Tennessee's State-Local Cybersecurity Superheroes:

A Partnership that's Saving the Day, One NCSR Assessment at a Time!

Feb 2023 – May 2024

NASCIO Award Category: Cross Boundary Partnerships

Submitting State: State of Tennessee

Contacts: Addy Newsom, Project Coordinator State CIO Office

Curtis Clan, Chief Information Security Officer

BACKGROUND

Because the State of Tennessee depends heavily upon the internet and cyberspace for conveniences, critical services, and economic prosperity, one of our highest priorities is to protect the confidentiality, integrity, and availability of the data that is shared, received, processed, and stored statewide. Although security is managed very tightly at the State level, there are some local government organizations and municipalities that lack the funding and resources required to protect their assets as robustly as the State can. With the support of the Administration and the Governor's Cybersecurity Advisory Council, the State committed to expanding towards a more "whole-of-government" approach for cybersecurity, which includes increased partnering with local governments and industry experts. Doing so furthers Tennessee's statewide cybersecurity posture and better protects our citizens overall. Reducing Tennessee's statewide cybersecurity risk requires innovative approaches that fully leverage our collective capabilities and the entire cybersecurity community. The State's centralized IT organization, Strategic Technology Solutions (STS), is working with key federal, state, and local government partners to better identify and manage cybersecurity risks statewide.

IDEA

In late 2022, to improve partnerships with local government and better protect citizen data at all levels, Strategic Technology Solutions (STS) developed a plan to leverage American Rescue Plan Act (ARPA) funding to assist with improving Tennessee's whole-of-government cybersecurity posture. The idea was to facilitate statewide completion of the National Cyber Security Review (NCSR). The NCSR is an assessment designed to measure potential cybersecurity gaps and capabilities of all branches of state government, counties, cities, local jurisdictions, and other entities. The assessment's goal is to assess opportunities for improvement and identify significant risks or gaps to protect our citizens and safeguard data. The benefits of implementing the NCSR assessment include increased awareness, risk mitigation, and enhanced communication regarding cyber safeguards.

- Improved awareness and two-way communication between state and local government leaders
- Increased sense of community statewide
- Fostering partnership and trust between state and local government
- Interagency two-way communication and cooperation between the technical department and other state agencies
- Increased outreach and communication between all levels of government statewide

PROJECT SCOPE

In February of 2023, STS partnered with Deloitte to bring this project to fruition and form the TN NCSR project team. The goal for the team was to support approximately 1,500 counties, cities, local jurisdictions, and other entities within Tennessee with the completion of the NSCR. This service was provided free to all participating organizations. Various government entities possess different roles, responsibilities, authorities, and capabilities that can all be brought to bear on cyber incidents. These efforts must be coordinated to achieve optimal results. STS engaged with key partners (Tennessee Cybersecurity Advisory Council, NCSR Engagement Committee, Department of Education, Department of Safety, TEMA, and additional key stakeholders) to collectively address cyber education, vulnerabilities, threats, and consequences. All State Departments, counties, cities, and other jurisdictions within Tennessee were encouraged to participate in the NCSR assessment. In addition to helping them complete the survey and identify their cybersecurity gaps and vulnerabilities, after reviewing individual results STS then provided recommendations on how each entity could close those identified gaps. Additionally, each entity was also encouraged to become a member of the Multi-State Information and Sharing Analysis Center (MS-ISAC) to further improve communications and collaboration at a national level (no membership cost associated). The FY22-FY25 State and Local Cybersecurity Grant Program (SLCGP) then provided the mechanism for these entities to apply for funds enabling them to afford the improvements needed. NSCR completion is a requirement for Tennessee's SLCGP applicants.

The Nationwide Cybersecurity Review is a no-cost, anonymous, annual self-assessment. All State Departments, local governments, tribal nations, and territorial (SLTT) governments are encouraged to participate. It is designed to measure the gaps and capabilities of SLTT governments' cybersecurity programs and is based on the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). Tennessee aims to increase participation in the annual assessment, leading to several benefits to state and local entities. Completing the survey with the Tennessee team allows entities to receive organization-specific metrics to identify gaps and develop a benchmark to gauge year-to-year progress, as well as anonymously measure results against peers. Participants also attain reporting and resources to help prioritize next steps

towards desired cybersecurity improvement. Through further recommendations, entities gain access to a repository of informative references, such as NIST 800-53, COBIT, and the CIS Controls that can assist in managing cybersecurity risk. STS has utilized a state-sponsored team to assist in survey completion, which standardized answers and led to more accurate data for analysis.

