The State of Tennessee's Strategic Technology Solutions Division Presents:

State and Local Cybersecurity Grant Program (SLCGP)

Q&A Webinar | November 2025

TN Department of Finance & Administration | Strategic Technology Solutions

Welcome!

Agenda:

- Introductions
- Program Overview
- Eligibility Requirements
- Application Requirements
- Application Example
- Helpful Resources
- Questions

Introductions

The TN SLCGP Team

- STS Business Operations
  - Christopher Romaine
  - Rebekah Jenkins
  - Marla Riley
  - Alexandra Raver
- Cybersecurity Team
  - Curtis Clan
  - Aime Nsengiyumva
  - Brendan Taylor

Program Overview

What is the SLCGP?

- A federally funded grant program designed to build cybersecurity capabilities at the state and local levels.
- Supports planning, equipment, training activities, and implementation of state and federal cybersecurity strategies.
- Tied to local needs identified through the Nationwide Cybersecurity Review (NCSR).

Eligibility Requirements

Who can apply?

Eligible Tennessee subrecipients of SLCGP include

- Local Governments
- A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under state law), regional or interstate government entity, or agency or instrumentality of a local government
- An Indian tribe or authorized tribal organization
- A rural community, unincorporated town or village, or other public entity
- A public educational institution (e.g., elementary school, secondary school, or institution of higher education) if it is an agency or instrumentality of a state or local government under state and/or local law

Who cannot apply?

Ineligible subrecipients of SLCGP

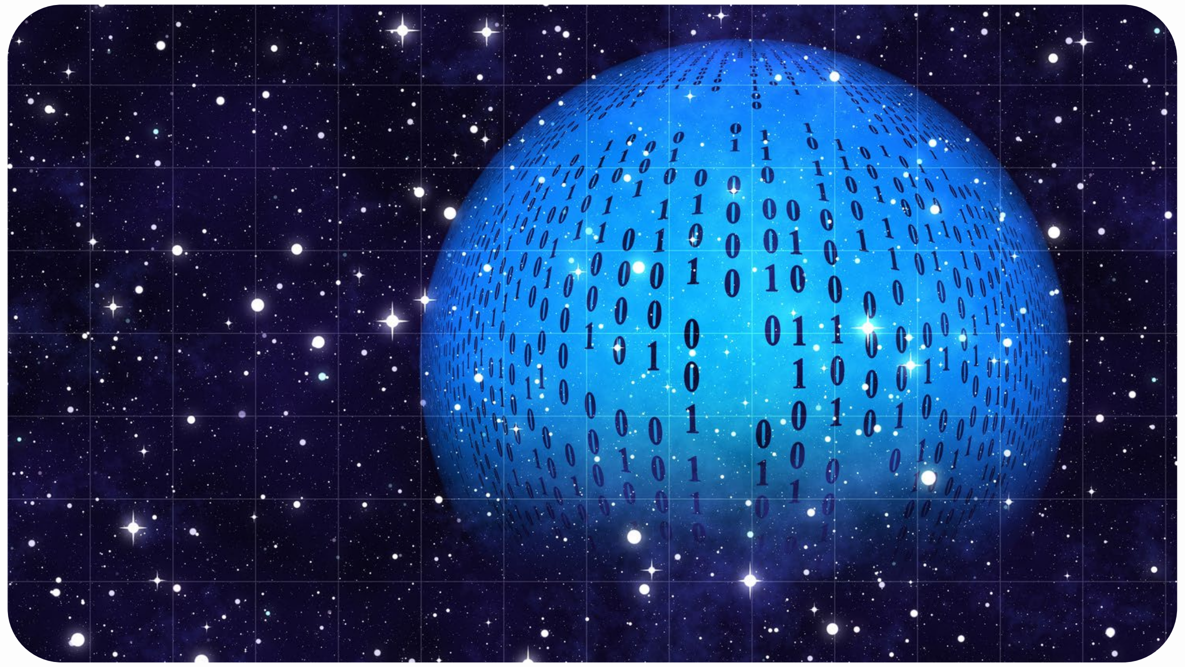
- Nonprofit organizations
- For-profit organizations
- Private educational institutions

FFY2024 SLCGP Funding for Year Three

The total funding available for local entities is approximately $6M

Project 1: Cybersecurity Detection and response -Endpoint Direction and Response (EDR)

Project 2: Access to end -user cybersecurity training for all local government employees



Project 3: Direct reimbursement for cybersecurity gaps identified in completed NCSR assessments

Application Requirements

How to apply?

