2020 NASCIO State IT Award Submission

Cybersecurity

Tennessee Cybersecurity Advisory Council's "Whole-of-Government" Approach

Submitted on July 15th, on behalf of the State of Tennessee

by Strategic Technology Solutions, Department of Finance and Administration

in partnership with the State of Tennessee Cybersecurity Advisory Council

Contact: *Addy Newsom, Special Projects Coordinator – CIO Office*

The State of Tennessee relies heavily on information technology to conduct business each day. The state's IT portfolio contains a vast amount of personally identifiable information (PII); therefore one of the highest priorities of the state is to protect the confidentiality, integrity, and availability of the data received, processed and stored. The maintenance and oversight of the state's information technology security program is essential to both leveraging and protecting data. The enterprise state cybersecurity program includes, but is not limited to: governance, policy, compliance, audit, security operations center, vulnerability management, disaster recovery, and security awareness. Due to the breadth of Tennessee's portfolio and the variance of resources and practices between each Branch, the State is faced with the challenge of providing cybersecurity services with an encompassing, whole-of-government approach. To this end, the State of Tennessee formed a Cybersecurity Advisory Council in 2019.

Significant improvements have been made in the area of governance, risk and compliance for the centralized portion of information technology over the past several years. This has been largely achieved through the consolidation of IT resources from Executive Branch Departments in the State of Tennessee. One of the most notable cybersecurity advancements for the state has been the formation of a statewide cybersecurity council.

The Tennessee Cybersecurity Advisory Council was formed in support of Governor Lee's goal to increase cybersecurity across the entire state, regardless of branch or type of government. In the Fall of 2019, Strategic technology Solutions (STS) drafted a charter and presented it to the Governor's Chief Operating Officer, Chief of Staff, and the Commissioner of the Department of Finance and Administration. With Executive Leadership on board and the Administration's support, the new Council was formed and the first meeting was held on September 11th, 2019 with STS serving as staff to the council.

The Council is co-chaired by the Governor's Chief Operating Officer and State's Chief Information Officer. It contains members representing all branches of TN state government. The council's impressive membership includes the Governor's Chief of Staff, State Chief Information Security Officer, Director of Tennessee Emergency Management Department, Attorney General, Secretary of State, State Comptroller, Director of Tennessee Bureau of Investigation (TBI), Tennessee Adjutant General, Commissioner of Labor and Workforce Development, Commissioner of Safety & Homeland Security, Director of Tennessee Higher

Education Commission, State Treasurer, and Commissioner of the Department of Finance & Administration.

The Council's mission is to provide a collaborative source of knowledge, expertise and information sharing in the field of cyber security supporting the confidentiality, integrity and availability of services and resources. The collective responsibility of the Council is to develop recommendations to the Governor regarding the organizational structure, authority, governance, policies and responsibilities for a coordinated, multidisciplinary, broad-based approach to cybersecurity within the State of Tennessee.

The Tennessee Cybersecurity Advisory Council is currently designing and implementing programs to strengthen public partnerships in cybersecurity. The developing programs will ultimately increase the amount of cyber services available to local county and municipal governments. Increased statewide engagement provides a more accurate threat picture, which subsequently enhances Tennessee's cyber posture. The Council identified four primary areas of focus:

1. *Preparing for and responding to major cyber disruptions*
2. *Establishing coordinated programs that develop highly skilled cybersecurity professionals*
3. *Information sharing, education, and collaboration with Local governments & municipalities*
4. *Promoting the awareness of state security resources and services across the state*

Subsequently, the Council has created four working subgroups, each dedicated to one of the four focus areas. These subgroups are each co-chaired by two Council members, and each team is comprised of multidisciplinary subject matter experts. Each subgroup has determined the goals and priorities of their focus area and are currently working on the identification and ranking of whole-state government resources required to achieve those goals. They are also working on the development of ensuing implementation roadmaps. The primary expected outcome from the overall Council's work is a formalized statewide cybersecurity governance plan, which will include the detailed roadmaps that address the four identified areas of focus.

Simply creating the Council and getting all branches of government "at the table together" was a major step towards achieving whole-of-government approach to the state's cybersecurity governance. Yet, as with any coordinated, multidisciplinary, broad-based approach or effort, risks inherently exist that result from resource sprawl. As such, the Council recognized that achieving a formalized statewide cybersecurity governance plan would be a large undertaking, and that undertakings of this nature typically require a multi-year approach to implementation.

Keeping this in mind, the Council wanted to set a strong baseline for year one, and therefore tasked STS with accurately capturing an inventory of current cybersecurity roles and resources within the state based on the National Initiative for Cybersecurity Careers and Studies' (NICCS) National Initiative for Cybersecurity Education Cybersecurity Workforce Framework (NICE Framework). The NICE Framework provided a blueprint to categorize, organize, and describe cybersecurity work (figure 1.0).

Figure 1.0

Once data was gathered from all areas, Tennessee's capability inventory was loaded into a Tableau dashboard. STS then created interactive data visualizations to accurately portray the State of Tennessee's current cyber matrix. Each Council member was given access to the dashboard, and can drill down to granular levels of detail based on specific role/position, department, or branch of government. Users can categorize information by categories, specialty areas, work roles tasks, and knowledge, skills and abilities. With an accurate picture of cybersecurity coverage for the state, the Council was able to identify gaps and set goals towards filling those gaps over the next two to three years.

