Plan. Members of the CRWG include the Office of Public Safety and Homeland Security, VANG, Virginia Department of Emergency Management (VDEM), VITA, the Virginia State Police (VSP), and the Virginia Fusion Center (VFC).

IV. Incident Response

The Challenge:

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

Features of Virginia's Governance Approach:

- VITA leads non-emergency cyber incident response.
- A unified command (UC) structure integrates cyber emergency response with the existing emergency management response.
- The cyber UC structure includes VITA, Virginia Department of Emergency Management (VDEM), Virginia State Police (VSP), and the affected entity to manage emergency cyber incident response.
- The Commonwealth uses an advisory panel of public and private stakeholders to regularly assess emergency response activities, including cybersecurity.

The Commonwealth utilizes laws and policies to clarify incident response governance. The laws establish foundational roles, responsibilities, and processes that all Commonwealth agencies and departments must follow to report non-emergency and emergency incidents. These laws and supporting policies describe what constitutes a cyber incident, what criteria is used to evaluate the severity of an incident and defines the roles and responsibilities of agencies tasked with resonding to an incident.

VITA defines a cyber incident as an event that threatens to do harm, attempts to do harm, or does harm to the system and/or network.[430] A cyber event "is any observable occurrence in a system, network, and/or workstation."[431] Example events include a system crashing and rebooting, unwanted emails bypassing firewalls and being delivered, and packets flooding the network. VITA directs agencies and departments to record events to determine "the baseline for normal activity on systems/networks" so that if events rise to an incident, "corroborating evidence is available" for investigative and possible law enforcement purposes to understand the deviation from the norm. For example, malware and denial-of-service attacks are characterized as incidents.

If the cyber incident occurs on the state network, VITA is the lead agency that manages the response. The Commonwealth's IT Incident Response Policy, which is drafted by VITA, specifies that all agencies "document and implement threat detection practices; information security monitoring and logging practices; and information security incident handling practices."[432] VITA incident response policy instructs departments and agencies to conduct incident response tests/exercises at least once a year "to determine the incident response effectiveness and document the results."[433] VITA also reviews and approves IT disaster recovery and continuity plans

developed and maintained by all executive agencies.

When cyber incidents occur, agency directors must, by law, report them to VITA within 24 hours "from when the department discovered or should have discovered their occurrence."[434] While department or agency directors track events to identify the "norm," there are specific conditions that trigger an incident that should be reported to the VITA CIO. VITA specifies that agencies report incidents that "have a real impact on your organization" such as "detection of something noteworthy or unusual (new traffic pattern, new type of malicious code, specific IP as source of persistent attacks)."[435] VITA incident response guidelines specify reportable incidents to include:[436]

- An adverse event to an information system, network, and/or workstation; OR
- Exposure, or increase risk of exposure, of Commonwealth data; OR
- Threat of the occurrence of such an event or exposure.

VITA provides agencies and departments with an online Information Security Incident Reporting Form to capture, organize, and analyze reported incidents from across the enterprise.[437] The VITA Commonwealth's Security Incident Response Team (CSIRT) categorizes each security incident based on the type of activity.[438]

The VITA Computer Incident Response Team (CIRT) coordinates all reported incidents from across the Commonwealth's agencies and departments.[439] The CIRT is comprised of the agency/department ISO and the VITA CSRM incident management staff. The CIRT, agency management, and the ISO determine whether the incident requires an immediate response.

If the cyber incident is deemed an emergency or impacts local or private critical infrastructure, the incident is managed through a Unified Command (UC) structure (see Figure 2 below), which "is scalable and may be adjusted to accommodate unique requirements or incident complexity."[440] An emergency is defined by law as "any occurrence, or threat thereof, whether natural or man-made, which results or may result in substantial injury or harm to the population or substantial damage to or loss of property or natural resources."[441]

The UC structure is led by the VDEM Virginia Emergency Support Team (VEST), which "coordinates the response to and recovery from the overall emergency and any cascading effects of the incident" within the UC.[442] VDEM also provides resources and emergency management expertise for local and state governments to prevent, prepare for, and respond to incidents. The cyber-specific response is led by a Cyber Unified Coordination Group (Cyber-UCG), which aligns with the overall emergency management VEST (see Figure 2 below).[443]

The Cyber-UCG is composed of five entities: VITA, VDEM, VSP, VFC, and the affected entity. Roles and responsibilities for cyber incident response are broken down by agency. The VITA CISO oversees the protection of Commonwealth networks and lends its technical expertise to the Cyber-UCG during response operations. VSP is the lead agency for threat response, "overseeing and coordinating" cyber criminal investigations.[444] VDEM manages asset response, or the coordination or resources to support cyber incident response. The VFC coordinates and disseminates non-sensitive/non-identifying information to Cyber-UCG agencies, federal agencies and/or private CI partners to ensure the response is timely and effective.

The VFC also collects and analyzes law enforcement information at the conclusion of an incident.[445] Finally, a representative from the affected entity, such as local government or a private sector organization, provides information regarding impacted systems. The

Cyber-UCG structure is scalable and applicable to both small- and large-scale incidents.

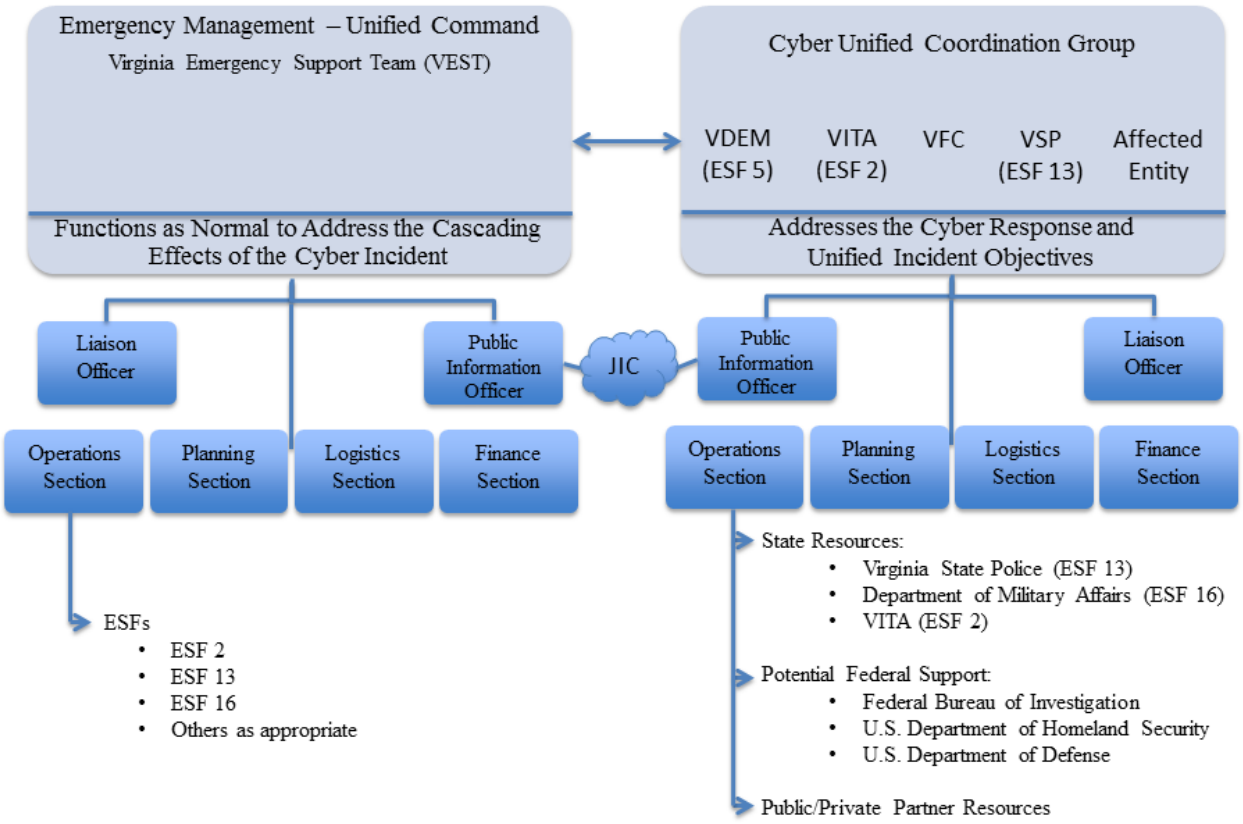


Figure 2. Virginia Unified Command Structure (DRAFT)

(Taken from the 2017 Commonwealth of Virginia, Department of Emergency Management "Cyber Incident Response Plan")

To manage an emergency response, local government officials and private companies may request state or federal assistance. To this end, the Governor may call on the Secretary of Public Safety and Homeland Security (PSHS) to provide additional resources, such as expertise housed within the Department of Military Affairs. PSHS serves as the Governor's Homeland Security Advisor and oversees 11 agencies, including VSP and the Department of Military Affairs, which includes VANG.[446] VANG can leverage cyber-trained personnel to help respond to an emergency cyber incident.[447] In addition, the VSP High-Tech Crimes (HTC) division may play a role in cyber-crime incident response by providing digital forensic analysis and investigative services to local, state, and federal law enforcement agencies.

The Commonwealth regularly assesses emergency response activities, including cyber incident response. The SCP, created by law in 2016, is an advisory body within PSHS and is chaired by the Secretary of Public Safety and Homeland Security. The 34-member SCP is charged with assessing "the implementation of statewide prevention, preparedness, response, and recovery initiatives" and making recommendations to the Governor to address emergency preparedness.[448] Members include representatives from the House and Senate, executive branch, and local governments; private citizens; the Attorney General; and the Lt. Governor. The SCP submits annual reports to the Governor outlining the Commonwealth's emergency preparedness efforts, including cybersecurity.

V. Information Sharing

The Challenge:

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

Features of Virginia's Governance Approach:

- The VITA CSRM provides the bulk of information sharing about operational issues to government departments and agencies.
- The VITA CSIRT distributes cyber intelligence to Commonwealth agencies and law enforcement.
- The VFC shares information about cyber threats across state, federal, and local governments.
- To facilitate information sharing about a broad range of cybersecurity topics with the private sector, the Commonwealth established the VCSP.

The Commonwealth utilizes an array of governance mechanisms to share different types of information across government, public, and private organizations (see Table 1 below for a summary of various information sharing entities).

Table 1. Summary of Information Sharing Entities

Information Sharing Entities	Type of Information Shared	Target Audience
VITA CSRM	Cybersecurity operational information	Departments and agencies
VITA CSIRT	Information security information	Agencies and state law enforcement
PSHS VFC	Cyber threat intelligence	State, local, and federal governments
VCSP	A broad range of cybersecurity information	Private sector

To support information sharing at the department and agency levels about a broad range of cybersecurity operational issues, the VITA CSRM conducts monthly Information Security Officers Advisory Group (ISOAG) meetings, which provide security training and facilitate knowledge exchange. "In 2015, more than 1,700 security professionals attended the ISOAG meetings."[449] The ISOAG meetings allow ISOs to "talk about the issues that are facing state agencies such as cloud security, lockdown of computers, lockdown of servers, compliance, latest security patches, and other day-to-day topics that are of concern to ISOs," said Lee Tinsley, CIO of the Department of Veterans Services.[450] In addition, the CSRM used the ISO

Security Council as a resource to assist in sharing best practices between agencies.

The CSIRT, also part of VITA, distributes "cyber intelligence information to both agencies and law enforcement within the commonwealth."[451] The CSIRT "develops relationships with state, Federal, and local partners" and regularly exchanges information about information security issues with these entities.[452]

The VFC also plays an important role by sharing information about cyber threats across state, federal, and local governments. Organized under PSHS, the VFC collects, analyzes, and shares "threat intelligence between the federal government and state, local, and private sector partners."[453] The VFC is physically located within VSP headquarters and collaborates regularly with the HTC division and VITA. The close proximity of the VFC with the VSP allows for "quick, ready access to investigators," which is a unique feature of state fusion centers. According to Rob Reese, manager of the Cyber Intelligence Unit at the VFC, this close collaboration improves the quality of threat analysis and allows law enforcement and prosecutors to work together more quickly at the inception of a suspected cyber crime, carefully collecting and inventorying evidence required to build a successful case.[454]

Although the VFC cyber capability is new, established in late 2016 and fully staffed in the first quarter of 2017, leaders plan to provide additional resources in the coming years to increase staff.[455] Today, the VFC is focused on identifying cyber threats to the Commonwealth's network, private companies doing business in the Commonwealth, localities, and private citizens, and sharing that information with VFC partners. As the VFC capability grows over the next several years, the focus will include "looking at the broader scope of what the state enterprise is experiencing in cyber-space," analyzing that information, and sharing it with public and private infrastructure owner/operators, the VSP HTC division, and VITA.[456]

To facilitate information sharing about a broad range of cybersecurity topics with the private sector, the Richmond FBI – in partnership with VITA and several private companies – formed the VCSP. The VCSP is a partnership of approximately 220 private sector entities (such as major critical infrastructure owner/operators, retailors, and healthcare providers), and the public sector (see Figure 3 below for an overview of membership). There are three VCSP advisors/liaisons: the FBI, the VITA CISO, and a representative from a large power company.[457] The VCSP gathers cyber professionals from across industries in a trusted environment to share information and lessons learned.[458] At the five meetings held each year, VCSP members collaborate to share threat intelligence and discuss credential management issues and risks associated with supply chain security.

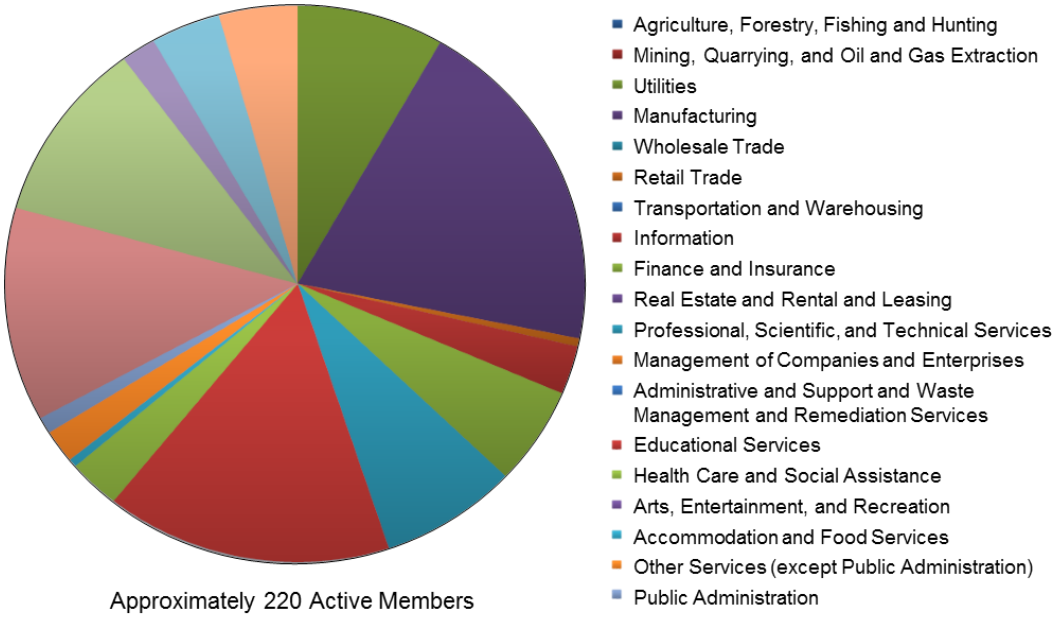


Figure 3. VCSP Membership Representation as of April 2016 [459]

In addition, the Commonwealth is in the process of expanding information sharing through an Information Sharing and Analysis Organization (ISAO).[460] In April 2015, the Governor signed an executive order "establishing the Nation's first state-level Information Sharing and Analysis Organization (ISAO)."[461] The ISAO is "intended to enhance the voluntary sharing of critical cybersecurity threat information in order to confront and prevent potential cyberattacks."[462] ISAOs are designed to "complement existing structures and systems that are used to share critical cybersecurity threat information across levels of government and industry sectors."[463]

VI. Workforce & Education

The Challenge:

How to work across multiple public and private organizations to shape responses to cybersecurity workforce shortages and education needs?

Features of Virginia's Governance Approach:

- The Commonwealth utilized several governance mechanisms and developed programs to strengthen partnership between government, higher education, and industry.
- The Commonwealth collaborated with institutions of higher education to create the Virginia Cyber Range, a virtual, cloud-based environment to enhance cybersecurity education in Virginia's high schools, colleges, and universities.
- Virginia's community colleges and industry have collaborated to instantiate apprenticeship and credentialing programs.
- VITA has leveraged its role across government to provide certification programs for existing state workers.

To address a talent gap in cyber-skilled workers, the Commonwealth used several governance mechanisms, and developed programs to strengthen partnership between government, higher education, and industry.[464] Many of these efforts were the result of the Commission (see Sections I and V), which made several recommendations to improve the cyber workforce.