Cybersecurity and risk management, including governance, budget and resource requirements, security frameworks, data protection, training and awareness, insider threats, and third-party risk are all covered in the NCSR. Having more data points statewide enables state leaders to identify similar cybersecurity gaps across different entity types and sizes to allow for strategic decision-making for maximum impact across the State of Tennessee at both the State and Local level.

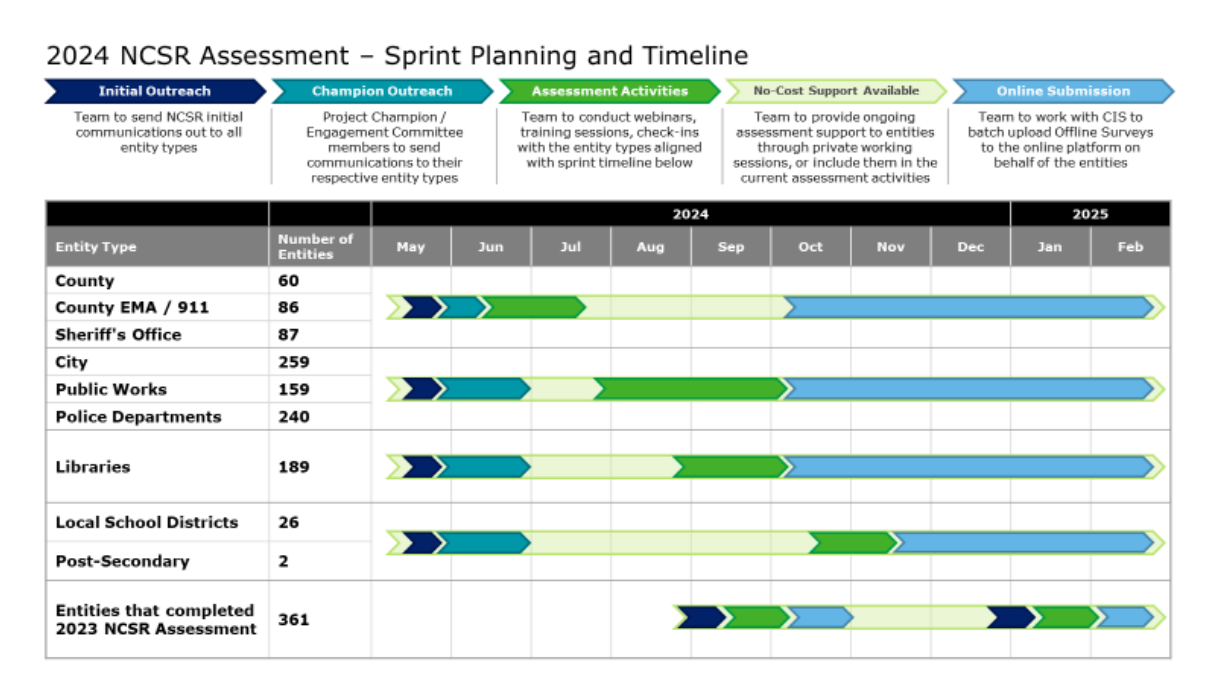
State Resource Layout

- $13.5 million ARPA Grant
- Sponsor
- Program Director
- Program Managers (2)
- 3 State team members
- Weekly 30-minute meetings for the state team
- Tri-Weekly small-group meetings with the vendor team
- Weekly status update meetings with the vendor team
    - Vendor Engagement Resources
        - Program Director
        - Program Manager
        - Project Manager
        - 12-15 consultants
        - Tri-weekly small-group meetings with the state program managers
        - Weekly status update meetings with the state team
- Center for Internet Security (CIS) Coordination Effort
    - Coordination for the online survey portal and answer pre-population from entities' offline surveys.
    - Twice monthly touchpoint meetings