While completing the inventory process, STS also discovered varying discrepancy, inconsistency, and lack of datasets for the Tennessee local government contacts that the Council hopes to serve. So, creating a single-source of record for cybersecurity contacts across the state became the second goal for year one. This task was assigned to the Security Information Sharing, Education, & Awareness Workgroup – which is the Council subgroup dedicated to expanding cybersecurity support and communications to Tennessee local governments and municipalities. This team was able to compile a master contact list, as well as define a process to ensure the record will be maintained accurately and remain available to appropriate stakeholders as needed. The subgroup intends to also leverage the contact list to begin a new campaign program designed to push out information proactively. Regular updates will be distributed to the community via a centralized cyber website and email campaign called the Tennessee Cyber Hub. The Cyber Hub is to be housed at the TN.gov/cybersecurity domain, and is currently in development (figure 1.1).

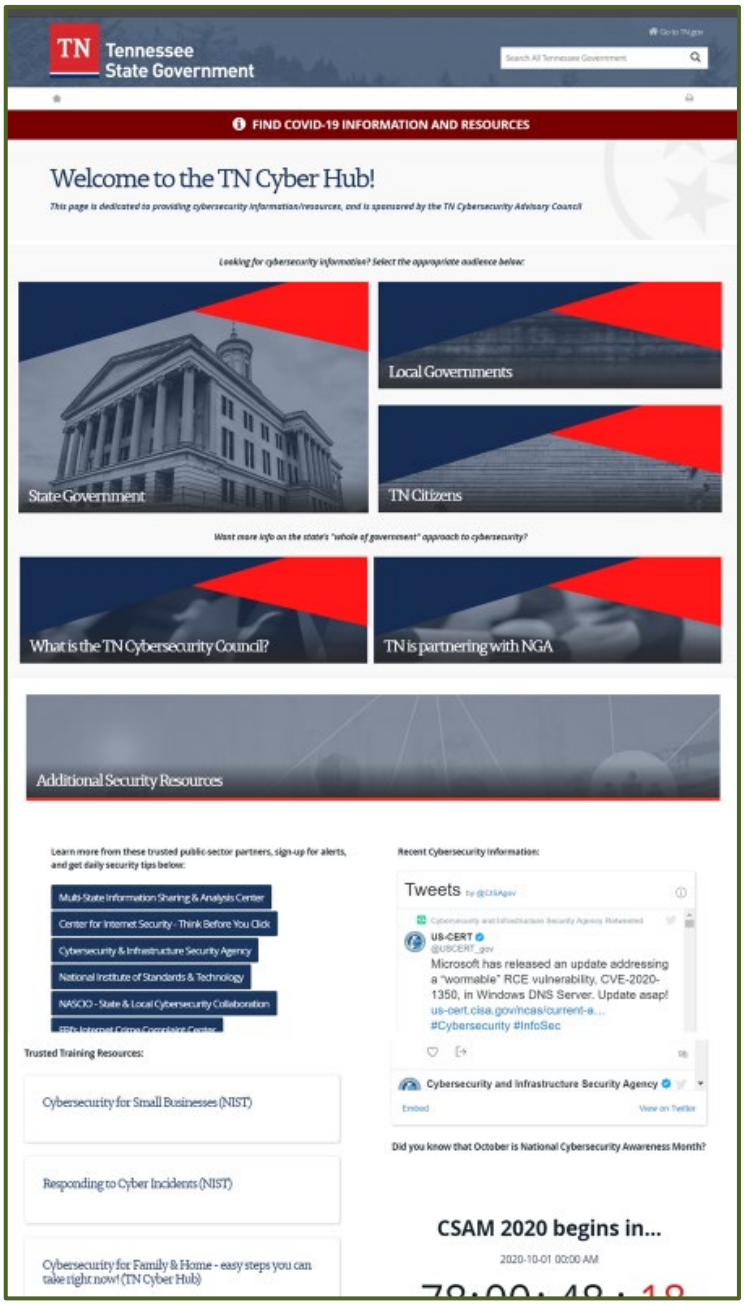

Figure 1.1

The third opportunity for improvement was to be expected in a public sector group. The Council recognized that obtaining the funding and staffing to accomplish actions outlined in subgroup roadmaps as an additional challenge and risk. As part of mitigation of this risk, the Council sought to receive input and experience from subject matter experts and peer states. Research lead to the discovery of a program that could help address some of the roadblocks. The Tennessee Cybersecurity Council submitted an application to participate in the National Governor's Association (NGA) Center of Excellence's *Workshop for Advancing State Cybersecurity,* and was granted one of the six competitive spots available to all 50 states.

Through participation in this NGA workshop, the Council has received valuable information and recommendations, particularly in the area of public/private partnerships. The Council also intends to leverage the Administration's relationship with the Legislature, in order to make the case for necessary funding by communicating expected benefits of said funding in year two and beyond. Leveraging NGA subject matter expertise and proven practices in areas such as these will go a long way into propelling the success of the Tennessee Cybersecurity Advisory Council for years to come.