To strengthen cybersecurity education, the Commonwealth developed a partnership with higher education institutions and created the Virginia Cyber Range in 2016. The Cyber Range is a virtual, cloud-based environment designed to enhance cybersecurity education in Virginia's high schools, colleges, and universities.[465] It was originally a recommendation put forth by the Commission in 2015. The General Assembly provided $4 million to support the Cyber Range and directed Virginia Tech to "serve as the coordinating entity."[466] "The Virginia Cyber Range is led by an executive committee representing public institutions of higher education that are nationally recognized centers of academic excellence in cybersecurity within the Commonwealth of Virginia."[467]

This education initiative includes teaching the teachers as well as the students. The Cyber Range offers two primary services: (1) a courseware repository providing teachers from high schools, colleges, and universities with access to standardized lessons to download and use in the classroom; and (2) access to the cloud (through Amazon Web Services) to host

cybersecurity labs and exercises for students.[468] The courses expose students to cybersecurity concepts, while the cloud-hosted lab environment allows students to practice those concepts in a hands-on environment. The goal is to provide teachers with courses and lessons contributed by any of the nine National Security Agency (NSA)/DHS Cybersecurity Centers of Academic Excellence (CAEs) in the Commonwealth to improve the quality and variety of cybersecurity education. Allowing teachers to share materials developed by CAEs reduces the amount of time and the associated cost to develop coursework. While the Cyber Range is currently only accessible to faculty members at Virginia public high schools and colleges, discussions are underway to determine whether materials could be made available to other states and interested parties on a fee basis.

The Commonwealth used governance mechanisms to promote collaboration between industry and higher education to support workforce development for new and existing workers. For new workers, in 2016 the General Assembly acted on a Commission recommendation and passed the New Economy Workforce Grant Program (NEWGP). The NEWGP allocates $12 million over two years to a variety of Virginia's community colleges to provide direct subsidies to students to cover a portion of the cost of obtaining industry credentials.[469,470] To implement this grant, "Virginia's Community Colleges consulted with Virginia businesses to develop the list of eligible credentials that can provide access to a wide variety of high-demand jobs, such as…computer network specialist…"[471] [472] In addition, there is a concerted effort to leverage the thousands of military Veterans in the Commonwealth to address cyber workforce shortages. For example, in 2016 the Governor announced "Cyber Vets Virginia," an initiative designed to provide Veterans with access to cybersecurity training opportunities and resources to encourage Veterans to enter the cyber workforce.[473] Cyber Vets Virginia offers access to free cyber training via private sector partners for eligible Veterans living in Virginia and interested in working in the cyber industry.[474]

To increase cyber skills across its government workforce, the Commonwealth leveraged the role of VITA. VITA instituted a policy requiring that all ISOs meet certification requirements and receive training to understand Virginia's information security policies and procedures. To help employees meet this requirement, the Commonwealth now offers an ISO Certification Program that is administered by the VITA CSRM. Since instituting the policy in 2015, the VITA CSRM has awarded 91 certifications, a 90 percent increase over 2013, before the policy was implemented.[475] "ISO certification is an important element of the commonwealth information security program [because it] demonstrates an understanding of information security risks and commitment to promoting information security in the commonwealth."[476]

Commission recommendations also led to a series of laws intended to help bring younger cyber-skilled employees into the state workforce. Specifically, the General Assembly passed a law establishing a scholarship program that provides two-year scholarships to college students who study cybersecurity in exchange for a commitment of two years of public service at a Virginia state agency.[477]

VII. Deep Dive: Virginia Cybersecurity Commission

Introduction

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

The Challenge

Cybersecurity risks within a state are realized across multiple public and private organizations. Developing a comprehensive, cross-sector approach to addressing these risks requires mechanisms to incorporate these various perspectives.

The Solution

In 2014, the Governor used executive order authority to establish the Virginia Cybersecurity Commission, a temporary body of experts from across the executive and legislative branches of government and the private sector. The Commission developed cross-cutting recommendations to strengthen cybersecurity across the Commonwealth, many of which have been implemented.

The Background

The Commission's objective was to create a list of actionable recommendations for the Governor and the General Assembly to consider to strengthen the Commonwealth's cybersecurity posture. Membership reflected the Commonwealth's understanding that cybersecurity is an issue that requires both public and private sector cooperation to address. Co-chair and Secretary of Technology Karen Jackson called the Commission and the resulting list of recommendations a "game changer" for those advocating for changes in law to support cybersecurity-related investments, describing it as a "grounding document" that influenced decisions on budget, policy, and the law.[478]

The Commission was comprised of the Secretaries of Technology, Commerce and Trade, Public Safety, Education, Health and Human Resources, Veterans Affairs, and Homeland Security, and 11 citizens appointed by the Governor. The latter represented private industries such as a global credit card company, a large law firm, and defense and aerospace companies, among others.[479]

Over two years, the Commission held nine meetings, several Working Group sessions, and nine Town Hall events to develop a set of recommendations. "There were five subcommittees, each focusing on a specific area of interest to the Commission…: (1) Infrastructure; (2) Education and Workforce; (3) Public Awareness; (4) Economic Development; and (5) Cyber Crime."[480] The Commission was charged to:[481]

- Identify high-risk cybersecurity issues facing the Commonwealth,

- Provide advice and recommendations regarding how to secure state networks, systems, and data,
- Provide suggestions regarding how to include cybersecurity into the Commonwealth's emergency management and disaster response capabilities,
- Offer suggestions to promote cyber awareness among citizens, businesses, and government entities,
- Recommend changes to training and education programs (K-12 and beyond) to build a pipeline of cybersecurity professionals, and
- Offer strategies to improve economic development opportunities throughout the Commonwealth.

The members broke into working groups to study cybersecurity-related risks across the five areas.[482] For example, the Cyber Crime Work Group, which included Brian Moran, Secretary of Public Safety and Homeland Security, and Paul Tiao, private attorney and partner at Hunton and Williams, LLP, "reviewed existing statutes governing crimes in cyberspace" and studied how to improve "coordination between the private sector and law enforcement on information sharing and prosecuting cybercrimes."[483] The Work Group reviewed Virginia statutes, such as the Computer Crimes Act and Data Breach Notification Act, with assistance from:

- Students from the George Washington University Trachtenberg School of Public Policy
- Virginia Attorney General's Office
- VSP
- Office of Public Safety and Homeland Security[484]

"As a result of the group's research, the Work Group proposed, introduced (and successfully passed in the 2015 General Assembly session) legislation to support law enforcement in its fight against cybercrime…"[485]

The Commission finalized its recommendations and, after two years, concluded activities on March 29, 2016. The Commission submitted a set of 29 recommendations to the Governor for consideration. Many of these recommendations required executive department and/or agency action, such as adoption of identity management and encryption standards for all Commonwealth departments and agencies. Other recommendations required coordination with and approval from the General Assembly. For example, in 2015, the General Assembly passed SB1307, which "clarifies language for search warrants for seizure, examination of computers, networks, and other electronic devices."[486] The Commission has seen many of its recommendations implemented and continues to influence executive and legislative actions today.

VIII. Acronyms

Acronym	Definition
CAE	Cybersecurity Center of Academic Excellence
CIO	Chief Information Officer
CIRT	Computer Incident Response Team
CISO	Chief Information Security Officer
CRWG	Cyber Response Working Group
CS&C	Office of Cybersecurity and Communications
CSIRT	Commonwealth Security Incident Response Team
CSRM	Commonwealth Security and Risk Management
Cyber-UCG	Cyber Unified Coordination Group
DHS	Department of Homeland Security
FBI	Federal Bureau of Investigation
FFRDC	Federally Funded Research and Development Center
HSSEDI	Homeland Security Systems Engineering and Development Institute
HTC	High Tech Crimes
ISAO	Information Sharing and Analysis Organization
ISO	Information Security Officer
ISOAG	Information Security Officers Advisory Group
IT	Information Technology
ITAC	Information Technology Advisory Council
NASCIO	National Association of State Chief Information Officers
NEWGP	New Economy Workforce Grant Program
NSA	National Security Agency
PSHS	Public Safety and Homeland Security
SCP	Secure Commonwealth Panel
SLTT	State, Local, Tribal and Territorial
UC	Unified Command
VANG	Virginia National Guard
VCSP	Virginia Cyber Security Partnership
VDEM	Virginia Department of Emergency Management
VEST	Virginia Emergency Support Team
VFC	Virginia Fusion Center
VITA	Virginia Information Technology Agency
VSP	Virginia State Police

Cybersecurity Governance in the State of Washington

A CASE STUDY

December 2017

Homeland Security

NASCIO
Representing Chief Information Officers of the States

Washington State Fast Facts[487,488]

ELECTED OFFICIALS:

- Governor Jay Inslee
- WA House of Representatives: 98 Representatives
- WA State Senate: 49 Senators

STATE CYBERSECURITY EXECUTIVES:

- Chief Information Officer (CIO) Michael Cockrill
- Chief Information Security Officer (CISO) Agnes Kirk
- Major General Bret D. Daugherty (Adjutant General, WA National Guard)

STATE DEMOGRAPHICS:

- Population: 7,288,000
  Workforce in "computers and math" occupations: 4%

EDUCATION:

- Public with a high school diploma: 48.6%
- Public with an advanced degree: 41.4%

COLLEGES AND UNIVERSITIES:

- 34 community colleges
- 6 public universities
- 15 private colleges

KEY INDUSTRIES:

- Information and communication technology
- Agriculture/food manufacturing
- Aerospace
- Clean technology
- Forest products
- Life science/global health
- Maritime
- Military/defense
- Sciences
- Logistics
- Manufacturing
- Technology

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 Washington'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 Washington 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 Washington 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.[489]

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 this case study covers a broad range of areas, each related section provides an overview of Washington's governance approach, rather than a detailed exploration. Individual states and organizations seeking greater detail would likely need to engage directly with Washington to better understand how to tailor solutions to their specific circumstances.

In recent years, the Washington executive and legislative branches have taken a series of deliberate steps to govern cybersecurity as an enterprise-wide strategic issue across both state government and a diverse set of private and public-sector organizations. (In this case study, "agency" refers to executive branch agencies.)

In 2015, the state Office of CyberSecurity, OCS, was consolidated into Washington Technology Solutions along with all other state IT services. OCS, led by the state Chief Information Security Officer sets statewide cybersecurity strategies and planning activities. The state CISO reports

to the state CIO, who oversees WaTech.[490] To incorporate private sector perspectives into the state's strategic planning process, the legislature created the WaTech Technology Services Board (TSB).[491] The TSB is an oversight body to the Office of the Chief Information Officer (CIO) that provides input regarding the state's strategic vision and planning process for information technology (IT) and security issues, as well as oversight of major IT projects.[492] This body allows the CIO to incorporate emerging trends, issues, and industry best practices as part of the deliberative policymaking process. The TSB actions include, but are not limited to, advising the CIO regarding data center investments, IT disaster recovery planning, business application/system governance, and quality assurance for IT projects.[493]

To respond to a declared "significant cyber event," the state established formal procedures and processes among various federal, state, local, and private sector entities. A significant cyber incident is defined "as an event that is likely to cause, or is causing, harm to critical functions and services across the public and private sectors by impairing the confidentiality, integrity, or availability of electronic information, information systems, services, or networks; and/or threaten public safety, undermine public confidence, have a negative effect on the economy, or diminish the security posture."[494] The Cyber Annex to the Washington State Comprehensive Emergency Management Plan (CEMP) defines a significant cyber event and provides formal processes and procedures to coordinate various parties. The formal CEMP is needed because all the "required resources, authorities and execution responsibilities do not reside in one department, agency, organization or company within the State of Washington."[495]

The Governor formally designated the Homeland Security Advisor (HSA), who reports directly to the Governor, with the responsibility to lead response efforts across the state and engage with federal, local, and private sector stakeholders in response to "significant" cyber-events. The HSA partners with a Cyber Unified Coordination Group (UCG), which consists of representatives from federal, state, and local governments, academia, private industry, and critical infrastructure owners/operators, to have a coordinated response to a significant cyber event. As noted in the Cyber Annex Washington State CEMP, Cyber UCG participants, in turn, act and provide assistance upon request from the HSA.[496] The Cyber Annex Washington State CEMP specifies that "during a significant cyber incident triggering state-level coordination," the HSA coordinates activities through the Cyber UCG.

To address the challenge of cyber workforce shortages, the state has a multi-threaded approach that has used a variety of governance mechanisms to bring together public and private organizations. State officials worked across the business community and a not-for-profit organization to modify the education curriculum and standards to strengthen science, technology, engineering, and math (STEM) subjects. Leaders from two- and four-year colleges worked together to create a cybersecurity academic path for students who begin in community college and want to continue to earn a degree from a four-year college. To address cybersecurity workforce training needs, officials worked across the business community, government, and not-for-profit organizations to develop an apprenticeship program that will train, certify, and place people from underrepresented groups in the technology industry.

These, and other efforts described in the rest of this case study, were the result of many years of concerted, diligent effort by many individuals. Several key officials across government worked for years to understand cybersecurity risks and build relationships to enable stronger state-wide efforts to address cyber threats. Cybersecurity is a challenge that cuts across many issues and many interdependent stakeholders.

Washington uses a range of governance mechanisms to work across different public, private, academic, and nonprofit organizations. Leadership on the part of individuals who made cybersecurity and cybersecurity governance a priority across government, public, and private organizations was very important. However, leadership was not everything. As Washington demonstrates, the priority must be translated into tangible laws, policies, processes, and structures that instantiated and aligned cybersecurity governance with broader cybersecurity priorities.

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.[497]

The case study explores cross-enterprise governance mechanisms used by Washington 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 Washington's governance approach, rather than a detailed exploration. Individual states and organizations seeking greater detail would likely need to engage directly with Washington 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."[498] 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 Washington's Governance Approach:

- The state Chief Information Officer (CIO) develops a statewide strategic information technology (IT) plan that sets direction for how the state will use and secure technology.
- An oversight board, which includes public and private sector representatives, advises the CIO about cybersecurity investments, risks, and policy changes.

Washington State's cross-government cybersecurity strategy and planning activities are led by the state's CIO and informed by the Chief Information Security Officer (CISO). As shown in Figure 1 below, both the CIO and CISO functions reside within Washington Technology Solutions (WaTech). The CIO, who is also the Director of WaTech, is appointed by the Governor and "is charged with preparing and leading the implementation of a strategic direction and enterprise architecture for information technology for state government."[499] WaTech was created in 2015, after a change in state law consolidated IT services to serve all state agencies and departments.[500]

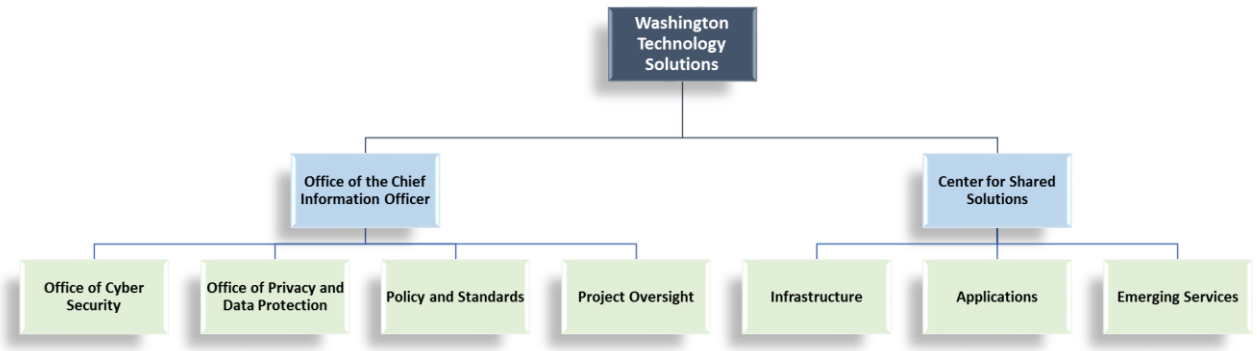


Figure 1. WaTech Organizational Chart (September 2017)

As part of this responsibility, the law directs the CIO to prepare a state strategic IT plan every two years.[501] This plan, called the Strategic Roadmap, identifies priorities for moving the state forward both in using technology to enable mission delivery and in securing and protecting those technologies.[502,503] For example, the most recent roadmap identifies initiatives (e.g.,

enhanced identity management and integrated cloud-based identity services) to address sophisticated cyber threats emanating from the increased use of cloud computing and mobile devices over the next several years. To track progress on the impact of cybersecurity-related initiatives, the CISO publishes a biweekly cyber health report and distributes it to departments and agencies. This health report provides a snapshot of information security measures, such as types of attacks, trends, measures of effectiveness and mitigations, and allows for ongoing adjustments to key initiatives.