- State of Tennessee’s Strategic Technology Solutions emails contacts and posts on our website the funding availability for SLCGP.

- Applicants must complete the National Cybersecurity Review (NCSR) assessment.

- Applicants must complete the Local Government Investment Justification (IJ) Worksheet.

- Submit completed IJ’s to cybersafetn@tn.gov by the application deadline date.

Applying?

- All eligible applicants must complete the National Cybersecurity Review (NCSR) assessment.
- Projects for Direct reimbursement for cybersecurity gaps identified in completed NCSR assessments (Project 3) must clearly articulate findings discovered in your NCSR assessment and comply with the requirements of the Authorized Equipment List (AEL)
- Projects selected for funding must be approved by the Cybersecurity Planning Committee
- Application deadline is **December 12, 2025, 12:00 PM CST / 1:00 PM EST**

How to get started with the NCSR

Email NCSR@TN.gov to get started on the NCSR with our team of cybersecurity professionals.
If you completed in 2024, you must complete it again to become grant-eligible!

What is NCSR and how they help your organization?

NCSR is a no-cost, annual self-assessment to help organizations improve their cybersecurity maturity.

Receive no-cost support completing the NCSR and access to suggested corrective actions, metrics specific to your organization to help you identify areas of improvement, prioritize next steps, and increase your cybersecurity maturity over time.

STS will provide guidance to your organization through webinars, walkthroughs, working sessions, and office hours.

Have questions? Contact the team at NCSR@tn.gov.

TN

Complete the Investment Justification Form

01 Required to be considered for funding.

02 Proposed projects must align with NCSR findings.

03 Must comply with the Authorized Equipment List (AEL) for Project type 3.

04 Submit by Friday December 12, 2025,
12 p.m. CT / 1 p.m. ET to:
cybersafetn@tn.gov.

Previous Project Examples

Previous Project Examples

Previous project examples have included:

SIEM (security information and event management) – (DE.AE-3) Provides logging architecture supports real-time collection of device logs, file integrity monitoring (FIM) events, and any other application or system that supports syslog.

Vulnerability Management – (DE.CM-8) Provides continuous discovery and prioritization of security vulnerabilities.

Email Filtering, Protection, and Encryption – (DE.CM-4) Provides the users with an easy-to-use filtering solution with virus, phishing, and spam protection, along with email Encryption.

CyberSecurity Training – (PR.AT-1) Provides weekly and annual cyber security training videos and quizzes for training, along with phishing simulation to help gauge employee training retention.

DMARC Management – Provides management for DMARC reporting on all sending sources for the domain.

Backup for Microsoft 365 – (PR.IP-4) Provides cloud backup for Microsoft 365 Email, OneDrive, and SharePoint.

Previous Project Examples

Password Management – Provides a secure means for the employees to store passwords that can be managed by the entity in an administrative portal. More secure alternative than users storing passwords in their browsers.

Compliance Management Application (GRC) – (ID.GV-3) Provides an application to manage compliance and policies based on many different Frameworks.

Upgrade to Microsoft 365 Premium –These subscriptions do not have the logging and security necessary for the security add-ons listed above. Upgrading all the licenses to Microsoft 365 Business Premium will provide this functionality. This would also provide the ability to enroll endpoints into Intune to manage policies and deploy Defender for Endpoint.

Network Firewall – (DE.CM-1) Provides network security, regulating inbound and outbound traffic, separating trusted and untrusted networks, and network traffic monitoring.