Following the NCSR assessment, a Plan of Actions and Milestones (POA&M) and customized cybersecurity recommendation document is created and shared with each participating entity via data repository. These POAMs include high level recommendations for remediation of the NCSR findings and are developed in conjunction with STS such that it met the needs of participating entities. To provide the most value to the entities, enhanced recommendations are tailored to individual organizations based on their survey answers. The breadth and detail of remediation advice provided within the Cybersecurity Recommendations varies depending on a given entity's staff, budget, size, infrastructure, complexity, and IT maturity. By addressing identified gap and issues, there is increased trust and collaboration between State and Local government, which leads to targeted state assistance provided by the SLCGP grants, and an increase of cybersecurity maturity awareness at an entity level throughout Tennessee. Through these efforts, STS seeks to create a safe and secure cyberspace for Tennessee localities and safeguard the State's data to remain interoperable, secure, and resilient.

IMPLEMENTATION

The Tennessee NCSR project guides policies at an entity level and at a State Department level. Additionally, it provides data for guidance for funding and procurement based on score analysis and overall state recommendations. The Tennessee NCSR project utilizes an Agile approach to maximize flexibility. Entities are placed into internal focus sprints according to entity type to allow for customized outreach activities. Entities are provided with an offline spreadsheet version of the survey, which contains helpful explanations for each question. If additional assistance is needed, the project team offers office hours, webinars, and individual working sessions to facilitate survey completion. Entities are tracked throughout the process and are sent check-in emails periodically to ensure they receive the support they need.



Key Project Areas

- Creation of a statewide contact list for all entities, totaling over 3,000 contacts.
- Communications plan for reaching all 3,000+ contacts.\
- Stakeholder Engagement Committee: 40-member committee providing input on outreach activities and opportunities.
- Conference and speaking opportunities to increase buy-in across the state.
- Universal and directed outreach materials.
- Webinar engagement and office hour availability for efficient one-to-many communications.
- One-on-one meetings with the assessment team for confidential survey support.
- Website (https://www.tn.gov/cybersecurity/local-government-cybersecurity/nationwide-cybersecurity-review--ncsr--assessment.html)
    - 24/7 availability of outreach materials and socialization of project benefits
    - Readily available survey information, FAQ guides, and video walkthroughs
    - Easily accessible grant information and links
    - General Recommendations applicable to all entities across the State

Defining Success

Several factors and variables are essential for successful implementation of the Tennessee NCSR project. First, the ability of the project team to contact each entity. Alongside positive contact, participation in the survey is another metric of success. One of the main project goals is to increase eligibility for the SLCGP grant. An increase in grant applicants year-over-year indicates the success of one of the main goals of the project. Analysis of survey results allows the state to procure services in lieu of grant funding that are aligned with the greatest needs across the state. An increase in grant applicants who apply to utilize these services in lieu of funding is indicative of successful analysis and metric usage to guide service options. Finally, entity participation year-over-year, and analysis of maturity changes over time, is a metric that will be viewed in the coming years to gauge overall success of the project.

Key Stakeholders for Success

- Governor's Tennessee Cybersecurity Advisory Council - Advocate
- CIO - Advocate
- CISO – Oversight
- Deputy CISO - Oversight
- Stakeholder Engagement Committee, 40 members – Advocate, Outreach Efforts

The STS NCSR Engagement Committee is a group of select organizations that provide insight into various local/government organization types, to help influence NCSR participation, and drive annual NCSR adoption in organizations across the state of Tennessee.

Partnering Across TN to Promote the NCSR to Over 1500 Organizations
Engagement Committee Members

NCSR Partnership

State of Tennessee
Strategic Technology Solutions (STS)

Center for Internet Security (CIS)