The CIO and CISO advise state legislators and the Governor's office on a range of cyber-related strategic issues. Current CIO Michael Cockrill notes, "technology is involved in everything our citizens do, especially related to privacy and cybersecurity, so I spend a lot of my time consulting with state legislators and the governor's office about public policy issues related to technology and cybersecurity."[504]

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 Washington's Governance Approach:

- The CIO evaluates and approves IT and cyber-related spending requests across state departments and agencies.
- The CIO creates IT acquisition policies and procedures to evaluate and manage risks associated with proposed IT acquisitions across state departments and agencies.

For both budget and acquisitions, the CIO has authority to evaluate department and agency IT and cybersecurity budget requests and recommend which investments should be included in the annual state budget process. The annual budget process is used to identify, propose, and fund cybersecurity investments at a variety of levels:

1. Within WaTech operations,
2. Within the Office of Cybersecurity, and
3. Investments at each agency.

Each state department and agency prepares an annual IT budget as part of a centralized budgeting process. The CIO evaluates current IT spending and prioritizes new IT and cyber-related spending requests against portfolio-based IT management and cyber-related criteria developed by the CIO.[505] The CIO establishes priority ranking categories for the proposals based on several categories of risk and other factors, with no more than one-third of the submitted proposals ranked in the highest priority category.[506]

Based on this prioritization, the CIO recommends to the Director of Washington's Office of Financial Management (OFM) to fund all or part of submitted agency IT budgets and additional IT or cyber-related budget proposals.[507] (The OFM has final approval authority over the development and submission of the Governor's budget request to the state legislature.) This prioritization informs the final funding decisions by the Governor and the legislature. In addition, as mentioned above in the Strategy & Planning section, the TSB plays a role in setting the criteria and the weighting for those criteria on IT budget and planning activities.[508]

The CIO also formulates IT acquisition policies that apply to all state agencies. These policies establish that the CIO review, approve, and oversee all major IT investments.[509] The CIO determines what constitutes a major IT investment, but size of the investment and potential type and severity of risks to the state's network are always considered as part of the evaluation process. To aid in the evaluation process, the CIO provides departments and

agencies with a standardized IT Project Assessment tool to "assess the cost, complexity, and statewide significance of an anticipated [IT]" and the corresponding risk profile of proposed projects.[510] Projects with higher risk profiles receive varying levels of direct oversight.

The CIO considers severity in terms of "impact on citizens, visibility to the public and Legislature, impact on state operations, and the consequences of doing nothing."[511] Risk is evaluated according to "impact of the IT investment on the organization, the effort needed to complete the project, the stability of or familiarity with the proposed technology, and the agency preparedness."[512] In addition, the TSB plays a role in the acquisition process by reviewing major IT policy changes and providing oversight of major IT investments. The CIO is chair of the TSB.

III. Risk Identification & Mitigation

The Challenge:

How to identify and mitigate cybersecurity risks across multiple organizations?

Features of Washington's Governance Approach:

- The CISO sets standards to govern information security that apply to all state government systems and conducts security assessments.
- For every project, departments/agencies are responsible for producing a risk assessment that guides the implementation for security controls for that project.
- The CISO oversees a design review and reviews agency risk assessments. All departments and agencies must go through that process prior to launching a new system or service.
- The Military Department collaborates with critical infrastructure owners and operators to develop plans that address cybersecurity threats and risks to critical infrastructure.
- The Military Department identifies risks that would require a coordinated emergency response from the state.

Governance for cross-organizational risk identification and mitigation is shared by the CISO and the Military Department. The CISO focuses on risks to state networks, while the Washington Military Department focuses on risks that could impact critical infrastructure and that would require an emergency response.

The Office of Cyber Security (OCS), which is located within the WaTech Office of the Chief Information Officer and led by the CISO, is charged with identifying and mitigating cyber risks to state government networks.[513] The CISO, who reports to the CIO, sets information security standards for state systems and advises the Governor and state legislators on various cyber issues.

The OCS is responsible for identifying potential risks to the state government's network, managing the state's Security Operations Center (SOC), conducting risk assessments, implementing data controls, and determining the appropriate data architecture based on risk profiles of various types of data. The risk identification process starts when departments/agencies produce a risk

assessment for new information technology projects (see Budget and Acquisition section).

These assessments guide the implementation for security controls for that project. The CISO oversees a design review and reviews agency risk assessments prior new systems or services being launched. For example, in 2016, the OCS conducted 225 design reviews and discussions of major systems to ensure that they met security standards prior to being installed on the network and conducted 17 security assessments at state agencies, which identified mitigated vulnerabilities to the state's network.[514,515] The OCS also reviews "annual attestation reports from all state agencies detailing their level of compliance with state security guidelines and best practices."[516]

In addition to risk identification and mitigation actions of the OCS, the Washington Military Department plays a role in identifying risks that could require a coordinated emergency response from the state. The Military Department is focused on identifying risks, such as hazards that cause injury and/or damage from natural and technology disasters, that could necessitate an emergency response, and planning for a coordinated emergency response.[517] The Military Department maintains the State Threat and Hazard Identification and Risk Assessment, a Federal Emergency Management Agency risk assessment that identifies risks and emergency plans and capabilities available to respond in an emergency.

The Washington Military Department also leads efforts to coordinate with private sector owner/operators of critical infrastructure and key resources (CIKR) to develop plans to address cybersecurity threats to CIKR. In 2008, the Military Department developed the State of Washington Infrastructure Protection Plan in collaboration with public agencies and the private sector.[518] The plan articulates "an all-hazards approach to identify and protect CIKR with statewide, regional or national implications that if lost or disrupted," while acknowledging that "protection of CIKR is primarily the responsibility of its owner/operators with government support as necessary."[519] (See Incident Response section for additional information about how cyber incidents are addressed.)

For example, as part of its coordination role, the Military Department facilitated meetings of the Washington State Energy Coordinating Council (ECC) as it developed the Washington State Sector Specific Plan for Critical Energy Infrastructure.[520] The ECC, which includes private sector owner/operators of energy critical infrastructure (i.e., oil, natural gas, electric utility), is part of the standing Infrastructure Protection Subcommittee of the Washington Committee on Homeland Security.[521] The plan identifies key issues and mitigation programs and measures across issue areas including data and information sharing, critical infrastructure mapping, interdependencies, out-of-state infrastructure critical to Washington operations, and emergency response, restoration, and recovery.

IV. Incident Response

The Challenge:

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

Features of Washington's Governance Approach:

- The CIO, in coordination with the CISO, develops policy and leads response to cyber incidents that could pose a threat to the state's data architecture and/or systems.
- The Military Department leads the response to significant incidents that could impact the public and private sectors.
- A Cyber UCG, which includes public and private sector organizations, helps manage significant incidents.

Governance for cross-organizational cyber incident response is shared. If the threat is to the state government network, it is led by the CIO, in coordination with the CISO. If the Governor declares a significant cyber incident, it is led by the HSA.

The CIO develops the incident response policy to address possible IT security incidents that could pose a threat to the state's data architecture and/or systems.[522] The law defines a security incident as an accidental or intentional event resulting in "an imminent threat of the unauthorized access, loss, disclosure, modification, disruption, or destruction of communication and information resources."[523]

The OCS, which reports to the CISO, is the central point of contact for state government agencies to report and respond to suspicious activity and security incidents on the state network.[524] OCS staff includes a cadre of cyber professionals who are on call 24 hours a day, seven days a week, and are trained to identify, respond to, and mitigate cyber threats.[525] In 2016, OCS staff blocked more than 100 million malicious activities each week, blocked more than 12 distributed denial of service attacks on the state's network, and responded to 47 major cybersecurity incidents involving 19 state agencies.[526] In addition, to mitigate potential risks, the OCS trains state agency leaders by conducting exercises to help them identify and respond to cyber attacks. The office also hosts regular technical and policy training sessions with IT security professionals from across the state enterprise to remain current with the latest security tools and best practices.

As shown in Figure 2 below, the incident response policy sets forth a five-step response process that articulates the roles and responsibilities of the CIO, CISO, and agencies.

Figure 2. Five-Step Response Process to an IT Security Incident on the State Network[527]

Once an agency notifies the CISO, through the OCS, of an IT security incident, the CISO and OCS staff work with the agency IT staff to determine the scope, severity, and cause of the incident, as well as to determine what corrective actions are needed to rectify the situation.[528] The CISO can provide specialized capabilities to agency IT staff to assist in response efforts. For example, the OCS Computer Emergency Readiness Team (CERT), comprised of digital forensic experts, investigates malware intrusions on state-owned computers to determine method and origin of infection. In addition, the CERT provides statewide incident response for state agencies.[529]

Next, the CISO determines whether to notify the CIO and the Assistant Attorney General for the CIO. The CISO and the Washington State Attorney General determine whether public notification is warranted and provide the CIO with that determination.[530] The CIO may then convene the Security Incident Communications Team (SICT) if public notification of the IT security incident is required by law. The SICT may include heads of the agency or agencies impacted, legal counsel, the CISO, and members of law enforcement, among others.[531] Finally, the CIO may authorize public notification of the IT security incident if required under law.[532]

If the Governor declares a significant cyber incident, the HSA, who is also the Adjutant General, leads the response at the state level and coordinates at the federal level.[533] The Adjutant General is head of the Washington Military Department and as such oversees the Emergency Management Division and the Army, Air, and State National Guards. A significant cyber incident is defined as "an event likely to cause, or is causing, harm to critical functions and services across the public and private sectors by impairing the confidentiality, integrity, or availability of electronic information, information systems, services, or networks; and/or threaten public safety, undermine public confidence, have a negative effect on the economy, or diminish the security posture."[534] Cyber incidents that impact CIKR sectors would be deemed significant.[535] The Governor also directs the CIO to coordinate with the HSA if the significant cyber incident involves state agency IT systems.

The HSA reports directly to the Governor in the event of a significant cyber event and coordinates response efforts with the support of the Cyber UCG, which is organized through the State Emergency Operations Center (SEOC). Formal coordination is needed because all the "required resources, authorities and execution responsibilities do not reside in one department, agency, organization or company within the State of Washington."[536] The HSA partners with the Cyber UCG (which consists of representatives from federal, state, and local governments, academia, private industry, and critical infrastructure owners/operators) to respond quickly to a significant cyber event.

The SEOC provides a dedicated space to organize Cyber UCG members from across government and the private sector to address "incident prioritization, critical resource allocation, and situational awareness for issues arising as a result of a significant cyber incident."[537] Representatives from CIKR sectors are encouraged to communicate and coordinate

with the Cyber UCG and are "integrated physically and virtually into the UCG" during a significant cyber incident affecting CIKR sectors."[538] Cyber UCG participants have the authority to act and assist upon request from the HSA.[539] In addition, the Washington State Fusion Center (WSFC) "may host the Cyber UCG when activated and generate cyber alerts to notify federal, state, regional, local, tribal, and private sector partners with early warning indicators and potential actionable intelligence measures."[540]

Also, state law provides that the Governor may activate the National Guard to help with incident response.[541] The Washington National Guard is equipped to address certain cyber threats because of its expertise in industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems. Many members of the Washington National Guard are trained by the federal government to respond to security incidents impacting ICS and SCADA, and therefore are well prepared to deploy in response to cyber incidents that require this expertise.

V. Information Sharing

The Challenge:

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

Features of Washington's Governance Approach:

- The SOC supports information sharing across state departments and agencies.
- The state participates in cross-state information sharing bodies (e.g., the Multi-State Information Sharing and Analysis Center [MS-ISAC], the DHS National Cybersecurity and Integration Center [NCCIC].
- The state is in the process of developing a SLTT-ISAC to strengthen sharing with SLTT partners.

Washington State uses a range of governance structures to promote sharing of different types of information within state government and between the state government, federal government, and private sector. David Morris, the Washington State CTO for Cyber Security, characterizes information sharing in terms of trusted relationships, where "security is all about building trust relationships" and that those "relationships need to be in place *before* they are needed."[542]

Within the state government, the OCS SOC is "the nerve center for information sharing and monitoring enterprise security."[543] The SOC gathers a variety of threat information from monitoring state networks and from engaging with several information sharing bodies: the Cyber Incident Response Coalition and Analysis Sharing, a regional information sharing body; the MS-ISAC; and the DHS NCCIC. The SOC communicates threat information to state, local, and/or tribal government representatives and/or critical infrastructure partners. Stakeholders use this threat information in different ways to inform operational adjustments to network defenses.

In the event of a significant cyber event, the WSFC plays a role in facilitating incident-related information sharing, leveraging the "Homeland Security Information Network, a national secure and trusted web-based portal for information sharing and collaboration…"[544] The WSFC is designed to organize cyber alerts, notifications, and updates emanating from the Cyber UCG, NCCIC, and Seattle Federal Bureau of Investigation Joint Cyber Task Force, as well as to communicate with the SEOC and WSFC cyber stakeholders.[545] "In addition, the WSFC engages with other national homeland security fusion center cyber programs through the Cyber Intelligence Network (an outreach network of corporate security, information security and intelligence community professionals) to augment the SEOC common situational awareness of a significant cyber incident."[546]

At the regional level, officials are expanding information sharing beyond the federal, state, and regional levels to include local partners. The OCS is in the process of establishing a Washington State-level Information Sharing and Analysis Center (ISAC).[547] The Washington-specific ISAC will provide actionable threat information to SLTT partners. The CTO and CISO, in collaboration with the CIO, are "highly focused" on establishing the state ISAC to build the trusted relationships necessary to identify and respond to cyber threats within the context of regional Washington environments.[548]

In addition to the federal information sharing resources listed above, the Washington CISO participates in national-level information sharing with peers through 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."[549] The Washington CIO sits on the executive board of NASCIO and the CISO sits on the cyber advisory board. NASCIO plays a significant role and builds trusted relationships with fellow state CISOs, trading best practices and emerging trends across the threat landscape.

VI. Workforce & Education

The Challenge:

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

Features of Washington's Governance Approach:

- K-12 curriculum standards were changed to include computer science and STEM graduation requirements and enabled public school districts to award college credits for Advanced Placement computer science classes.
- Community colleges and four-year universities have partnered to enable community college graduates in cybersecurity programs to transfer credits to four-year universities.
- A public-private partnership, led by the WTIA, offers an apprenticeship program to train underrepresented groups in the technology industry.
- The state is developing a program that would fund cybersecurity training and certifications for individuals in exchange for a paid position in a government organization.

Washington used a variety of governance mechanisms to bring together public and private organizations to address cybersecurity workforce shortages and education needs. These organizations included business, K-12 public education, community colleges, four year colleges, and not-for-profit organizations.

State officials worked across the business community and a not-for-profit organization to modify the K-12 curriculum to address the need for greater student understanding of STEM subjects. Starting in 2013, the state legislature, Governor, and business community worked together to address the need to include computer science classes in the K-12 curriculum. The Governor signed a bill to allow Washington public school districts "to award a math or science credit to students who enroll in an AP Computer Science class" to encourage more students to enroll in computer science classes, reduce the STEM skills gap, and "provide more opportunities for students to gain real-world experience and knowledge in a cutting-edge industry."[550] This legislation was an early step toward strengthening STEM-related education and was supported by Washington business leaders, including Microsoft, as well as the nonprofit code school code.org.[551]

Building on these first steps, in 2015 the Governor announced that the Washington K-12 public school curriculum would include new computer science education standards. The new *Washington State Computer Science K–12 Learning Standards* address the need for graduates in STEM. "The new standards map out computer literacy goals for students in elementary and middle schools, while also mandating levels of proficiency a student needs to pass a high school computer science course."[552] According to Governor Inslee, in 2016 "roughly 11 percent of Washington's schools meet these standards." However, by 2019, the Governor's goal is "to bump that up to 50 percent."[553]

Education changes were also made at the postsecondary levels. Leaders from select two-and-four year colleges worked together to create a cybersecurity academic path for students who begin in community college and want to continue to earn a degree from a four-year college. Typically, four-year colleges accepted few, if any, academic credits from community colleges. However, a partnership between select community and four-year colleges allows eligible students to transfer all credits to a four-year college. This structural change is enduring, allowing for a pipeline of students to transition smoothly from community college to four-year college. For example, students who complete a two-year degree in one of the cybersecurity-focused programs at Whatcom Community College can transfer all of their credits to either the University of Washington or Western Washington University.[554]

To address cybersecurity workforce training needs, officials worked across the business community, government, and nonprofit organizations to develop an apprenticeship program. This program is training existing workers to qualify for IT and cyber-related jobs. Washington leveraged an existing nonprofit organization, the Washington Technology Industry Association (WTIA), and a federal grant to launch an apprenticeship program to respond to "technology companies in Washington…struggling to fill their growing number of vacant, skilled positions."[555] As a private industry-led nonprofit entity, Apprenti can respond more quickly to changes in market-based workforce demands across a number of businesses. The WTIA, whose membership includes private technology and communications companies, manages and operates the apprenticeship program. The WTIA is expected "to provide training and jobs for up to 1,000 people, 600 of them in the technology industry."[556] As of 2015, there were "more than 240 registered apprenticeship training programs in the state with more than 10,000 active apprentices."[557]

In the future, the CIO, CISO, and Governor are working to establish new paths to fill the workforce gap. One initiative is a plan to launch Cyber Washington, a dedicated effort to try to bridge the gap between academia (education providers) and the private sector (job providers). Cyber Washington will launch a program to attract top talent to state and local IT vacancies. In exchange for state funding of training and certifications, individuals participating in the program will agree to work for the government for a period of time. This will provide participants with both education and professional experience to be competitive candidates for hire among the many Washington-based technology firms. While the details are still being developed among all parties, this program already has the support of key government officials, as well as private sector leaders such as Amazon, Microsoft, and Expedia.[558] Additionally, the state is partnering with higher education to expand online cybersecurity educational programs that will result in certifications for specific cyber skills that both public and private companies have agreed meet their workforce needs. This program will build on the cyber defense

programs offered by the cyber centers of academic excellence programs.

