TN Department of Commerce & Insurance

Tennessee Emergency Communications Board
Reimbursement Requirements For
E-911 PSAP CYBERSECURITY EXPENSES

Effective July 1, 2023

The Tennessee Emergency Communications Board ("TECB") was created "for the purpose of assisting emergency communications district boards of directors in the area of management, operations, and accountability, and establishing emergency communications for all citizens of the state."[1] The TECB is authorized to develop and implement a plan for providing statewide wireless enhanced 911 service, establish operating standards concerning acceptable uses of revenue for emergency communications districts and establish technical operating standards. The TECB is also authorized to act on the behalf of the state's districts to implement wireless enhanced 911 service pursuant to Docket 94-102 of the Federal Communications Commission (hereafter, "the FCC") and subsequent rulings and orders of the FCC, and other federal and state laws and regulations.

To further its statutory purpose, the TECB has the power and authority to:

> Respond to requests from emergency communications districts, commercial mobile radio service providers or other parties and subject to availability of funds, review and approve requests for reimbursements for expenditures or payment of obligations incurred to implement, operate, maintain, or enhance statewide wireless enhanced 911 service in conformance with any rules or orders of the federal communications commission, and other federal and state requirements that pertain to wireless enhanced 911 service;[2]

Pursuant to such authority, during the May 3, 2023 meeting, the Board voted to provide a designated amount per emergency communications district for reimbursements of seventy-five percent (75%) of ECD expenditures for obtaining cybersecurity items or services. Cybersecurity is defined as the protection of computer systems and networks from attack by malicious actors that may result in unauthorized information disclosure, theft of, or damage to hardware, software, or data, as well as from the disruption or misdirection of the services they provide.

Compliance with the following procedures is required to be eligible for cybersecurity cost recovery.

[1] Tenn. Code Ann. § 7-86-302(a).
[2] Tenn. Code Ann. § 7-86-306(a)(10).

TN Department of Commerce & Insurance

REIMBURSEMENT PROCEDURES

The following procedures shall be followed.

1) The ECD must submit its request for reimbursement in writing (via email, fax, or mail) to the TECB Executive Director, describing specifically items or services to be obtained and the estimated cost thereof and justifying the purchase. A menu of potential activities is provided as Attachment B to this document. If your activity does not fall within a category described on this attachment, please provide a detailed explanation of the cybersecurity related benefits of your activity.
2) The TECB Executive Director, relying on staff and others, will review all requests and notify the ECD of approval or rejection. Appeals of rejections may be presented to the TECB members at the next scheduled meeting. Requests for appeal must be received no later than two (2) weeks prior to a board meeting to be considered during that meeting.
3) A signed request for reimbursement certifying the funds were expended for cybersecurity items or services must be submitted with a copy of original invoice(s), along with proof of payment totaling or exceeding the amount being requested for reimbursement. A sample Request for Reimbursement is attached hereto as Attachment A.
4) TECB staff shall process payment through the state's accounting system and keep records and schedules of requests and payments to ensure documentation is appropriate and maximum reimbursements are not exceeded.

Department of Commerce & Insurance

Attachment A

CYBERSECURITY COSTS
REIMBURSEMENT REQUEST

District:

Contact:

Address:

Description	Cost	25% ECD Match	TECB Reimbursement
TOTAL REQUEST			

CERTIFICATION

I hereby certify that the amount claimed on this request for reimbursement pursuant to Tenn. Code Ann. § 7-86-306(a)(11) was expended for cybersecurity items or services.

I further certify that the information supporting this request for reimbursement is true and accurate to the best of my knowledge and I hereby request reimbursement as an authorized representative of the ECD named above.

Signature of District Agent

Date

TN Department of Commerce & Insurance

ATTACHMENT B

CSF Categories
Tasks
Explanations

A. Asset Management, Anomalies and Events, Detection Processes
Network Monitoring
Automated network discovery, documentation of network device inventory, and subnets, monitoring device and network utilization, errors, and status with visualization and alerting

B. Anomalies and Events, Security Continuous Monitoring, Detection Processes, Response Planning, Communications, Analysis, Mitigation
Manage Detection and Response (MDR) 24x7
24x7 protection against advanced modern-day cyberthreats to include ransomware, utilizes an endpoint agent deployment along with live network and asset visibility to visualize alerts and hunt threats in real time

C. Asset Management, Risk Assessment
NIST Cybersecurity Framework Assessment
An independent 3rd party audit of you IT environment that is assessed against Industry Standards and includes:
- Comprehensive understanding of risks
- Vulnerability Assessment
- Penetration Test
- Understand cybersecurity maturity
- Documented Recommendations

D. Awareness and Training
Cybersecurity Instructor-Led Training
Instructor-led session, allowing clients to talk in more detail with their peers and the instructor focused on cyber security for either the Telecommunicator or Executive Leadership

E. Awareness and Training
Phishing Awareness Exercises
- Assists in the management of a culture of cyber defense
- Many successful attacks contain an element of social engineering
- Inexpensive, fast to execute
- Specifically address Continuity

F. Governance
Cybersecurity Policy Creation
Develop a cybersecurity policy that is aligned with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)

G. Governance
   Compliance Management
      Put in place an operational structure that will streamline the assessment, remediation and documentation processes for all IT requirements ensuring of adherence to all regulatory and legal obligations