Counties	Cities	Educational Institutions	Other organizations
ACM – Association of County Mayors; Anthony Holt	**TML** – Tennessee Municipal League; Mark Barrett	**TDOE** – Tennessee Department of Education; Vijay Gollapudi, Steven Sanders	**MTAS –** Municipal Technical Advisory Service; John Chlarson
CTAS – County Technical Advisory Services; Jon Walden	**TAMCAR** – Tennessee Association of Municipal Clerks & Recorders; Will Johnson		**TACP** – Tennessee Association of Chief of Police; Sharry Dedmon-Beard
EMA – Tennessee Emergency Management Agency; James Cotter	**TCMA** – Tennessee City Managers Association; Pat Hardy	**TBR –** Tennessee Board of Regents; Jon Calisi, Tom Sewell	**TSA** – Tennessee Sheriff Association; Jeff Bledsoe
Regional District Leaders Randall Lewis, Brian Young, Raul Hidalgo, Mickey Ledbetter, Sean Cothron , Josh Carney, Skip Burchett, Chaz Morrow, Justin Little, Matt Presson, Smita Sompalli		**THEC –** Tennessee Higher Education Commission; Heather King	**SOS** – Secretary of State; Phil Rogers, John Moravec, Jamie Ritter, Bessie Davis
Development District Executive Directors East Tennessee Development District – Mitch Loomis; Northwest Tennessee Development District – Melinda Goode; Greater Nashville Regional Council – Michael Skipper; Upper Cumberland Development District – Mark Farley; First Tennessee Development District – Mike Harrison; Southeast Tennessee Development District – Chuck Hammonds; South Central Tennessee Development District – Jerry Mansfield; Southwest Tennessee Development District – Joe Barker; MidSouth Development District – Anna McQuiston		**TN Tech** – Tennessee Tech University/ CEROC; Eric Brown	**TBI** – Tennessee Bureau of Investigations; Richard Littlehale

The purpose of the engagement committee includes:

- Maintaining effective two-way communication channels between local government/educational organizations and the STS NCSR team by aligning and distributing key messages while providing insight into any recognized roadblocks.
- Highlighting issues and problems in a timely manner, ensuring continuous improvement and the development of a human-centered experience for each organization before, during, and after the NCSR.
- Develop collaboration and partnership by aligning representative organizations and their respective networks across the state in the STS NCSR process to accelerate participation, completion outcomes, and impact.
- Identify potential outreach and presentation "roadshow" opportunities, both in-person and virtual, to expand the statewide reach of communications.
    - Vendor Support - Implementation
    - Entities- Advocate, End-user, Beneficiary
    - Center for Internet Security (CIS) – Implementation, Beneficiary
    - FEMA – NCSR is mandated for SLCGP grant – Grant governance

As a rapidly changing environment, cybersecurity benefits from collaboration and consistency. The NCSR evaluates security based on the industry leading NIST Cybersecurity Framework (NIST CSF). Answers to the survey must be kept confidential in accordance with State law. To assist the NCSR team in tracking progress, analyzing surveys, and making recommendations, process automation tools, analysis platforms, and a secure repository to safely store constituent data were created.

IMPACT

STS's unique cybersecurity approach ensures that Tennessee expands and matures enterprise cybersecurity programs across not only State governmental programs, but also, support county and local governmental entities by leveraging a trusted federal review, and investing in the appropriate enterprise cybersecurity tools, technologies, and education to best protect all Tennessean's data, at all levels of government.

The NCSR project has provided significant benefit to entities statewide. Tennessee now maintains a dynamic contact listing of over 3,000 contacts for local entities. Local entities now have a better understanding of how the State, through the services of Strategic Technology Solutions, can assist them before, during, and after any cybersecurity incidents. The State has gained understanding of the layout of cybersecurity for entities statewide, and the entities gained knowledge of their current cybersecurity maturity posture and steps they can make towards improvement. The increased collaboration and relationship building between State and Local government has been priceless and will benefit the state for years to come.