Washington leaders are now focused on measuring the outcomes of these many policy initiatives. In 2016, the Washington legislature passed a law directing the CIO and Director of WaTech to collaborate with community colleges, universities, the Washington Department of Commerce, and other stakeholders to "evaluate the extent to which the state is building upon its existing expertise in information technology to become a national leader in cybersecurity."[559] The law requires the WaTech Director to periodically evaluate the state's performance in achieving a variety of policy objectives, such as number of students graduating in the STEM fields.[560] The OCS must report its performance with regard to these policy objectives, as well as recommendations to the state legislature, before December 1, 2020. This baseline study will likely guide future cybersecurity investments in education and training, as well as a host of other matters.

VII. Deep Dive: Apprenti

Introduction

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

The Challenge

The demand for a trained, diverse cybersecurity workforce outstrips supply. Traditional models (e.g., recruiting graduates from select undergraduate and graduate schools) have not kept up with the demand. Workforce training, especially of those from a more diversified ethnic and socioeconomic background, is needed to address the demand for talent. The demand for a cybersecurity workforce cuts across multiple companies and industries. One company or industry alone cannot fully address the challenge.

The Solution

Create a public-private partnership, led by a single not-for-profit institution (called Apprenti), that offers an apprenticeship program to train underrepresented groups, such as women, minorities, and Veterans, in the technology industry. Once accepted, applicants receive a certification and are placed among several different participating businesses.[561]

Background

While community college and four-year university programs serve various workforce and education needs, the demand for a diversified cybersecurity workforce continues to outstrip supply. Workforce training, especially of those from more diverse ethnic and socioeconomic backgrounds, is needed to address the demand for talent. Several years ago, some members of the WTIA took the initiative to evaluate and gather consensus regarding how to address persistent market demand for a larger skilled workforce in various cybersecurity-related fields, such as data analysts, front-end software developers, and network administrators, among others.

The WTIA, founded in 1984, is a not-for-profit 501(c)6 organization industry trade association comprised of 600+ information and communications technology companies. Members include Microsoft, Amazon, Nordstrom, and Expedia, to name a few. The WTIA's three strategic priorities are to (1) help small and medium-sized firms attract and retain technical talent; (2) advocate for more private and public investments in computer science education at all education levels; and (3) "help create a long-term, sustainable technology industry by developing technical and entrepreneurial talent directly through programs and indirectly through partnerships."[562]

In 2015, the WTIA established the Washington Technology Workforce Institute (WTWI) and the pilot tech apprenticeship program Apprenti. Apprenti is a 501(c)(3) not-for-profit, whose mission is to serve as the tech sector's apprenticeship intermediary, connecting industry, government, and education using public/private partnerships to close the talent and diversity gaps.[563]

Apprenti represents a public/private partnership and is funded in part by a federal grant from the American Apprenticeship Initiative, the U.S. Department of Labor, the State of Washington's Department of Labor and Industry, and private sector partners. Hiring partners and private funders include Microsoft,

Amazon, Accenture, JP Morgan Chase, Comtech, Silicon Mechanics, and F5.

The federal grant provided Apprenti with initial seed capital to launch the program. State and local Department of Labor officials will continue monitoring the progress of Apprenti over the next several years in accordance with requirements outlined in the federal grant.

Applicants accepted into the Apprenti program receive a certification paid for by the WTWI worth approximately $15,000 in various occupations, such as database administrator, project manager, network security administrator, web developer, software developer, Windows systems administrator, Linux systems administrator, or IT support professional.[564]

Apprentices are hired by a partner company prior to beginning classroom training and receive a salary and benefits while learning on the job. Typically, companies spend approximately $75,000 in direct (salary) and indirect (benefits) costs to train an apprentice for the year. The goal is for the employer to cultivate the talent to a level where, at the end of the one-year apprenticeship program, the apprentice will be retained at entry-level market wage for that job. The goal is to train 600 women, Veterans, and/or minorities over the next five years. To date, 76 Apprenti graduates have been placed in apprenticeships, and the program is on track to place a total of 130 by the end of December 2017.[565]

One of the lessons learned from the Apprenti program is that how the entity is legally organized matters in terms of governance and funding issues. As a 501(c)3, Apprenti is allowed to receive funds from private foundations in addition to state and federal funds (to train workers, for example). This allows the program to draw from multiple funding streams. As a private industry-led nonprofit entity, Apprenti has direct access to tech companies for hiring and can respond more quickly to changes in market-based workforce demands.

VIII. Acronyms

Acronym	Definition
AP	Advanced Placement
CERT	Computer Emergency Readiness Team
CIKR	Critical Infrastructure and Key Resources
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CS&C	Office of Cybersecurity and Communications
DHS	Department of Homeland Security
ECC	Energy Coordinating Council
FFRDC	Federally Funded Research and Development Center
HSA	Homeland Security Advisor
HSSEDI	Homeland Security Systems Engineering
ICS	Industrial Control Systems
ISAC	Information Sharing and Analysis Center
IT	Information Technology
MS-ISAC	Multi-State Information Sharing and Analysis Center
NASCIO	National Association of State Chief Information Officers
NCCIC	DHS Cybersecurity and Communications Integration Center
OCS	Washington State Office of CyberSecurity
OFM	Washington's Office of Financial Management
SCADA	Supervisory Control and Data Acquisition Systems
SEOC	State Emergency Operations Center
SICT	Security Incident Communications Team
SLTT	State, Local, Tribal & Territorial
SOC	Security Operations Center
STEM	Science, Technology, Engineering, and Math
TSB	WaTech Technology Services Board
UCG	Unified Coordination Group
WaTech	Washington Technology Solutions
WSFC	Washington State Fusion Center
WTIA	Washington Technology Industry Association
WTWI	Washington Technology Workforce Institute

[i] 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.

[1] 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.

[2] About NASCIO. Available: https://www.nascio.org/AboutNASCIO.

[3] 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 nonvoting member appointed by the Chief Justice of the Georgia Supreme Court." Available: https://gta.georgia.gov/board-directors.

[4] MCL Chapter 18 Section 18.41. Available: http://www.legislature.mi.gov/(S(1kzimy1qiufegyrvb4usw53n))/mileg.aspx?page=getObject&objectName=mcl-18-41.

[5] State of New Jersey Technology Circular, "Enterprise Information Security Management," New Jersey Office of Information Technology, Policy No. YY-00-NJOIT, September 1, 2017.

[6] In 2003, the legislature passed House Bill 1926 (Nixon) and Senate Bill 1247 (Stosch) to establish VITA.

[7] WaTech unifies the former Office of the Chief Information Officer, the original Consolidated Technology Services, and the enterprise applications division of the Department of Enterprise Services. *See* WaTech, "WaTech | Re-inventing the Everyday Public Service Experience." Available: http://watech.wa.gov/about. See also RCW 43.105.006, http://apps.leg.wa.gov/RCW/default.aspx?cite=43.105.006.

[8] The strategic planning questionnaire focuses 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.

[9] MCL Chapter 18 Section 18.41. Available: http://www.legislature.mi.gov/(S(hn2qlonq5mn1lktnuf5rheug))/mileg.aspx?page=getObject&objectName=mcl-18-41.

[10] "IT Strategy Group Charter." Made available by DTMB. (2017, June 23).

[11] The IT Strategy Group also aligns specific strategies (e.g., cybersecurity, cloud, and mobile) with timelines and metrics, and "[ensures] that technology services deliver business value. Available: "DTMB IT Governance." Made available by DTMB (2017, June 23).

[12] WaTech, Consolidated Technology Services Roadmap. Available: http://watech.wa.gov/sites/default/files/ctsroadmap.pdf.

[13] 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.

[14] Interview with David Behen, former Director and CIO, DTMB. (2017, March 2).

[15] State of New Jersey, "Enterprise Information Security Policies and Standards." (2017, January 2017).

[16] https://law.lis.virginia.gov/vacode/title2.2/chapter2/section2.2-225/.

[17] Office of the Governor, Commonwealth of Virginia, Executive Order 8, "LAUNCHING "CYBER VIRGINIA" AND THE VIRGINIA CYBER SECURITY COMMISSION." (2014, February 25). Available: http://governor.virginia.gov/media/3036/eo-8-launching-cyber-virginia-and-the-virginia-cyber-security-commissionada.pdf.

[18] Interview with Secretary of Technology Karen Jackson. (2017, March 24).

[19] WaTech Technology Services Board. Available: http://ocio.wa.gov/boards-and-committees/technology-services-board-tsb-0. *See also* RCW 43.105.287 for a complete list of powers and duties of the Technology Services Board. The 13-member Technology Services Board is comprised of the CIO, three representatives from state agencies or institutions, three representatives from the private sector, two members of the state House of Representatives appointed by the Speaker of the House, two members of the state Senate appointed by the President of the Senate, one nonvoting member representing state agency bargaining units selected by the Governor, and one nonvoting member representing local governments selected by the Governor. For a current list of members, *see* http://ocio.wa.gov/technology-services-board-tsb/technology-services-board-tsb-board-members.

[20] http://ocio.wa.gov/sites/default/files/public/TECHNOLOGY%20SERVICES%20BOARD%20Charter.pdf

[21] Executive Order No.2001 – 3. Available: http://www.michigan.gov/formergovernors/0,4584,7-212-31303_31305-3054--,00.html.

[22] MCL Chapter 18 Section 18.41. Available: http://www.legislature.mi.gov/(S(oaeofmiadbhoherqkwo4pqv1))/mileg.aspx?page=getObject&objectName=mcl-18-41.

[23] The law directs executive branch agencies to "obtain CIO approval prior to the initiation of any Commonwealth information technology project or procurement [providing an] business case, outlining the business value of the investment, the proposed technology solution, if known, and an explanation of how the project will support the agency strategic plan, the agency's secretariat's strategic plan, and the Commonwealth strategic plan for information technology." Virginia code §2.2-2018.1. Available: https://law.lis.virginia.gov/vacode/title2.2/chapter20.1/section2.2-2018.1/ *See also* Virginia code §2.2-2007. Available: https://law.lis.virginia.gov/vacode/title2.2/chapter20.1/section2.2-2007/.

[24] RCW 43.105.240. Available: http://app.leg.wa.gov/RCW/default.aspx?cite=43.105.240.

[25] Agnes Kirk, Washington State CISO. (2017, September 14).

[26] Interview with Agnes Kirk, Washington State CISO. (2017, March 14).

[27] RCW 43.105.287. Available: http://apps.leg.wa.gov/rcw/default.aspx?cite=43.105.287.
[28] https://gta.georgia.gov/psg/article/accountability-change-management-and-process-improvement-act-2016-hb676-0
[29] 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.
[30] New Jersey Department of Treasury, Joint Circular No. 18-03-OMB/DPP/OIT, "Procurements of Information Technology (IT) Hardware, Software, Subscription-based Solutions and Related Services and Non-IT Equipment." (2017, August 22). Available: http://www.state.nj.us/infobank/circular/cir1803.pdf.
[31] Interview with David Weinstein, New Jersey CTO. (2017, September 6).
[32] D. Verton, "Look Who's MeriTalking: Virginia CIO Nelson P. Moe." MeriTalk.com. (2016, May 2). Available: https://www.meritalk.com/look-whos-meritalking-virginia-cio-nelson-p-moe/.
[33] Interview with CISO Mike Watson. (2017, March 25).
[34] WaTech Policy 121: Procedures: "IT Investments - Approval and Oversight - Appendix A: Severity and Risk Assessment." (2014, January 8). Available: https://ocio.wa.gov/policy/it-investments-approval-and-oversight-policy.
[35] The CIO considers severity in terms of "impact on citizens, visibility to the public and Legislature, impact on state operations, and the consequences of doing nothing." Risk is evaluated according to "impact of the IT investment on the organization, the effort needed to complete the project, the stability of or familiarity with the proposed technology, and the agency preparedness." From WaTech Policy 121: "IT Investments - Approval and Oversight - Appendix A: Severity and Risk Assessment." (2014, January 8). Available: https://ocio.wa.gov/sites/default/files/public/policies/121_Approval_Oversight_201711.pdf.
[36] 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.
[37] Georgia.gov, "Cybersecurity." Available: https://gta.georgia.gov/cybersecurity.
[38] Ibid.
[39] The Management and Budget Act 431 of 1984. Available: https://www.legislature.mi.gov/(S(ywkpivhjgisruy5qu4oyxeao))/mileg.aspx?page=GetMCLDocument&objectname=mcl-18-1204.
[40] Interview with Rod Davenport, CTO. (2017, May 4).
[41] NJ OIT Technology Circular (Policy No. 16-05-NJOIT). "System Architecture Review Policy." (2016, December 12). Available: http://www.nj.gov/it/docs/ps/16-05-NJOIT_System_Architecture_Review_Policy.pdf.
[42] Ibid.
[43] VITA, 2015 Commonwealth of Virginia Information Security Report. Available: https://www.vita.virginia.gov/media/vitavirginiagov/uploadedpdfs/vitamainpublic/security/2015COVSecurityAnnualReport.pdf.
[44] Washington State Office of Cyber Security, "About Us." Available: http://www.soc.wa.gov/about-us.
[45] This 2015 plan includes a strategic overview of risks to people, property, the economy, and the environment from potential cyber events, a characterization of the level of response needed by federal, state, and local entities, and a brief overview of types and likelihood of cyber-attacks. Available: https://mil.wa.gov/other-links/enhanced-hazard-mitigation-plan; https://mil.wa.gov/uploads/pdf/hazplancyber.pdf.
[46] Read more about the activities involved in these areas of support here: https://gta.georgia.gov/enterprise-portfolio-management-services.
[47] State of New Jersey Technology Circular, "Enterprise Information Security Management," New Jersey Office of Information Technology, Policy No. YY-00-NJOIT. (2017, September 1).
[48] New Jersey C.App.A:9-67. http://www.njleg.state.nj.us/2000/Bills/pl01/246_.pdf.
[49] New Jersey C.App.A:9-70. http://www.njleg.state.nj.us/2000/Bills/pl01/246_.pdf.
[50] Washington State Military Department, "Washington Infrastructure Protection Plan." (2008). Available: http://mil.wa.gov/uploads/pdf/PLANS/2008%20washington%20infrastructure%20protection%20plan.pdf
[51] Computer Security Incident Response and Handling Plan. (2016, October). Provided by GTA (2017, October 20).
[52] 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.
[53] Georgia.gov, "Incident Response and Reporting." Available: https://gta.georgia.gov/psg/article/incident-response-and-reporting.
[54] Michigan Cyber Disruption Response Strategy. (2013, September 16). Available: https://www.michigan.gov/documents/cybersecurity/Michigan_Cyber_Disruption_Response_Strategy_1.0_438703_7.pdf.
[55] State of New Jersey, "Cybersecurity Incident Response Plan," v1.0. (2017, February). Furthermore, "incidents may result from intentional or unintentional actions and may include loss or theft of agency information assets, unauthorized access to agency information assets, introduction of malicious code, or the failure of system security functions to perform as expected."
[56] Ibid.
[57] Ibid.
[58] The full definition of an event is provided as: "An event is any observable occurrence in a system, network, and/or workstation. Although natural disasters and other non-security related disasters (power outages) are also called events, these reporting requirements are for IS security related events only. Events can many times indicate an information security incident is happening."