Endpoint Backup – (PR.IP-4) Provides secure local and cloud backup for endpoints (PCs, Servers)

Helpful Resources

DHS Fiscal Year 2024 State and Local Cybersecurity Grant Program NOFO

https://www.fema.gov/sites/default/files/documents/fema_fy2024_slcgp_nofo.pdf

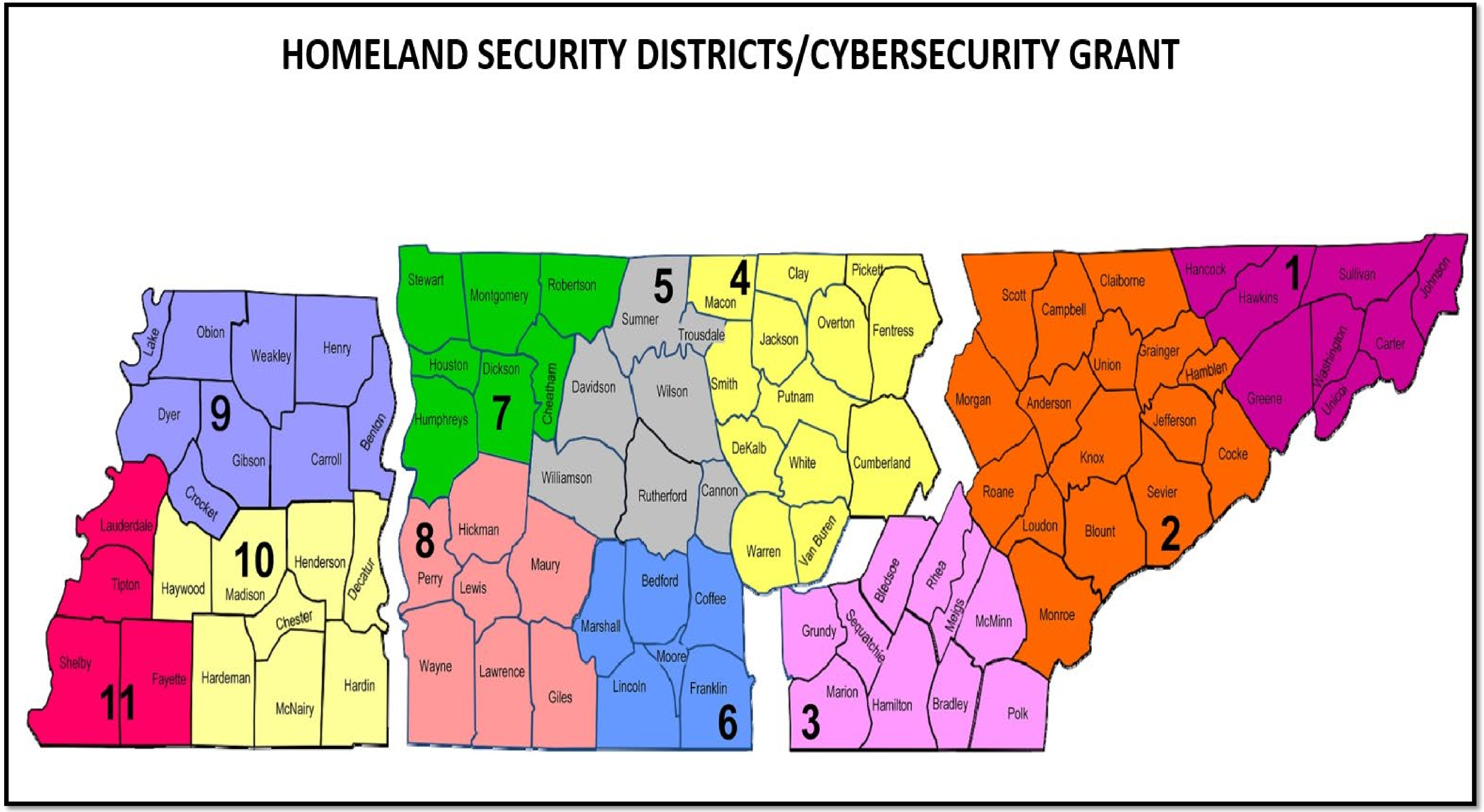
- Section A.10.b. - **Key Cybersecurity Best Practices for Individual Projects**
- Section C.3.b. - **Subrecipient Eligibility**
- **Section D.13 - Unallowable Costs**