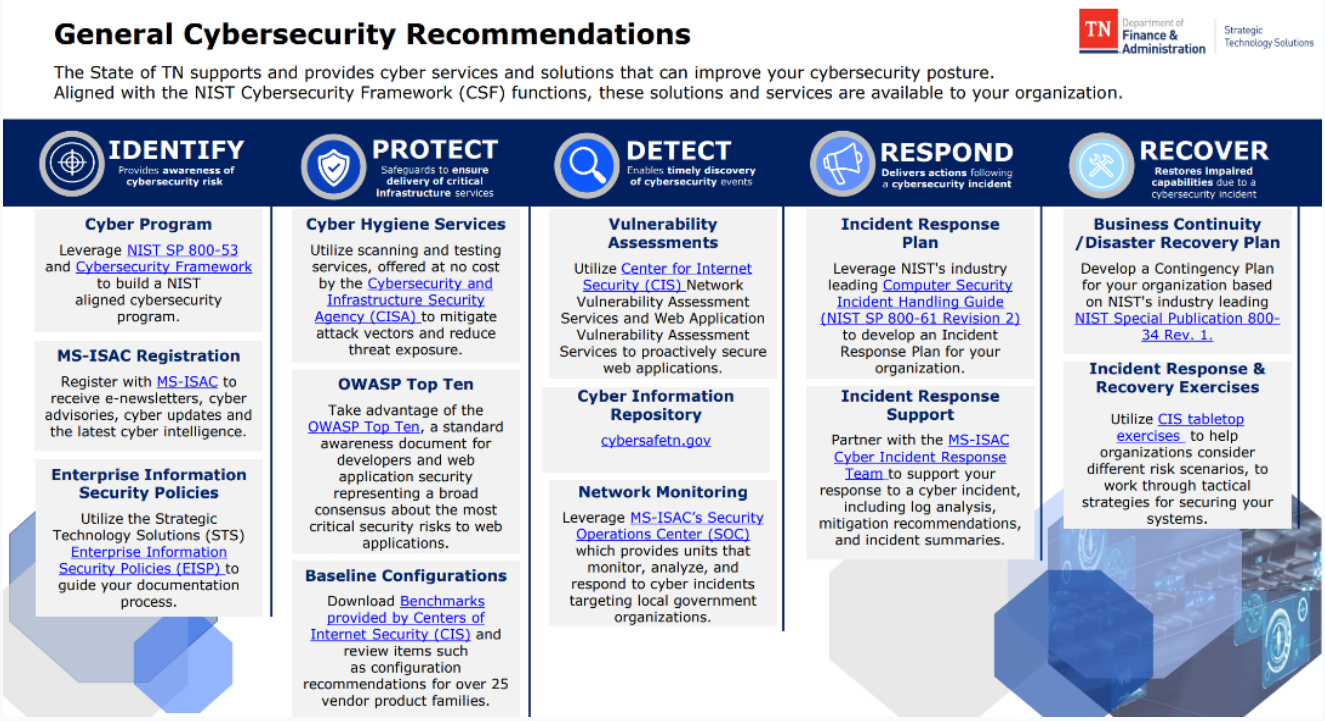
Prior to the collaborative efforts of the Tennessee NCSR team, only 22 entities across the State completed the NCSR. Following outreach efforts in partnership with several organizations across the State, 361 entities completed the survey in 2023, which is an increase of 1,540%. Now these 361 entities have an improved cybersecurity awareness, a dynamic plan of action and milestones, and an enhanced recommendations report for visualizing and prioritizing cybersecurity improvements year-over-year.

NCSR Participation Year	Number of Tennessee Entities
2022	**22**
2023	**361**
2024	**In-process**
Year-over year growth	**1540%**

One of the main benefits of completing the NCSR is eligibility for the State and Local Cybersecurity Grant Program (SLCGP). By working with the State's STS NCSR team, even smaller organizations were able to fulfill the NCSR requirement and become eligible for grant funding and services.

> *"Completing the NCSR was beneficial in helping us think differently about the big picture of our IT infrastructure. Although we're a small town with no dedicated IT resources, completing the NCSR was attainable and now we're eligible for grant funding to help us even more."*
>
> *-Town of Somerville*

The State also now offers General Cybersecurity Recommendations on its CyberSafeTN website. These recommendations include free services and resources applicable to entities across the State.



For those who completed the survey, the Plan of Action and Milestones gave them a good awareness of areas for improvement. In the first year of the project, Tennessee created over 400 POAMs and customized cybersecurity recommendations for both State and Local entities.

> *"Completing the NCSR and receiving our recommended Plan of Actions & Milestones has been a great step in the right direction for our cybersecurity plans. There is no ambiguity in what our next steps should be in becoming more cybersafe."*
>
> *-Tipton County, Non-IT Leader*

NEXT STEPS

The Tennessee NCSR project is currently funded through 2025 using ARPA funds. This will allow for two to three annual iterations of the online NCSR survey for each entity and ongoing recommendation support. The project has established a continued, no-cost, partnership with our group of 40 stakeholders on the engagement committee for long-term local support and outreach. Additionally, the General Recommendations bulletin posted on the CyberSafeTN website will be updated regularly to reflect any changes in best practices or available services throughout the life of the project.