[59] K. Bortle and A. Burge, "Guidance on Reporting Information Technology Security Incidents," VITA Commonwealth Security & Risk Management Incident Response Team. (2016, April 7). Available: https://www.vita.virginia.gov/security/default.aspx?id=317.
[60] §2.2-603(G). Available: https://law.lis.virginia.gov/vacode/title2.2/chapter6/section2.2-603/.
[61] VITA, "CSRM Information Security Incident Response Procedure v6_0." (2014, February 3). Available: https://www.vita.virginia.gov/media/vitavirginiagov/resources/presentations/pdf/InformationSecurityIncidentResponseProcedure.pdf.
[62] RCW 43.105.020 (19). Available: http://app.leg.wa.gov/RCW/default.aspx?cite=43.105.020.
[63] WaTech CIO Policies, 143 - IT Security Incident Communication. Available: https://ocio.wa.gov/policy/it-security-incident-communication.
[64] From redacted version of "State of Georgia, Georgia Technology Authority, Computer Security Incident Response & Handling Plan." Made available by GTA (2017, October 20).
[65] Complete list of CDRT organizations in section 6 of the CDRP. Available: https://www.michigan.gov/documents/cybersecurity/120815_Michigan_Cyber_Disruption_Response_Plan_Online_VersionA_507848_7.pdf.
[66] Ibid.
[67] State of New Jersey, "Cybersecurity Incident Response Plan," v1.0. (2017, February).
[68] State of New Jersey, "Enterprise Information Security Policies and Standards." (2017, February).
[69] State of New Jersey, "Cybersecurity Incident Response Plan," v1.0. (2017, February).
[70] Coordinated by the U.S. Department of Homeland Security.
[71] Interview with Captain David Kelly, Commander of the Intelligence Operations Division Michigan State Police; Captain Chris Kelenske, Commander of the Emergency Management and Homeland Security Division, Michigan State Police; and Chris Christensen, Director of Infrastructure Protection, DTMB. (2017, April 14).
[72] Va. Code Ann. §2.2-222.3 (2016).
[73] RCW 42.56.590. Available: http://apps.leg.wa.gov/rcw/default.aspx?cite=42.56.590.
[74] Ibid.
[75] Interview with Ashley Gelisse, Chief of Staff, DTMB, and Chad Laidlaw, Senior Policy Analyst, DTMB. (2017, June 8).
[76] The functions of the ROIC are threefold: conducting watch floor operations (Watch Ops), real-time tactical intelligence analysis (Analysis), and tracking assets (Asset Management and Coordination). During daily operations, these functions are performed to create a complete picture of the current operating environment throughout the state of New Jersey, including external factors that may also present immediate concerns (terrorism, severe weather events, gang or drug problems in neighboring states, etc.) as well as the resources available to address them. During crisis operations, these same functions remain paramount, albeit with much greater immediacy of information flow and expanded outreach to and integration with external agencies and federal partners. Drawing upon its resources and partners, the ROIC remains the center of gravity for the creation of a comprehensive common operating picture of relevant events and happenings within the state.
[77] New Jersey Office of the Governor, Executive Order 178, "Governor Christie Takes Action to Defend New Jersey and its Infrastructure from Cybersecurity Threats." (2015, May 20). Available: https://www.cyber.nj.gov/njccic-executive-order-signing/.
[78] Interview with Chris Rodriguez, former Director of NJ Office of Homeland Security and Preparedness (OHSP). (2017, September 15).
[79] Ibid.
[80] Ibid.
[81] Virginia Final Cyber Security Report, 2016. Available: https://cyberva.virginia.gov/media/6424/virginiacybersecurity_printfinal-83116.pdf.
[82] "Governor McAuliffe Announces State Action to Protect Against Cybersecurity Threats." (2015, April 20). Available: https://governor.virginia.gov/newsroom/newsarticle?articleId=8210.
[83] Ibid.
[84] Ibid.
[85] Interview with Ashley Gelisse, Chief of Staff, DTMB. (2017, March 2).
[86] Interview with Rod Davenport, CTO. (2017, May 4).
[87] Interview with David Morris, CTO. (2017, April 25).
[88] "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.
[89]Georgia Cyber Innovation and Training Center. Available: https://gta.georgia.gov/georgia-cyber-innovation-and-training-center.
[90] J. Scott Trubey, "New Georgia training center in Augusta to counter cyber threats." *Atlanta Journal-Constitution*. (2017, June 19). Available: http://www.myajc.com/news/local-govt--politics/new-georgia-training-center-augusta-counter-cyber-threats/rEs9KmrDuvKjdR7SFqw9hO/.
[91] 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.
[92] Merit Network, Inc., "About Us." Available: www.merit.edu/about-us.
[93] A. Alusheff, "Pinckney schools first in nation with cybersecurity program." *Detroit Free Press*. (2016, December 12). Available: http://www.freep.com/story/news/local/michigan/2016/12/12/pinckney-schools-cyber-security/95325834/.
[94] Interview with Joseph Sawasky, President and Chief Executive Officer, Merit Network, Inc.; Dr. Joe Adams, Vice President for Research and Cyber Security, Merit Network, Inc., and Executive Director, Michigan Cyber Range; and Pierrette Templeton, Director of

Communications and Marketing, Merit Network, Inc. (2017, June 23).
[95] Merit Network, Inc., "Regional Cybersecurity Education Collaboration." Available: https://www.merit.edu/cybered/.
[96] 2016 Virginia Acts of Assembly, Chapter 780, approved May 20, 2016. Available: https://budget.lis.virginia.gov/get/budget/3039/. "Out of this appropriation, $2,000,000 the first year and $2,000,000 the second year from the general fund is designated to support a cyber range platform to be used for cyber security training by students in Virginia's public high schools, community colleges, and four-year institutions. Virginia Tech shall form a consortium among participating institutions, and shall serve as the coordinating entity for use of the platform. The consortium should initially include all Virginia public institutions with a certification of academic excellence from the federal government."
[97] Virginia Cyber Range. Available: https://virginiacyberrange.org/.
[98] About the Virginia Cyber Range. Available: https://virginiacyberrange.org/about/.
[99] Virginia Cyber Range. Available: https://virginiacyberrange.org/.
[100] Office of Governor Inslee, "Federal apprenticeship grants will help Washington high-tech workers." Press Release. (2015, September 9). Available: http://www.governor.wa.gov/news-media/federal-apprenticeship-grants-will-help-washington-high-tech-workers. Washington won a $5 million U.S. Department of Labor grant under the American Apprenticeship Initiative in 2015.
[101] Apprenti, Careers. Available: https://apprenticareers.org/. *See also* Apprenti Tech Apprenticeship Update, provided by Jennifer Carlson, Director of Executive Director of the Washington Technology Industry Association Workforce Institute. (2017, July 20).
[102] While there may be other reports and material in the public domain beyond this sampling, the select secondary studies and reports below reflect those reviewed and analyzed for the state case study project and are included here for reference.
[103] Deloitte-NASCIO Cybersecurity Study - State Governments at Risk: Turning Strategy and Awareness into Progress, p. 22. (2016, September). Available: https://www.nascio.org/Publications/ArtMID/485/ArticleID/413/2016-Deloitte-NASCIO-Cybersecurity-Study-State-Governments-at-Risk-Turning-Strategy-and-Awareness-into-Progress.
[104] IBM Center for the Business of Government: Cybersecurity Management in the States: The Emerging Role of Chief Information Security Officers, p. 34. (2010, May). Available: http://www.businessofgovernment.org/report/cybersecurity-management-states-emerging-role-chief-information-security-officers.
[105] Pell Center for International Relations and Public Policy: State of the States on Cybersecurity, p. 7. (2015, November). Available: https://sentinelips.com/wp-content/uploads/2015/11/Pell-Center-State-of-the-States-Report.pdf.
[106] Deloitte-NASCIO Cybersecurity Study - State Governments at Risk: Turning Strategy and Awareness into Progress, p. 5. (2016, September). Available: https://www.nascio.org/Publications/ArtMID/485/ArticleID/413/2016-Deloitte-NASCIO-Cybersecurity-Study-State-Governments-at-Risk-Turning-Strategy-and-Awareness-into-Progress.
[107] Ibid.
[108] Deloitte-NASCIO Cybersecurity Study - State Governments at Risk: Turning Strategy and Awareness into Progress, p. 6. (2016, September). Available: https://www.nascio.org/Publications/ArtMID/485/ArticleID/413/2016-Deloitte-NASCIO-Cybersecurity-Study-State-Governments-at-Risk-Turning-Strategy-and-Awareness-into-Progress.
[109] Ibid.
[110] Ibid.
[111] IBM Center for the Business of Government: Cybersecurity Management in the States: The Emerging Role of Chief Information Security Officers, p. 35. (2010, May). Available: http://www.businessofgovernment.org/report/cybersecurity-management-states-emerging-role-chief-information-security-officers.
[112] Deloitte-NASCIO Cybersecurity Study - State Governments at Risk: Turning Strategy and Awareness into Progress, p. 12. (2016, September). Available: https://www.nascio.org/Publications/ArtMID/485/ArticleID/413/2016-Deloitte-NASCIO-Cybersecurity-Study-State-Governments-at-Risk-Turning-Strategy-and-Awareness-into-Progress.
[113] IBM Center for the Business of Government: Cybersecurity Management in the States: The Emerging Role of Chief Information Security Officers, p. 20. (2010, May). Available: http://www.businessofgovernment.org/report/cybersecurity-management-states-emerging-role-chief-information-security-officers.
[114] Pell Center for International Relations and Public Policy: State of the States on Cybersecurity, p. 6. (2015, November). Available: https://sentinelips.com/wp-content/uploads/2015/11/Pell-Center-State-of-the-States-Report.pdf.
[115] Deloitte-NASCIO Cybersecurity Study - State Governments at Risk: Turning Strategy and Awareness into Progress, p. 10. (2016, September). Available: https://www.nascio.org/Publications/ArtMID/485/ArticleID/413/2016-Deloitte-NASCIO-Cybersecurity-Study-State-Governments-at-Risk-Turning-Strategy-and-Awareness-into-Progress.
[116] Ibid.
[117] Georgia.gov, "Elected Officials." Available: https://georgia.gov/elected-officials.
[118] Statistical Atlas, "Overview of Georgia." Data based on US Census Bureau 2010 census. Available: https://statisticalatlas.com/state/Georgia/Overview.
[119] Information regarding elected officials and state cybersecurity executives was validated in November 2017. "Fast Fact" details were collected in October 2017.
[120] Technical College System of Georgia, "About TCSG." Available: https://tcsg.edu/about-tcsg/.
[121] University System of Georgia, "Prospective Students." Available: http://www.usg.edu/information/prospective_students/.
[122] CollgeCalc, "Private Colleges in Georgia." Available: http://www.collegecalc.org/colleges/georgia/private/.
[123] 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/.
[124] 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.
[125] Interview with Calvin Rhodes, Executive Director and Chief Information Officer, Georgia Technology Authority. (2017, August 28).
[126] Georgia.org, "Industries in Georgia/Information Technology/Cybersecurity." Available: http://www.georgia.org/industries/information-technology/cybersecurity/.
[127] Ibid.
[128] "'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.
[129] 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.
[130] 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/.
[131] 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.
[132] Interview with Dr. Steve Nichols, Chief Technology Officer, Georgia Technology Authority. (2017, August 22).
[133] 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.
[134] About NASCIO. Available: https://www.nascio.org/AboutNASCIO.
[135] O.C.G.A. § 50-25-1.
[136] 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.
[137] 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.
[138] O.C.G.A. § 50-25-4.
[139] 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.
[140] From Dr. Steve Nichols, Chief Technology Officer, Georgia Technology Authority. Email communication. (2017, October 28).
[141] 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.
[142] 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).
[143] 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.
[144] Ibid.
[145] Use of "Georgia Department of Defense" refers to Georgia's National Guard.
[146] 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.
[147] 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.
[148] 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.
[149] Interview with Stanton Gatewood, Chief Information Security Officer, Office of Information Security, Georgia Technology Authority. (2017, September 7).
[150] 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).
[151] Interview with Wade Damron, Director, Risk Management Services, Department of Administrative Services, Georgia Technology Authority. (2017, August 31).
[152] Some of the agencies' state budgets are supplemented with federal funds (e.g., grants).
[153] 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).
[154] Interview with Jeff McCord, Director, Intergovernmental Relations, Georgia Technology Authority. (2017, September 1).
[155] 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.
[156] Ibid.
[157] Georgia.gov, "Enterprise Portfolio Management." Available: https://gta.georgia.gov/epmo-main-page-0.
[158] 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.
[159] 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.
[160] From Dr. Steve Nichols, Chief Technology Officer, Georgia Technology Authority. Email communication. (2017, November 17).
[161] Georgia.gov, "Calvin Rhodes." Available: https://gta.georgia.gov/calvin-rhodes.
[162] Georgia.gov, "Governance, Risk and Consulting." Available: https://gta.georgia.gov/governance-risk-and-consulting.
[163] 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.
[164] Georgia.gov, "Cybersecurity." Available: https://gta.georgia.gov/cybersecurity.
[165] Ibid.
[166] 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).
[167] Georgia.gov, "Cybersecurity." Available: https://gta.georgia.gov/cybersecurity.
[168] Interview with Stanton Gatewood, Chief Information Security Officer, Office of Information Security, Georgia Technology Authority. (2017, September 7).
[169] 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).
[170] Georgia.gov, "Large IT Project Executive Decision-Making Board." Available: https://gta.georgia.gov/psg/article/large-it-project-executive-decision-making-board.
[171] "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.
[172] Georgia.gov, "Large IT Project Executive Decision-Making Board." Available: https://gta.georgia.gov/psg/article/large-it-project-executive-decision-making-board.
[173] Read more about the activities involved in these areas of support here: https://gta.georgia.gov/enterprise-portfolio-management-services.
[174] 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.
[175] 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).
[176] Ibid.
[177] 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.
[178] 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).
[179] 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).
[180] 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.
[181] 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.

[182] 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).
[183] 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).
[184] 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).
[185] Interview with Dr. Steve Nichols, Chief Technology Officer, Georgia Technology Authority. (2017, August 22).
[186] 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.
[187] Georgia.gov, "Incident Response and Reporting." Available: https://gta.georgia.gov/psg/article/incident-response-and-reporting.
[188] Interview with Stanton Gatewood, Chief Information Security Officer, Office of Information Security, Georgia Technology Authority. (2017, September 7).
[189] From redacted version of "State of Georgia, Georgia Technology Authority, Computer Security Incident Response & Handling Plan." Made available by GTA (2017, October 20).
[190] Ibid.
[191] Interview with Walter Tong, Director, Cyber Intelligence, Office of Information Security, Georgia Technology Authority. (2017, October 17).
[192] Cyber Storm V is coordinated by the U.S. Department of Homeland Security.
[193] 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.
[194] Georgia.gov, "Cyber Fusion and Threat Information." Available: https://gta.georgia.gov/cyber-fusion-and-threat-information.
[195] Ibid.
[196] Interview with Stanton Gatewood, Chief Information Security Officer, Office of Information Security, Georgia Technology Authority. (2017, September 7).
[197] Interview with Jeff McCord, Director, Intergovernmental Relations, Georgia Technology Authority. (2017, September 1).
[198] Georgia.gov, "A Look Ahead: Governor Deal Leads in Cyber." Available: https://gta.georgia.gov/annualreport/look-ahead-governor-deal-leads-cyber.
[199] 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.
[200] 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.
[201] 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/.
[202] 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.
[203] 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.
[204] 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.
[205] From "GETS Sourcing Governance Overview." Made available by GTA (2017, September 6).
[206] 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).
[207] Ibid.
[208] Ibid.
[209] From "GETS Sourcing Governance Overview." Made available by GTA (2017, October 26).
[210] From "GETS Sourcing Governance Overview." Made available by GTA (2017, September 6).
[211] 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).
[212] 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).
[213] "GETS Sourcing Governance Overview." Made available by GTA (2017, September 6).