H. Identity Management, Authentication and Access Control
   Password Management
      Software solution that will store and manage passwords in a safe encrypted place with an audit trail, revision history, and granular access control

I. Identity Management, Authentication and Access Control
      Privilege Escalation
      Audit system configuration to identify and remove/adjust local admin rights from users without giving up the operational capability of an application that needs to run with privileged permissions

J. Identity Management, Authentication and Access Control, Data Security
   System Hardening
      Checks operating systems against industry security baselines to determine whether the systems are configured to an acceptable level to protect against malicious attackers

K. Identity Management, Authentication and Access Control
   Multi-Factor Authentication
      Provide a user authentication method that requires the user to provide two or more verification factors to gain access to a system

L. Identity Management, Authentication and Access Control, Data Security
   System Hardening
      Checks operating systems against industry security baselines to determine whether the systems are configured to an acceptable level to protect against malicious attackers

M. Information Protection Processes and Procedures, Response Planning
   Cybersecurity Incident Response Plan
      Develop an Incident Response Plan that is based on the established industry standards provided by the National Institute of Standards and Technology (NIST) Special Publication 800-61: Computer Security Handling Guide

N. Information Protection Processes and Procedures
   Data Protection Backup solutions
      Utilize a backup and recovery solution that can quickly deploy as a virtual appliance in VMware vSphere and Microsoft Hyper-V environments that performs host-level backups of the virtual machines you choose to

protect. Backups should be tested for viability, and AI scans every backup to identify ransomware and prevent the use of infected files

O. Risk Assessment
   Cybersecurity Assessment Remediation Support
      Develop and execute a prioritized risk remediation plan based on risk level of the criticality impact and probability factors from most recent cybersecurity assessment

P. Risk Assessment
   External Penetration Test
      An external penetration test determines the environment's exposure to anonymous Internet attackers

Q. Risk Assessment, Information Protection Processes and Procedures
   Monthly Vulnerability Scanning and Assessment
      Automated recurring scanning of the network to discover, analyze and report on security flaws and vulnerabilities based on agreed parameters

R. Risk Assessment
   Ransomware Simulation
      Process of simulating a ransomware attack to see if your network is vulnerable to a ransomware attack and validate response plan through tabletop exercise

S. Risk Assessment
   Penetration Testing Web Applications
      Web application tests determine how well the system implements common security requirements within web applications that support the service

T. Security Continuous Monitoring
   Dark web ID Monitoring
      Monitors the dark web and detects compromised credentials in real time and notifies you immediately

U. Supply Chain Risk Management
   Third-Party Risk Management
      - Vendor risk mitigation strategies, policies for external dependencies, and contractual cybersecurity standards
      - Invite vendors into the platform to complete their standardized control assessment in an easy-to-use, secure tenant
      - Centralize supporting documents submitted as evidence of the presence of controls

Department of Commerce & Insurance

TENNESSEE EMERGENCY COMMUNICATIONS BOARD
Comparison of Alternative Funding Options for Cybersecurity Program
TECB Approved May 3, 2023

ECD	CTP Adjusted	ECD	CTP Adjusted
Anderson	50,000	Knox	100,000
Bedford	50,000	LaFollette	50,000
Benton	50,000	Lake	50,000
Bledsoe	50,000	Lauderdale	50,000
Blount	75,000	Lawrence	50,000
Bradley	75,000	Lewis	50,000
Brentwood	50,000	Lincoln	50,000
Bristol	50,000	Loudon	50,000
Campbell	50,000	Macon	50,000
Cannon	50,000	Madison	75,000
Carroll	50,000	Marion	50,000
Carter	50,000	Marshall	50,000
Cheatham	50,000	Maury	75,000
Chester	50,000	McMinn	50,000
Claiborne	50,000	McNairy	50,000
Clay	50,000	Meigs	50,000
Clinton	50,000	Monroe	50,000
Cocke	50,000	Montgomery	75,000
Coffee	50,000	Moore	50,000
Crockett	50,000	Morgan	50,000
Cumberland	50,000	Oak Ridge	50,000
Davidson	100,000	Obion	50,000
Decatur	50,000	Overton-Pickett	50,000
Dekalb	50,000	Perry	50,000
Dickson	50,000	Polk	50,000
Dyer	50,000	Putnam	50,000
Fayette	50,000	Rhea	50,000
Fentress	50,000	Roane	50,000
Franklin	50,000	Robertson	50,000
Gibson	50,000	Rutherford	75,000
Giles	50,000	Scott	50,000
Grainger	50,000	Sequatchie	50,000
Greene	50,000	Sevier	75,000
Grundy	50,000	Shelby	100,000
Hamblen	50,000	Smith	50,000
Hamilton	100,000	Stewart	50,000
Hancock	50,000	Sullivan	75,000
Hardeman	50,000	Sumner	75,000
Hardin	50,000	Tipton	50,000
Hawkins	50,000	Trousdale	50,000
Haywood	50,000	Unicoi	50,000
Henderson	50,000	Union	50,000

Henry	50,000		Van Buren	50,000
Hickman	50,000		Warren	50,000
Houston	50,000		Washington	75,000
Humphreys	50,000		Wayne	50,000
Jackson	50,000		Weakley	50,000
Jefferson	50,000		White	50,000
Johnson	50,000		Williamson	75,000
Kingsport	50,000		Wilson	75,000
				5,500,000