Authorized Equipment List

https://www.fema.gov/grants/tools/authorized-equipment-list

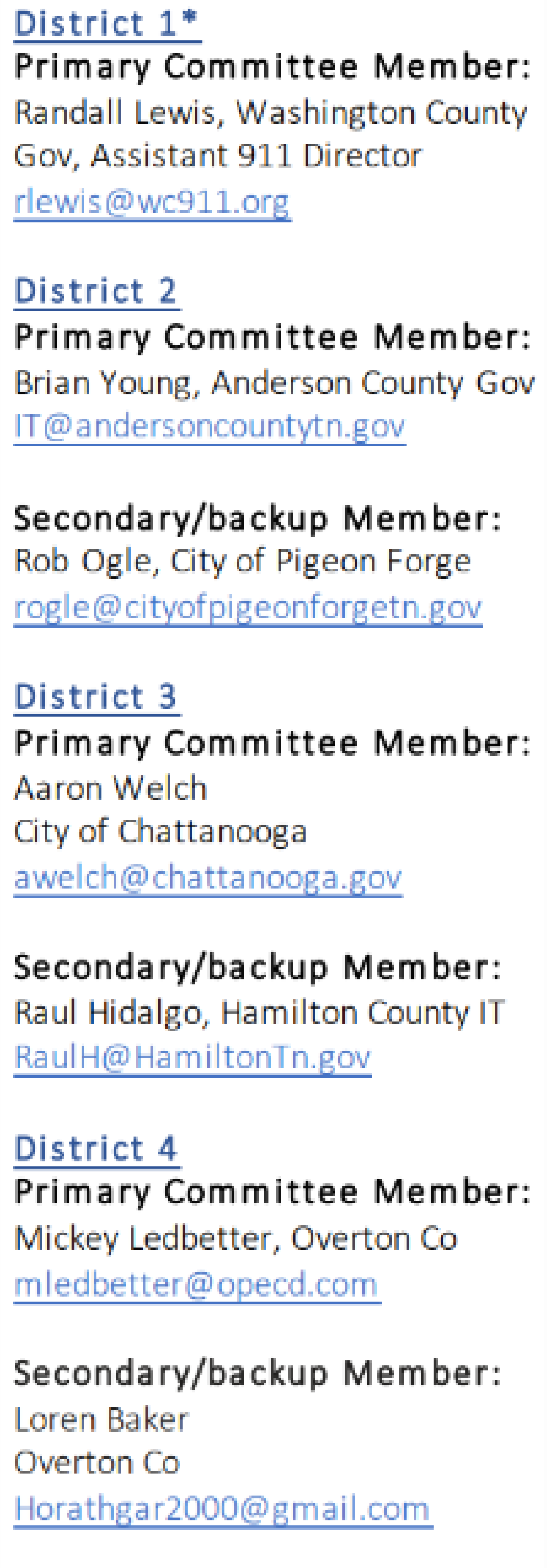
- The AEL contains approved equipment types allowed under FEMA’s preparedness grant programs, including SLCGP.

Cybersecurity Planning Committee Members/TN Homeland Security Districts Map



Cybersecurity Planning Committee Members/TN Homeland Security Districts Contacts

TN Cyber Grant Planning Committee - Local Membership District Info



District 1*
Primary Committee Member:
Randall Lewis, Washington County Gov, Assistant 911 Director
rlewis@wc911.org

District 2
Primary Committee Member:
Brian Young, Anderson County Gov
IT@andersoncountytn.gov