[214] Ibid.
[215] 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).
[216] Ibid.
[217] Michigan.gov, "Branches of Government." Available: http://www.michigan.gov/som/0,4669,7-192-29701---,00.html.
[218] Statistical Atlas, "Overview of Michigan." Data based on US Census Bureau 2010 census. Available: http://statisticalatlas.com/state/Michigan/Overview.
[219] Information regarding elected officials and state cybersecurity executives was validated in November 2017. "Fast Fact" details were collected in August 2017.
[220] Collegestats.org, "Michigan Colleges." Available: https://collegestats.org/colleges/michigan/.
[221] Michigan Economic Development Corporation, "Michigan's Public Universities." Available: http://www.michiganbusiness.org/universities-and-colleges-partners/.
[222] CollgeCalc, "Private Colleges in Michigan." Available: http://www.collegecalc.org/colleges/michigan/private/.
[223] Michigan Economic Development Corporation, "Core Industries." Available: http://www.michiganbusiness.org/core/industries/.
[224] 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.
[225] Interview with David Behen, former Chief Information Officer, DTMB. (2017, March 2).
[226] MCL Chapter 18 Section 18.41. Available: http://www.legislature.mi.gov/(S(1kzimy1qiufegyrvb4usw53n))/mileg.aspx?page=getObject&objectName=mcl-18-41.
[227] Interview with Captain David Kelly, Commander of the Intelligence Operations Division, Michigan State Police; Captain Chris Kelenske, Commander of the Emergency Management and Homeland Security Division, Michigan State Police; and Chris Christensen, Director of Infrastructure Protection, DTMB. (2017, April 14).
[228] Interview with Ashley Gelisse, Chief of Staff, DTMB. (2017, March 2).
[229] Read more about Merit Network in the Workforce & Education section.
[230] 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.
[231] About NASCIO. Available: https://www.nascio.org/AboutNASCIO.
[232] Michigan.gov, "Michigan Announces Cyber Initiative." Available: http://www.michigan.gov/snyder/0,4668,7-277-57577_57657-263758--,00.html.
[233] More about the P-20 initiative. Available: http://greatstartforkids.org/content/so-what-p-20-anyway.
[234] Michigan Cyber Initiative 2015. (2015). Available: http://www.michigan.gov/documents/cybersecurity/Mich_Cyber_Initiative_11.13_2PM_web_474127_7.pdf.
[235] Ibid.
[236] MCL Chapter 18 Section 18.41. Available: http://www.legislature.mi.gov/(S(hn2qlonq5mn1lktnuf5rheug))/mileg.aspx?page=getObject&objectName=mcl-18-41.
[237] "IT Strategy Group Charter." Made available by DTMB. (2017, June 23).
[238] Ibid.
[239] The IT Steering Committee is composed of at least two Agency Services representatives, Infrastructure & Operations General Manager, Agency Services Director, IT Procurement representative, IT Finance Director, Deputy CSO, and others. It meets every other week.
[240] "DTMB IT Governance." Made available by DTMB (2017, June 23).
[241] The Technology Council is composed of the Deputy CSO, Enterprise Architecture Director, and others. It meets every other week.
[242] Interview with Rajiv Das, Chief Security Officer, DTMB. (2017, June 23).
[243] The IT Solutions and Delivery Council is composed of the Chief Financial Officer (CFO), Business Relationship Managers, Center for Shared Solutions representatives (product owners), General Manager from IT Steering Committee, and others. It meets every other week.
[244] "DTMB IT Governance." Made available by DTMB (2017, June 23).
[245] The Financial Management Council is composed of the CFO, IT Finance Director, DTMB Internal Audit representative, and others. It meets monthly.
[246] "Financial Management Charter." Made available by DTMB. (2017, June 23).
[247] The Communications Council is composed of the Director's Office Assistant Administrator, Communications Specialist, Office of Organizational Performance Management Representative, and others. It meets weekly.
[248] "Communications Council Charter." Made available by DTMB. (2017, June 23).
[249] MCL Chapter 18 Section 18.41. Available: http://www.legislature.mi.gov/(S(oaeofmiadbhoherqkwo4pqv1))/mileg.aspx?page=getObject&objectName=mcl-18-41.
[250] Executive Order No.2001 – 3. Available: http://www.michigan.gov/formergovernors/0,4584,7-212-31303_31305-3054--,00.html.
[251] Policy 1365.00 Information Technology (IT) Standard Adoption, Acquisition, Development and Implementation. Available: http://www.michigan.gov/documents/dmb/1365.00_281431_7.pdf.
[252] The Management and Budget Act 431 of 1984. Available: https://www.legislature.mi.gov/(S(ywkpivhjgisruy5qu4oyxeao))/mileg.aspx?page=GetMCLDocument&objectname=mcl-18-1204.
[253] Interview with Rajiv Das, Chief Security Officer, DTMB. (2017, April 12).
[254] Ibid.

[255] Ibid.
[256] Interview with Rod Davenport, CTO. (2017, May 4).
[257] Interview with Rajiv Das, Chief Security Officer, DTMB. (2017, April 12).
[258] The "CISO as a service" capability was developed in response to findings identified by the 21st Century Infrastructure Commission, which was created by Executive Order 2016-5 in March 2016 and was "responsible for identifying strategic best practices to modernize the state's transportation, water and sewer, energy and communications infrastructure." It was composed of state and independent industry experts. Available: http://www.michigan.gov/snyder/0,4668,7-277-57738_57679_57726-381081--,00.html.
[259] Interview with Dr. Joe Adams, Vice President for Research and Cyber Security, Merit Network, Inc., and Executive Director, Michigan Cyber Range. (2017, April 10). Interview with Rajiv Das, Chief Security Officer, DTMB. (2017, April 12).
[260] Michigan Cyber Disruption Response Strategy. (2013, September 16). Available: https://www.michigan.gov/documents/cybersecurity/Michigan_Cyber_Disruption_Response_Strategy_1.0_438703_7.pdf.
[261] Interview with Captain David Kelly, Commander of the Intelligence Operations Division, Michigan State Police; Captain Chris Kelenske, Commander of the Emergency Management and Homeland Security Division, Michigan State Police; and Chris Christensen, Director of Infrastructure Protection, DTMB. (2017, April 14).
[262] Ibid.
[263] State of Michigan Cyber Disruption Response Plan, p. 1. (2015, October). Available: https://www.michigan.gov/documents/cybersecurity/120815_Michigan_Cyber_Disruption_Response_Plan_Online_VersionA_507848_7.pdf.
[264] State of Michigan Cyber Disruption Response Plan, introduction letter. (2015, October). Available: https://www.michigan.gov/documents/cybersecurity/120815_Michigan_Cyber_Disruption_Response_Plan_Online_VersionA_507848_7.pdf.
[265] Interview with Captain Chris Kelenske, Commander of the Emergency Management and Homeland Security Division, Michigan State Police. (2017, April 14).
[266] Complete list of CDRT organizations in section 6 of the CDRP. Available: https://www.michigan.gov/documents/cybersecurity/120815_Michigan_Cyber_Disruption_Response_Plan_Online_VersionA_507848_7.pdf.
[267] Ibid.
[268] Ibid.
[269] Interview with Captain David Kelly, Commander of the Intelligence Operations Division Michigan State Police; Captain Chris Kelenske, Commander of the Emergency Management and Homeland Security Division, Michigan State Police; and Chris Christensen, Director of Infrastructure Protection, DTMB. (2017, April 14).
[270] Ibid.
[271] Interview with David Behen, former Director and CIO, DTMB. (2017, March 2).
[272] Interview with Rajiv Das, CSO, DTMB. (2017, June 23).
[273] Interview with Ashley Gelisse, Chief of Staff, DTMB, and Chad Laidlaw, Senior Policy Analyst, DTMB. (2017, June 8).
[274] Interview with David Behen, former Director and CIO, DTMB. (2017, March 2).
[275] A third Kitchen Cabinet sub-council is being formed for Utilities and Resources. Source: Interview with Rajiv Das, CSO, DTMB. (2017, June 23).
[276] Interview with Meredith Grant, Chief Information Privacy & Security Officer, Henry Ford Health System, and Chair, Michigan Healthcare Cybersecurity Sub-Council. (2017, May 2).
[277] Interview with Captain David Kelly, Commander of the Intelligence Operations Division Michigan State Police; Captain Chris Kelenske, Commander of the Emergency Management and Homeland Security Division, Michigan State Police; and Chris Christensen, Director of Infrastructure Protection, DTMB. (2017, April 14).
[278] Interview with Ashley Gelisse, Chief of Staff, DTMB, and Chad Laidlaw, Senior Policy Analyst, DTMB. (2017, June 8).
[279] Interview with Rod Davenport, CTO. (2017, May 4).
[280] Merit Network, Inc., "About Us." Available: www.merit.edu/about-us.
[281] Training courses meet the Department of Defense's 8570 Information Assurance Workforce Improvement Program requirements and meet other needs such as incident response handling.
[282] Interview with Dr. Joe Adams, Vice President for Research and Cyber Security, Merit Network, Inc., and Executive Director, Michigan Cyber Range. (2017, April 10).
[283] Merit Network, Inc., "Get Trained at a Cyber Range Hub Today." Available: www.merit.edu/cyber-range-hubs.
[284] A. Alusheff, "Pinckney schools first in nation with cybersecurity program," Detroit Free Press. (2016, December 12). Available: http://www.freep.com/story/news/local/michigan/2016/12/12/pinckney-schools-cyber-security/95325834/.
[285] Ibid.
[286] Ibid.
[287] Merit Network, Inc., "Regional Cybersecurity Education Collaboration." Available: https://www.merit.edu/cybered/.
[288] The three initial higher education partners are Central Michigan University, Northern Michigan University, and Wayne State University.
[289] Merit Network, Inc., "Regional Cybersecurity Education Collaboration." Available: https://www.merit.edu/cybered/.
[290] In addition to leveraging its existing technology, technical donors like Cisco Systems provided video distribution equipment. Source: Interview with Joseph Sawasky, President and Chief Executive Officer, Merit Network, Inc.; Dr. Joe Adams, Vice President for Research and Cyber Security, Merit Network, Inc., and Executive Director, Michigan Cyber Range; and Pierrette Templeton, Director of

Communications and Marketing, Merit Network, Inc. (2017, June 23).
[291] Ibid.
[292] K. Johnson, "Governor Snyder is Seeking High School Students for a Unique Cybersecurity Competition." (2016, August 16). Available: https://www.merit.edu/governor-snyder-is-seeking-high-school-students-for-a-unique-cybersecurity-competition/.
[293] Interview with Joseph Sawasky, President and Chief Executive Officer, Merit Network, Inc.; Dr. Joe Adams, Vice President for Research and Cyber Security, Merit Network, Inc., and Executive Director, Michigan Cyber Range; and Pierrette Templeton, Director of Communications and Marketing, Merit Network, Inc. (2017, June 23).
[294] Members include higher education, K-12, government, healthcare, libraries, research institutions, and other Michigan nonprofits. Available: www.merit.edu/services.
[295] Merit Network, Inc., "Michigan Cyber Range." Available: https://www.merit.edu/cyberrange/.
[296] Training courses meet the Department of Defense's 8570 Information Assurance Workforce Improvement Program requirements and meet other needs such as incident response handling.
[297] Ibid.
[298] Merit Network, Inc., "Research and Development." Available: www.merit.edu/research.
[299] Merit Network, Inc., "Michigan Cyber Range." Available: https://www.merit.edu/cyberrange/.
[300] Ibid.
[301] Interview with Dr. Joe Adams, Vice President for Research and Cyber Security, Merit Network, Inc., and Executive Director, Michigan Cyber Range. (2017, April 10).
[302] "A Cyber Range Hub is a facility that provides certification courses, cybersecurity training exercises and product hardening/testing through a direct connection to the Michigan Cyber Range. A hub is a place where community can learn about cybersecurity, helping individuals to prepare for a career in cybersecurity and providing economic development." Available: www.merit.edu/become-a-cyber-range-hub.
[303] C. Halcom, "Wayne State to host new Michigan Cyber Range hub," Crain's Detroit Business. (2017, June 17). Available: http://www.crainsdetroit.com/article/20160621/NEWS/160629922/wayne-state-to-host-new-michigan-cyber-range-hub.
[304] The three initial higher education partners are Central Michigan University, Northern Michigan University, and Wayne State University.
[305] Interview with Joseph Sawasky, President and Chief Executive Officer, Merit Network, Inc.; Dr. Joe Adams, Vice President for Research and Cyber Security, Merit Network, Inc., and Executive Director, Michigan Cyber Range; and Pierrette Templeton, Director of Communications and Marketing, Merit Network, Inc. (2017, June 23).
[306] Regional Cybersecurity Education Collaboration. Available: https://www.merit.edu/wp-content/uploads/2016/10/RCEC_overview10_12.pdf.
[307] Interview with Joseph Sawasky, President and Chief Executive Officer, Merit Network, Inc.; Dr. Joe Adams, Vice President for Research and Cyber Security, Merit Network, Inc., and Executive Director, Michigan Cyber Range; and Pierrette Templeton, Director of Communications and Marketing, Merit Network, Inc. (2017, June 23).
[308] Statistical Atlas, "Overview of New Jersey." Data based on US Census Bureau 2010 census. Available: https://statisticalatlas.com/state/New-Jersey/Overview#nav-map/metro-area. Retrieved October 2017.
[309] Information regarding elected officials and state cybersecurity executives was validated in November 2017. "Fast Fact" details were collected in October 2017.
[310] New Jersey Legislature, General Information: Our Legislature. Available: http://www.njleg.state.nj.us/legislativepub/our.asp.
[311] Statistical Atlas, "Occupations in New Jersey." Data based on US Census Bureau 2010 census. Available: https://statisticalatlas.com/state/New-Jersey/Occupations. Retrieved October 2017.
[312] New Jersey Council of County Colleges. Available: http://www.njccc.org/.
[313] State of New Jersey, Office of the Secretary of Higher Education. Available: http://www.nj.gov/highereducation/colleges/schools_sector.shtml.
[314] New Jersey Economic Development Organization. Available: http://www.choosenj.com/key-industries.
[315] 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.
[316] The OIT was established by Executive Order No. 84 (1984), Executive Order No. 87 (1998), and Executive Order No. 42 (2006). All functions, powers, and duties from the Executive Orders were codified in OIT through the Office of Information Technology Reorganization Act of 2007, N.J.S.A. 52:18A-224 et seq.
[317] C.52:18A-225(7)(g), ftp://www.njleg.state.nj.us/20062007/PL07/56_.HTM.
[318] New Jersey Department of Law and Public Safety, "Analysis of the New Jersey Budget: Fiscal Year 2017-2018." Available: http://www.njleg.state.nj.us/legislativepub/budget_2018/LPS_analysis_2018.pdf.
[319] Interview with Mike Geraghty, New Jersey CISO and Director of NJCCIC, September 1, 2017.
[320] Ibid.
[321] State of New Jersey, "Enterprise Information Security Policies and Standards," January 2017.
[322] Ibid. The CISO and Director of the NJCCIC is also responsible for developing, implementing, and measuring the performance of the information security program by "setting strategic information security planning across the Executive branch…, publishing and maintaining statewide information security policies and standards and providing cybersecurity subject matter expertise to state agencies…."
[323] State of New Jersey Technology Circular, "Enterprise Information Security Management," New Jersey Office of Information Technology, Policy No. YY-00-NJOIT, September 1, 2017.

[324] 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.
[325] About NASCIO. Available: https://www.nascio.org/AboutNASCIO.
[326] State of New Jersey Technology Circular, "Enterprise Information Security Management," New Jersey Office of Information Technology, Policy No. YY-00-NJOIT, September 1, 2017.
[327] Ibid.
[328] State of New Jersey, Office of Homeland Security and Preparedness, Organization overview, https://www.njhomelandsecurity.gov/organization.
[329] National Institute of Standards and Technology (NIST) Cybersecurity Framework for Improving Critical Infrastructure, Draft Version 1; NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations; International Standards Organization 27002:2013 Information Technology — Security Techniques — Code of Practice for Information Security Controls; Center for Internet Security Top 20 Critical Security Controls; Cloud Security Alliance Cloud Controls Matrix; applicable laws and regulatory requirements, lessons learned, industry best practices, and other New Jersey state government business and technology-related considerations.
[330] Information security policies and standards are authorized under N.J.S.A. 52:18a-227, which defines the role of the New Jersey Office of Information and Technology (NJOIT) in the development of policies and standards governing the use of technology by state agencies.
[331] State of New Jersey, "Enterprise Information Security Policies and Standards," January 2017.
[332] State of New Jersey Technology Circular, "Enterprise Information Security Management," New Jersey Office of Information Technology, Policy No. YY-00-NJOIT, September 1, 2017. Available: http://www.nj.gov/highereducation/colleges/schools_sector.shtml.
[333] Interview with David Weinstein, New Jersey CTO, September 6, 2017.
[334] Ibid.
[335] Interview with Mike Geraghty, New Jersey CISO and Director of the NJCCIC, September 1, 2017.
[336] New Jersey Department of Treasury, Joint Circular No. 18-03-OMB/DPP/OIT, "Procurements of Information Technology (IT) Hardware, Software, Subscription-based Solutions and Related Services and Non-IT Equipment," August 22, 2017. Available: http://www.state.nj.us/infobank/circular/cir1803.pdf.
[337] Ibid.
[338] Interview with David Weinstein, New Jersey CTO, September 6, 2017.
[339] New Jersey Department of Treasury, Joint Circular No. 18-03-OMB/DPP/OIT, "Procurements of Information Technology (IT) Hardware, Software, Subscription-based Solutions and Related Services and Non-IT Equipment," August 22, 2017. Available: http://www.state.nj.us/infobank/circular/cir1803.pdf.
[340] State of New Jersey Technology Circular, "Enterprise Information Security Management," New Jersey Office of Information Technology, Policy No. YY-00-NJOIT, September 1, 2017.
[341] Interview with Mike Geraghty, New Jersey CISO and Director of the NJCCIC, September 1, 2017.
[342] Ibid.
[343] NJ OIT Technology Circular (Policy No. 16-05-NJOIT). "System Architecture Review Policy." December 12, 2016. Available: http://www.nj.gov/it/docs/ps/16-05-NJOIT_System_Architecture_Review_Policy.pdf.
[344] Ibid.
[345] The image is adapted from the OIT Technology Circular regarding SAR process, published in December 2016.
[346] New Jersey Office of the Governor, Executive Order 225, "Governor Chris Christie Signs E.O. To Bolster NJ's Cyber Security, IT Enterprise," June 1, 2017. Available: http://www.nj.gov/governor/news/news/552017/approved/20170601a.html.
[347] State of New Jersey Technology Circular, "System Architecture Review Procedure," New Jersey Office of Information Technology, Policy No. 16-05-P1-NJOIT, December 12, 2016. Available: http://www.nj.gov/it/docs/ps/16-05-NJOIT%20P%20System%20Architecture%20Review%20Procedure.pdf.
[348] Ibid.
[349] Ibid.
[350] State of New Jersey, "Enterprise Information Security Policies and Standards," January 2017.
[351] Ibid.
[352] State of New Jersey, "Cybersecurity Incident Response Plan," v1.0, February 2017.
[353] Ibid. The CISO must update the plan at least once a year.
[354] Ibid.
[355] Ibid. Furthermore, "incidents may result from intentional or unintentional actions and may include loss or theft of agency information assets, unauthorized access to agency information assets, introduction of malicious code, or the failure of system security functions to perform as expected."
[356] Ibid.
[357] Ibid.
[358] State of New Jersey, "Enterprise Information Security Policies and Standards," January 2017.
[359] Ibid.
[360] Ibid.
[361] Ibid.
[362] Ibid. Examples of incidents a team might handle are users who:

- Download and install unapproved software, hacking tools, etc.
- Access or download materials in violation of the Acceptable Use policy
- Send spam promoting a personal business
- Email harassing messages to coworkers
- Set up an unauthorized website on one of the agency's computers
- Use file or music sharing services to acquire or distribute pirated materials
- Transfer sensitive materials from the agency to external locations

[363] State of New Jersey, "Enterprise Information Security Policies and Standards," February 2017.