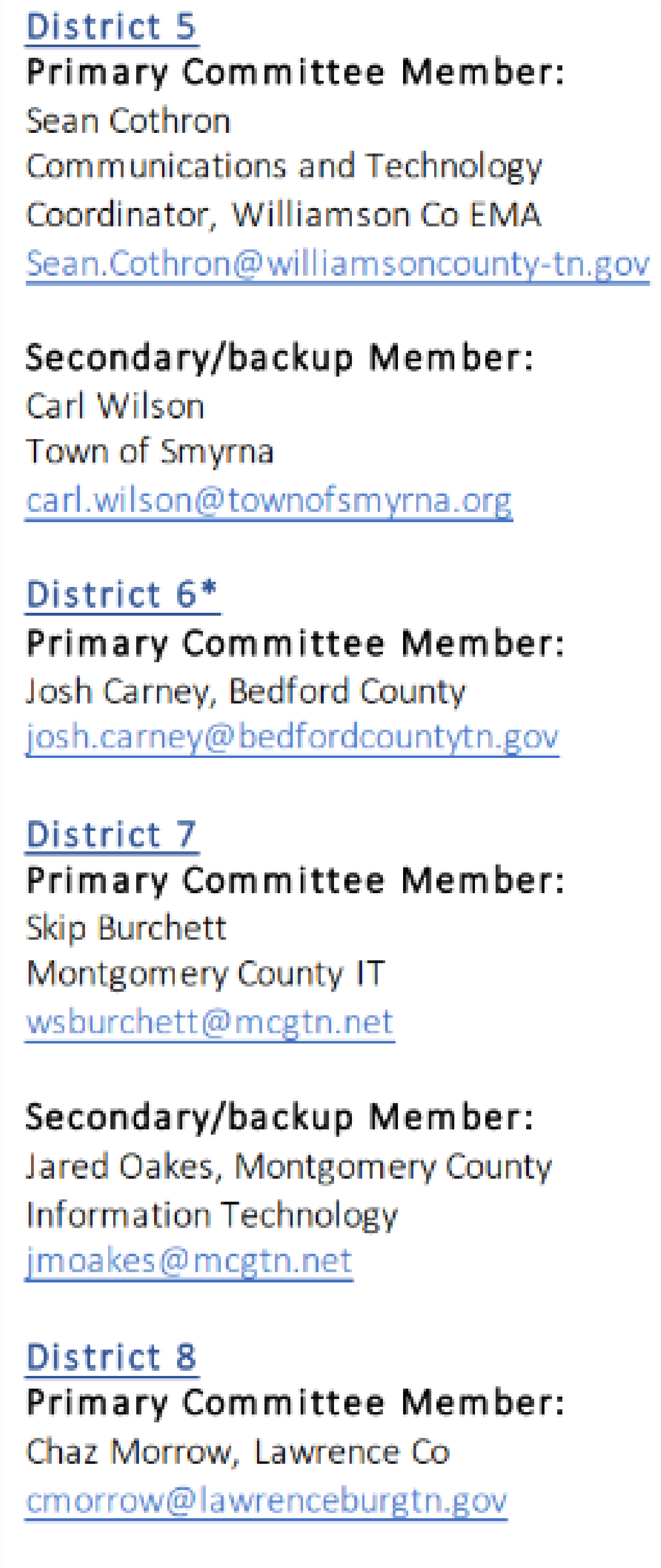
Secondary/backup Member:
Rob Ogle, City of Pigeon Forge
rogle@cityofpigeonforgetn.gov

District 3
Primary Committee Member:
Aaron Welch
City of Chattanooga
awelch@chattanooga.gov

Secondary/backup Member:
Raul Hidalgo, Hamilton County IT
RaulH@HamiltonTn.gov

District 4
Primary Committee Member:
Mickey Ledbetter, Overton Co
mledbetter@opecd.com

Secondary/backup Member:
Loren Baker
Overton Co
Horathgar2000@gmail.com



District 5
Primary Committee Member:
Sean Cothron
Communications and Technology Coordinator, Williamson Co EMA
Sean.Cothron@williamsoncounty-tn.gov