[364] Ibid. Agencies shall consider the following factors when determining the severity of an incident:
- Threat to human safety
- Scope of impact—number and criticality of systems, services, agencies, and people affected
- Financial impact to the agency or state—loss of revenue, financial penalties, etc.
- Sensitivity of the information—personally identifiable information or other confidential data
- Probability of propagation—likelihood that the malware or negative impact will spread or propagate to other systems or agencies
- Reputational impact to the state or an individual agency
- Legal obligations and risks—notification requirements, regulatory issues, potential lawsuits, etc.

[365] State of New Jersey, "Cybersecurity Incident Response Plan," v1.0, February 2017.

[366] Ibid. Any business or public entity required under this section to disclose a breach of security of a customer's personal information shall, in advance of the disclosure to the customer, report the breach of security and any information pertaining to the breach to the Division of State Police in the Department of Law and Public Safety for investigation or handling, which may include dissemination or referral to other appropriate law enforcement entities.

[367] Ibid.

[368] The functions of the ROIC are threefold: conducting watch floor operations (Watch Ops), real-time tactical intelligence analysis (Analysis), and tracking assets (Asset Management and Coordination). During daily operations, these functions are performed to create a complete picture of the current operating environment throughout the state of New Jersey, including external factors that may also present immediate concerns (terrorism, severe weather events, gang or drug problems in neighboring states, etc.), as well as the resources available to address them. During crisis operations, these same functions remain paramount, albeit with much greater immediacy of information flow and expanded outreach to and integration with external agencies and federal partners. Drawing upon its resources and partners, the ROIC remains the center of gravity for the creation of a comprehensive common operating picture of relevant events and happenings within the state.

[369] New Jersey Office of the Governor, Executive Order 178, "Governor Christie Takes Action to Defend New Jersey and its Infrastructure from Cybersecurity Threats," May 20, 2015. Accessible: https://www.cyber.nj.gov/njccic-executive-order-signing/.

[370] Interview with Chris Rodriguez, former Director of New Jersey Office of Homeland Security and Preparedness (OHSP), September 15, 2017.

[371] State of New Jersey, Office of Homeland Security and Preparedness, Organization, https://www.njhomelandsecurity.gov/organization.

[372] Nussbaum, Brian. "State-Level Cyber Security Efforts: The Garden State Model." *Center for Internet and Society at Stanford Law School*. August 24, 2015. Available: http://cyberlaw.stanford.edu/blog/2015/08/state-level-cyber-security-efforts-garden-state-model.

[373] Ibid.

[374] Interview with Chris Rodriguez, former Director of New Jersey Office of Homeland Security and Preparedness (OHSP), September 15, 2017.

[375] Ibid.

[376] New Jersey C.App.A:9-67. Available: http://www.njleg.state.nj.us/2000/Bills/pl01/246_.pdf.

[377] Ibid.

[378] Ibid.

[379] Interview with Chris Rodriguez, former Director of New Jersey Office of Homeland Security and Preparedness (OHSP), September 15, 2017.

[380] Ibid.

[381] Taken from conversation with Mike Geraghty, New Jersey CISO and Director of the NJCCIC, September 1, 2017.

[382] SANS CyberAces.org, "Your gateway to cybersecurity skills and careers," Accessed August 21, 2017, http://cyberaces.org/.

[383] State of New Jersey Technology Circular, "Enterprise Information Security Management," New Jersey Office of Information Technology, Policy No. YY-00-NJOIT, September 1, 2017.

[384] Ibid.

[385] Statistical Atlas, "Overview of Virginia." Data based on US Census Bureau 2010 census. Available: http://statisticalatlas.com/state/Virginia/Overview. Retrieved August 2017.

[386] Information regarding elected officials and state cybersecurity executives was validated in October 2017. "Fast Fact" details were collected in August 2017.

[387] Virginia.gov, "VITA Organization." Available: https://www.vita.virginia.gov/about/.

[388] 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.

[389] In 2003, the legislature passed House Bill 1926 (Nixon) and Senate Bill 1247 (Stosch) to establish VITA.

[390] Virginia Information Technologies Agency, "ITRM Policies, Standards & Guidelines." https://www.vita.virginia.gov/library/default.aspx?id=537#securityPSGs.
[391] Office of the Governor, Commonwealth of Virginia, Executive Order 8, "LAUNCHING "CYBER VIRGINIA" AND THE VIRGINIA CYBER SECURITY COMMISSION," February 25, 2014, http://governor.virginia.gov/media/3036/eo-8-launching-cyber-virginia-and-the-virginia-cyber-security-commissionada.pdf.
[392] Commonwealth of Virginia, "Cyber Commission Final Report." (2016, March 29). Available: https://cyberva.virginia.gov/media/8139/cyber-commission-final-report.pdf.
[393] "Virginia Cyber Security Partnership." (2016, April). Available: https://1pdf.net/download/virginia-cyber-security-partnership_591328a7f6065d001d719da3.
[394] Virginia Final Cyber Security Report. (2016). Available: https://cyberva.virginia.gov/media/6424/virginiacybersecurity_printfinal-83116.pdf.
[395] Virginia Cyber Security Partnership," (2016, April). Available: https://1pdf.net/download/virginia-cyber-security-partnership_591328a7f6065d001d719da3.
[396] The Virginia Cyber Range. Available: https://virginiacyberrange.org/.
[397] Ibid. The nine colleges and universities designated as NSA/DHS Cybersecurity CAEs) or Department of Defense (DoD) Cyber Crime Center (DC3) National Centers of Digital Forensics Academic Excellence (CDFAEs) are:

1. George Mason University – NSA/DHS CAE in Cyber Defense Education (CAE-CDE) and Research (CAE-R)
2. James Madison University – NSA/DHS CAE-CDE
3. Lord Fairfax Community College – NSA/DHS CAE -CDE 2-Year Education (CAE-CDE 2Y)
4. Longwood University – DC3 CDFAE
5. Norfolk State University – NSA/DHS CAE-CDE
6. Northern Virginia Community College – NSA/DHS CAE-CDE 2Y
7. Radford University – NSA/DHS CAE-CDE
8. Tidewater Community College – NSA/DHS CAE-CDE 2Y
9. Virginia Tech – NSA/DHS CAE-R, and CAE in Cyber Operations (CAE-O)
10. Danville Community College – NSA/DHS CAE-CDE 2Y

[398] 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.
[399] About NASCIO. Available: https://www.nascio.org/AboutNASCIO.
[400] "The Commonwealth strategic plan for information technology shall be updated annually and submitted to the Secretary for approval," § 2.2-2007. Available: https://lis.virginia.gov/cgi-bin/legp604.exe?151+ful+CHAP0768.
[401] Virginia code §2.2-225. Available: https://law.lis.virginia.gov/vacode/title2.2/chapter2/section2.2-225.
[402] VITA, "CY 2017 Update to the Commonwealth Strategic Plan for Information Technology for 2017 – 2022." Available: https://www.vita.virginia.gov/it-governance/cov-strategic-plan-for-it/itsp---2017-update/.
[403] Ibid.
[404] Ibid.
[405] Ibid.
[406] Va. Code Ann. §2.2-225 (1999).
[407] Va. Code Ann. §2.2-2100 (1985).
[408] Office of the Governor, Commonwealth of Virginia, Executive Order 8, "LAUNCHING "CYBER VIRGINIA" AND THE VIRGINIA CYBER SECURITY COMMISSION," February 25, 2014, http://governor.virginia.gov/media/3036/eo-8-launching-cyber-virginia-and-the-virginia-cyber-security-commissionada.pdf.
[409] Commonwealth of Virginia, "Cyber Commission Final Report." (2016, March 29). Available: https://cyberva.virginia.gov/media/8139/cyber-commission-final-report.pdf.
[410] Interview with Secretary of Technology Karen Jackson (2017, March 24).
[411] Ibid.
[412] The law directs executive branch agencies to "obtain CIO approval prior to the initiation of any Commonwealth information technology project or procurement [providing an] business case, outlining the business value of the investment, the proposed technology solution, if known, and an explanation of how the project will support the agency strategic plan, the agency's secretariat's strategic plan, and the Commonwealth strategic plan for information technology." Virginia code §2.2-2018.1. Available: https://law.lis.virginia.gov/vacode/title2.2/chapter20.1/section2.2-2018.1/ *See also* Virginia code §2.2-2007. Available: https://law.lis.virginia.gov/vacode/title2.2/chapter20.1/section2.2-2007/.
[413] D. Verton, "Look Who's MeriTalking: Virginia CIO Nelson P. Moe." MeriTalk.com (2016, May 2). Available: https://www.meritalk.com/look-whos-meritalking-virginia-cio-nelson-p-moe/.
[414] Interview with CISO Mike Watson (2017, March 25).
[415] Ibid.
[416] The CIO established a CSRM directorate within VITA to fulfill his information security duties under §2.2-2009. The CSRM is led by the Commonwealth's CISO.
[417] VITA, 2015 Commonwealth of Virginia Information Security Report. Available: https://www.vita.virginia.gov/media/vitavirginiagov/uploadedpdfs/vitamainpublic/security/2015COVSecurityAnnualReport.pdf.

[418] Ibid., pp. 3-4.
[419] Virginia.gov, Governor McAuliffe Announces Virginia Adopts National Cybersecurity Framework. (2014, February 12). Available: https://governor.virginia.gov/newsroom/newsarticle?articleId=3284. See also NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, February 12, 2014, Available: https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.
[420] VITA, 2015 Commonwealth of Virginia Information Security Report, p. 16. Available: https://www.vita.virginia.gov/media/vitavirginiagov/uploadedpdfs/vitamainpublic/security/2015COVSecurityAnnualReport.pdf.
[421] Va. Code Ann. §2.2- 2009.
[422] VITA, 2015 Commonwealth of Virginia Information Security Report. Available: https://www.vita.virginia.gov/media/vitavirginiagov/uploadedpdfs/vitamainpublic/security/2015COVSecurityAnnualReport.pdf. Page 13 of the report lists evaluation criteria for each type of program.
[423] Interview with Mike Watson (2017, March 25).
[424] Interview with Lee Tinsley, CIO, Virginia Department of Veterans Services (2017, June 12).
[425] Ibid.
[426] Executive Directive 6, "Governor McAuliffe Signs Executive Directive to Strengthen Cybersecurity Protocol." (2015, August 31). Available: http://governor.virginia.gov/newsroom/newsarticle?articleId=12544.
[427] Ibid.
[428] The Secure Commonwealth Panel (SCP) is established as an advisory board within the meaning of § 2.2-2100, in the executive branch of state government. The Panel consists of 36 members as follows: three members of the House of Delegates, one of whom shall be the Chairman of the House Committee on Militia, Police and Public Safety, and two non-legislative citizens to be appointed by the Speaker of the House of Delegates; three members of the Senate of Virginia, one of whom shall be the Chairman of the Senate Committee on General Laws and Technology, and two non-legislative citizens to be appointed by the Senate Committee on Rules; the Lieutenant Governor; the Attorney General; the Executive Secretary of the Supreme Court of Virginia; the Secretaries of Commerce and Trade, Health and Human Resources, Technology, Transportation, Public Safety and Homeland Security, and Veterans and Defense Affairs; the State Coordinator of Emergency Management; the Superintendent of State Police; the Adjutant General of the Virginia National Guard; and the State Health Commissioner, or their designees; two local first responders; two local government representatives; two physicians with knowledge of public health; five members from the business or industry sector; and two citizens from the Commonwealth at large. Except for appointments made by the Speaker of the House of Delegates and the Senate Committee on Rules, all appointments shall be made by the Governor.
[429] Interview with Isaac Janak, Cyber Security Program Manager, Office of Secretary of Public Safety and Homeland Security (2017, June 12).
[430] K. Bortle and A. Burge, Cyber Security Incident Response, VITA. (2016, April 7).
[431] K. Bortle and A. Burge, "Guidance on Reporting Information Technology Security Incidents," VITA Commonwealth Security & Risk Management Incident Response Team. (2016, April 7). Available: https://www.vita.virginia.gov/security/default.aspx?id=317.
[432] VITA, IT Incident Response Policy. (2014, July 1). Available: https://www.vita.virginia.gov/media/vitavirginiagov/it-governance/psgs/sec501-pampp-templates/doc/VITA-CSRM-IT-Incident-Response-Policy-v1_0.docx.
[433] Ibid.
[434] Va. Code Ann. §2.2-603(G).
[435] VITA Guidance on Reporting Information Technology Security Incidents. Available: https://www.vita.virginia.gov/security/default.aspx?id=317.
[436] Ibid.
[437] VITA Information Security Incident Reporting Form. Available: https://vita2.virginia.gov/security/incident/secureCompIncidentForm/threatReporting.cfm.
[438] VITA, 2015 Commonwealth of Virginia Information Security Report, p. 7. Available: https://www.vita.virginia.gov/media/vitavirginiagov/uploadedpdfs/vitamainpublic/security/2015COVSecurityAnnualReport.pdf. "All executive branch agencies including institutions of higher education are required to report information security incidents to VITA except for the University of Virginia (UVA), Virginia Polytechnic Institute and State University (VPI), and the College of William and Mary." *See* https://www.vita.virginia.gov/security/default.aspx?id=317.
[439] VITA, "CSRM Information Security Incident Response Procedure v6_0," revised 2/3/2014. Available: https://www.vita.virginia.gov/media/vitavirginiagov/resources/presentations/pdf/InformationSecurityIncidentResponseProcedure.pdf.
[440] Virginia Department of Emergency Management, "Draft Cyber Incident Response Plan." (2017, May), p. 2.
[441] Va. Code Ann. §44-146.16.
[442] Virginia Department of Emergency Management, "Draft Cyber Incident Response Plan." (2017, May), p. 2.
[443] The UC structure includes reference to emergency support functions (ESFs). According to DHS Federal Emergency Management Agency (FEMA), "ESFs provide the structure for coordinating Federal interagency support for a Federal response to an incident. They are mechanisms for grouping functions most frequently used to provide Federal support to States…" *See* DHS, FEMA Emergency Support Function Annexes. Available: https://www.fema.gov/media-library/assets/documents/25512.
[444] Virginia Department of Emergency Management, "Draft Cyber Incident Response Plan." (2017, May), p. 2.
[445] Ibid, p. 4.
[446] Virginia Public Safety and Homeland Security, Cybersecurity, https://pshs.virginia.gov/homeland-security/cyber-security/.
[447] Ibid. Since 2011, the VANG has participated in National Level Cyber Exercises such as the US Cyber Command's Cyber Guard (focus on

protection of critical infrastructure), DoD's Cyber Flag (focused on federal cyber National Mission Forces), and the National Guard's annual Cyber Shield exercise (focused on defense of military networks).
[448] Va. Code Ann. §2.2-222.3.
[449] VITA, 2015 Commonwealth of Virginia Information Security Report, p. 4. Available: https://www.vita.virginia.gov/media/vitavirginiagov/uploadedpdfs/vitamainpublic/security/2015COVSecurityAnnualReport.pdf.
[450] Interview with Lee Tinsley, CIO, Virginia Department of Veterans Services (2017, June 12).
[451] VITA, 2015 Commonwealth of Virginia Information Security Report, p. 7. Available: https://www.vita.virginia.gov/media/vitavirginiagov/uploadedpdfs/vitamainpublic/security/2015COVSecurityAnnualReport.pdf.
[452] Ibid.
[453] Virginia Public Safety and Homeland Security, Cybersecurity, https://pshs.virginia.gov/homeland-security/cyber-security/.
[454] Interview with Rob Reese, Lead Analyst, Virginia Fusion Center (2017, June 28).
[455] Interview with Captain Kevin M. Hood, Division Commander, Criminal Intelligence Division, Virginia State Police (2017, June 28).
[456] Interview with Isaac Janak, Cyber Security Program Manager, Office of Secretary of Public Safety and Homeland Security (2017, June 12).
[457] Virginia Cyber Security Partnership (2016, April). Available: https://1pdf.net/download/virginia-cyber-security-partnership_591328a7f6065d001d719da3.
[458] Virginia Final Cyber Security Report, 2016. Available: https://cyberva.virginia.gov/media/6424/virginiacybersecurity_printfinal-83116.pdf.
[459] Virginia Cyber Security Partnership (2016, April), p. 3. Available: https://1pdf.net/download/virginia-cyber-security-partnership_591328a7f6065d001d719da3.
[460] Ibid, p. 7.
[461] Virginia.gov, Governor McAuliffe Announces State Action to Protect Against Cybersecurity Threats (2015, April 20). Available: https://governor.virginia.gov/newsroom/newsarticle?articleId=8210.
[462] ReedSmith, Technology Law Dispatch. Available: https://www.technologylawdispatch.com/2015/04/data-cyber-security/virginia-launches-first-statelevel-information-sharing-and-analysis-organization/.
[463] Virginia.gov, Governor McAuliffe Announces State Action to Protect Against Cybersecurity Threats (2015, April 20). Available: https://governor.virginia.gov/newsroom/newsarticle?articleId=8210.
[464] As of January 2017, according to Governor McAuliffe, "36,000 cyber jobs are open in the Commonwealth" and cannot be filled due to a lack of talent. YouTube video, "Governor Terry McAuliffe's DCC Press Conference on Cybersecurity" (2017, January 27). Available: https://www.youtube.com/watch?v=OpVlWQJZN3U.
[465] Virginia Cyber Range. Available: https://virginiacyberrange.org/.
[466] 2016 Virginia Acts of Assembly, Chapter 780, approved May 20, 2016. Available: https://budget.lis.virginia.gov/get/budget/3039/. "Out of this appropriation, $2,000,000 the first year and $2,000,000 the second year from the general fund is designated to support a cyber range platform to be used for cyber security training by students in Virginia's public high schools, community colleges, and four-year institutions. Virginia Tech shall form a consortium among participating institutions, and shall serve as the coordinating entity for use of the platform. The consortium should initially include all Virginia public institutions with a certification of academic excellence from the federal government."
[467] Virginia Cyber Range. Available: https://virginiacyberrange.org/about/.
[468] Ibid.
[469] State Council of Higher Education for Virginia, "New Economy Workforce Credential Grant Institution Information." Available: http://www.schev.edu/index/institutional/grants/workforce-credential-grant.
[470] VCCS, "Training Programs are Included in Virginia's New Economy Workforce Industry Credential Grants Program (Updated 6/20/17)." Available: http://cdn.vccs.edu/wp-content/uploads/2016/07/THE-LIST-new-version_updated6.20.17.pdf. Example industry certifications include CISCO Certified Entry Networking Technician, CISCO Certified Network Professional, and Microsoft MTA Networking Fundamentals, among others.
[471] C. P. Nuckols, Virginia Community Colleges, Press Release, "Governor McAuliffe Announces Workforce Grant Program" (2016, July 27). Available: http://www.vccs.edu/newsroom-articles/governor-mcauliffe-announces-workforce-grant-program/.
[472] Virginia.gov, "New Economy Workforce Credential Grant." Available: http://www.schev.edu/index/institutional/grants/workforce-credential-grant. Eligible students pay only one-third of the cost of the program, meaning the government subsidizes two-thirds of the cost if the student completes the program. "This grant program, the first of its kind, provides a pay-for-performance model for funding noncredit workforce training that leads to a credential in a high demand field," such as those related to computers.
[473] CyberVirginia, Cyber Veterans Initiative, http://cybervets.virginia.gov/
[474] Ibid.
[475] VITA, 2015 Commonwealth of Virginia Information Security Report, p. 16. Available: https://www.vita.virginia.gov/media/vitavirginiagov/uploadedpdfs/vitamainpublic/security/2015COVSecurityAnnualReport.pdf.
[476] Ibid., p. 17.
[477] Office of the Governor, Commonwealth of Virginia, "Governor McAuliffe Announces $1 Million in Cybersecurity Scholarships" (2016, August 10). Available: https://governor.virginia.gov/newsroom/newsarticle?articleId=16192.
[478] Interview with Secretary of Technology Karen Jackson (2017, March 24).
[479] For a complete list of members, *see* Cyber Virginia, "Commonwealth of Virginia Cyber Commission First Year Report" (2015). Available: https://cyberva.virginia.gov/media/5442/mary-washington-commission-presentation-2-24-2016.pdf.

[480] Cyber Virginia, Cyber Commission Final Report (2016, March 29). Available: https://cyberva.virginia.gov/media/8139/cyber-commission-final-report.pdf.
[481] Cyber Virginia, "Commonwealth of Virginia Cyber Commission First Year Report" (2015). Available: https://cyberva.virginia.gov/media/5442/mary-washington-commission-presentation-2-24-2016.pdf.
[482] Ibid, p. 4.
[483] VITA, 2015 Commonwealth of Virginia Information Security Report, p. 9. Available: https://www.vita.virginia.gov/media/vitavirginiagov/uploadedpdfs/vitamainpublic/security/2015COVSecurityAnnualReport.pdf
[484] VITA, 2015 Commonwealth of Virginia Information Security Report, Available: https://www.vita.virginia.gov/media/vitavirginiagov/uploadedpdfs/vitamainpublic/security/2015COVSecurityAnnualReport.pdf
[485] Cyber Virginia, "Commonwealth of Virginia Cyber Commission First Year Report" (2015). Available: https://cyberva.virginia.gov/media/5442/mary-washington-commission-presentation-2-24-2016.pdf.
[486] In 2015, the General Assembly passed SB1307, which "clarifies language for search warrants for seizure, examination of computers, networks, and other electronic devices." *See* Cyber Virginia, Cyber Commission Final Report (2016, March 29). Available: https://cyberva.virginia.gov/media/8139/cyber-commission-final-report.pdf.
[487] All statistics taken from the Statistical Atlas, Overview of Washington, data based on US Census Bureau 2010 census. Available: http://statisticalatlas.com/state/Washington/Overview except the population data which is taken from US Census Bureau, Population estimates, July 1, 2016, (V2016). Available: https://www.census.gov/quickfacts/fact/table/WA#viewtop. Retrieved August 2017.
[488] Information regarding elected officials and state cybersecurity executives was validated in September 2017. "Fast Fact" details were collected in August 2017.
[489] 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.
[490] WaTech unifies the former Office of the Chief Information Officer, the original Consolidated Technology Services, and the enterprise applications division of the Department of Enterprise Services. *See* WaTech, "WaTech Re-inventing the Everyday Public Service Experience." Available: http://watech.wa.gov/about. See also RCW 43.105.006, http://apps.leg.wa.gov/RCW/default.aspx?cite=43.105.006.
[491] RCW 43.105.287. Available: http://apps.leg.wa.gov/rcw/default.aspx?cite=43.105.287.
[492] WaTech Technology Services Board. Available: http://ocio.wa.gov/boards-and-committees/technology-services-board-tsb-0. *See also* RCW 43.105.287 for a complete list of powers and duties of the Technology Services Board. For a current list of members, *see* http://ocio.wa.gov/technology-services-board-tsb/technology-services-board-tsb-board-members.
[493] WaTech Technology Services Board, "Policy Actions." Available: http://ocio.wa.gov/sites/default/files/public/policy%20actions_120616.pdf.
[494] Washington State Comprehensive Emergency Management Plan (CEMP), Annex D (2015, March 4). Available: https://mil.wa.gov/uploads/pdf/PLANS/wastatesignificantcyberincidentannex20150324.pdf.
[495] Ibid.
[496] Ibid.
[497] 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.
[498] About NASCIO. Available: https://www.nascio.org/AboutNASCIO.
[499] Ibid.
[500] WaTech unifies the former Office of the Chief Information Officer, the original Consolidated Technology Services, and the enterprise applications division of the Department of Enterprise Services. *See* WaTech, "WaTech | Re-inventing the Everyday Public Service Experience." Available: http://watech.wa.gov/about. See also RCW 43.105.006, http://apps.leg.wa.gov/RCW/default.aspx?cite=43.105.006.
[501] RWC 43.105.220. Available: http://app.leg.wa.gov/rcw/default.aspx?cite=43.105&full=true#43.105.220.
[502] Ibid.
[503] WaTech, Consolidated Technology Services Roadmap. Available: http://watech.wa.gov/sites/default/files/ctsroadmap.pdf.
[504] Interview with Michael Cockrill, Washington State CIO (2017, March 13).
[505] RCW 43.105.240. Available: http://app.leg.wa.gov/RCW/default.aspx?cite=43.105.240.
[506] Agnes Kirk, Washington State CISO. (2017, September 14).
[507] Interview with Agnes Kirk, Washington State CISO. (2017, March 14).
[508] RCW 43.105.287. Available: http://apps.leg.wa.gov/rcw/default.aspx?cite=43.105.287.
[509] WaTech Policy 121: Procedures: "IT Investments - Approval and Oversight - Appendix A: Severity and Risk Assessment." (2014, January 8). Available: https://ocio.wa.gov/policy/it-investments-approval-and-oversight-policy.
[510] WaTech, Office of Chief Information Officer, Agency Preliminary Assessment Tool, https://stofwadeptofenterpriseservices.formstack.com/forms/agency_preliminary_assessment_tool.
[511] WaTech Policy 121: "IT Investments - Approval and Oversight - Appendix A: Severity and Risk Assessment." (2014, January 8). Available: https://ocio.wa.gov/policy/appendix-severity-and-risk-assessment.
[512] Ibid.
[513] Washington State Office of Cyber Security, "About Us." Available: http://www.soc.wa.gov/about-us.
[514] Ibid.

[515] Office of CyberSecurity by the Numbers, Office of CyberSecurity Year in Review. (2017, February 16). Available: https://cybersecurity.wa.gov/cybersecurity-by-the-numbers-bb05664d7477.
[516] Office of Cybersecurity, "Highlights 2016: Monitoring of agencies' compliance with security standards and best practices." Available: https://cybersecurity.wa.gov/office-of-cybersecurity-highlights-2016-816d54e6565d.
[517] This 2015 plan includes a strategic overview of risks to people, property, the economy, and the environment from potential cyber events, a characterization of the level of response needed by federal, state, and local entities, and a brief overview of types and likelihood of cyber-attacks. Available: https://mil.wa.gov/other-links/enhanced-hazard-mitigation-plan; https://mil.wa.gov/uploads/pdf/hazplancyber.pdf.
[518] Washington State Military Department, "Washington Infrastructure Protection Plan." (2008). Available: http://mil.wa.gov/uploads/pdf/PLANS/2008%20washington%20infrastructure%20protection%20plan.pdf.
[519] Ibid.
[520] Washington State Energy Coordinating Council, Washington State Sector Specific Plan for Critical Energy Infrastructure. (2011, November 2011). Available: http://www.commerce.wa.gov/wp-content/uploads/2016/05/Energy-WA-State-Energy-Sector-Specific-Plan-2011.pdf.
[521] Ibid.
[522] WaTech CIO Policies, 143 - IT Security Incident Communication. Available: https://ocio.wa.gov/policy/it-security-incident-communication.
[523] RCW 43.105.020 (19). Available: http://app.leg.wa.gov/RCW/default.aspx?cite=43.105.020.
[524] Washington State Office of Cyber Security, "About Us." Available: http://www.soc.wa.gov/about-us.
[525] A. Kirk, "IT security staff needed to battle hackers," Office of Cybersecurity, State of Washington. (2017, May 30). Available: https://cybersecurity.wa.gov/agnes-kirk-96b464e57a5a.
[526] Office of CyberSecurity by the Numbers, Office of CyberSecurity Year in Review. (2017, February 16). Available: https://cybersecurity.wa.gov/cybersecurity-by-the-numbers-bb05664d7477.
[527] Image derived from information included in WaTech CIO Policies, 143 - IT Security Incident Communication. Available: https://ocio.wa.gov/policy/it-security-incident-communication.
[528] Ibid.
[529] Correspondence with Agnes Kirk, Washington State CISO. (2017, June 29).
[530] Ibid.
[531] Ibid.
[532] RCW 42.56.590. Available: http://apps.leg.wa.gov/rcw/default.aspx?cite=42.56.590.
[533] State of Washington, Office of the Governor, "Designation as Senior Official and Homeland Security Advisor for the State of Washington." (2015, July 29). Available: https://mil.wa.gov/uploads/pdf/emergency-management/hsa-tagcyberletterfromgovernor.pdf.
[534] Washington Military Department, Emergency Management Division, "Washington State Comprehensive Emergency Management Plan." (2016, June). Available: https://mil.wa.gov/uploads/pdf/PLANS/final-wacemp-basic-plan-june2016-signed.pdf.
[535] Washington State CEMP, Annex D. (2015, March 4). Available: https://mil.wa.gov/uploads/pdf/PLANS/wastatesignificantcyberincidentannex20150324.pdf.
[536] Ibid.
[537] Ibid.
[538] Ibid.
[539] Ibid.
[540] Ibid.
[541] The power of the Governor to declare a state of emergency may be found at RCW 43.06.010(12), while the power of the Governor to order the National Guard to active status may be found at RCW 38.08.040.
[542] Interview with David Morris, CTO. (2017, April 25).
[543] Office of CyberSecurity, Security Operations Center, What We Do. Available: http://soc.wa.gov/node/481.
[544] Washington State CEMP, Annex D. (2015, March 4). Available: https://mil.wa.gov/uploads/pdf/PLANS/wastatesignificantcyberincidentannex20150324.pdf.
[545] Ibid.
[546] Ibid.
[547] Interview with David Morris, CTO. (2017, April 25).
[548] Ibid.
[549] The primary state members are senior officials from state government who have executive-level and statewide responsibility for IT leadership. *See* NASCIO, "About NASCIO." Available: https://www.nascio.org/AboutNASCIO.
[550] Governor Jay Inslee's Communications Office, "From coding to creating cool apps: Governor Inslee signs bill to promote computer science in schools." (2014, May 13). Available: http://www.governor.wa.gov/news-media/coding-creating-cool-apps-governor-inslee-signs-bill-promote-computer-science-schools.
[551] Ibid.
[552] State of Washington Office of the Superintendent of Public Schools, "Computer Science K-12 Learning Standards." (2017, March 21). Available: http://www.k12.wa.us/ComputerScience/LearningStandards.aspx.
[553] J. Stang, "Washington Gov. Inslee pushes for broad adoption of new computer science education standards," Geekwire.com. (2016, December 8). Available: http://www.geekwire.com/2016/washington-gov-inslee-pushes-broad-adoption-new-computer-science-

education-standards/.

[554] Washington State has four state colleges and universities designated by the National Security Agency as National Centers of Academic Excellence in Information Assurance/Cyber Defense: (1) Whatcom College in Bellingham; (2) City University in Seattle; (3) the University of Washington in Bothell; and (4) Highline College in Des Moines. *See* https://cybersecurity.wa.gov/agnes-kirk-96b464e57a5a.

[555] Governor Inslee, Office of Governor Inslee, "Federal apprenticeship grants will help Washington high-tech workers," Press Release. (2015, September 9). Available: http://www.governor.wa.gov/news-media/federal-apprenticeship-grants-will-help-washington-high-tech-workers. Washington won a $5 million U.S. Department of Labor grant under the American Apprenticeship Initiative in 2015.

[556] Ibid.

[557] Ibid. Information on apprenticeships is available at www.lni.wa.gov.

[558] Apprenti, About. Available: https://apprenticareers.org/about/.

[559] RCW 43.105.801. Available: http://app.leg.wa.gov/rcw/default.aspx?cite=43.105&full=true#43.105.285.

[560] Ibid. The new law specifically requires the WaTech Director to track how the state develops "future leaders in cybersecurity, as evidenced by an increase in the number of students trained, and cybersecurity programs enlarged in educational settings from a January 1, 2016, baseline"; and (2) develops "broad participation in cybersecurity trainings and exercises or outreach, as evidenced by the number of events and the number of participants."

[561] Interview with Jennifer Carlson, Director of Executive Director of the Washington Technology Industry Association Workforce Institute. (2017, May 3).

[562] Apprenti, Members. Available: https://www.washingtontechnology.org/about/#members.

[563] Interview with Jennifer Carlson, Director of Executive Director of the Washington Technology Industry Association Workforce Institute. (2017, May 3).

[564] Apprenti, Careers. Available: https://apprenticareers.org/. *See also* Apprenti Tech Apprenticeship Update, July 20, 2017, provided by Jennifer Carlson, Director of Executive Director of the Washington Technology Industry Association Workforce Institute.

[565] Interview with Jennifer Carlson, Director of Executive Director of the Washington Technology Industry Association Workforce Institute. (2017, May 3).