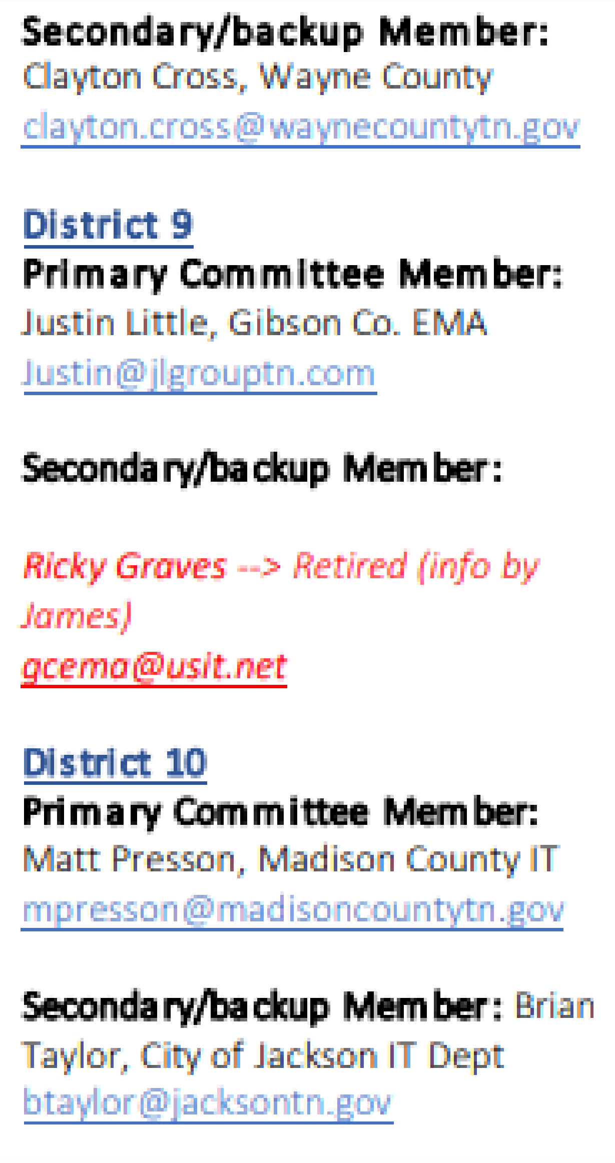
Secondary/backup Member:
Carl Wilson
Town of Smyrna
carl.wilson@townofsmyrna.org

District 6*
Primary Committee Member:
Josh Carney, Bedford County
josh.carney@bedfordcountytn.gov

District 7
Primary Committee Member:
Skip Burchett
Montgomery County IT
wsburchett@mcgtn.net

Secondary/backup Member:
Jared Oakes, Montgomery County Information Technology
jmoakes@mcgtn.net

District 8
Primary Committee Member:
Chaz Morrow, Lawrence Co
cmorrow@lawrenceburgtn.gov



Secondary/backup Member:
Clayton Cross, Wayne County
clayton.cross@waynecountytn.gov

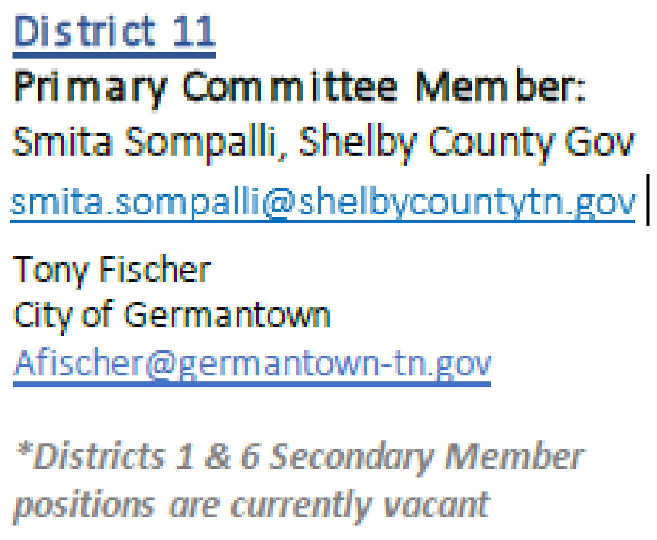
District 9
Primary Committee Member:
Justin Little, Gibson Co. EMA
Justin@jlgrouptn.com

Secondary/backup Member:

Ricky Graves --> Retired (info by James)
gcema@usit.net

District 10
Primary Committee Member:
Matt Presson, Madison County IT
mpresson@madisoncountytn.gov

Secondary/backup Member: Brian Taylor, City of Jackson IT Dept
btaylor@jacksontn.gov



District 11
Primary Committee Member:
Smita Sompalli, Shelby County Gov
smita.sompalli@shelbycountytn.gov

Tony Fischer
City of Germantown
Afischer@germantown-tn.gov

**Districts 1 & 6 Secondary Member positions are currently vacant*

QUESTIONS?

Your Cybersecurity Grant Team:

Marla Riley and Alexandra Raver

Email us: cybersafetn@tn.gov

Your NCSR Team:

Email: ncsr@tn.gov

Your Cybersecurity Grant District Representative: