TN Department of Commerce & Insurance | Tennessee Emergency Communications Board

Connections

A Newsletter from the TECB

Volume 2 | Number 1
Spring 2023

On behalf of the Tennessee Emergency Communications Board ("TECB"), I want to personally express my gratitude to all of those that attended the recent town hall meetings. We appreciate your presence and active participation. Your insightful questions, comments, and feedback are crucial to shaping the TECB's mission and the decisions that it will make in the future. We hope that you found the meetings informative and valuable. If you were unable to attend any of the town halls, you can view the Nashville meeting here.

The TECB is committed to serving Tennessee's Emergency Communications Districts and we appreciate your willingness to collaborate for the betterment of 9-1-1 in Tennessee.

Curtis Sutton, *Executive Director*

ASTORS AWARD

L-R: Hon. Blake Lay, David Crews, Benjamin Glover, Steve Martini, Brad Anders, Greg Cothron. Not pictured: Jennifer White, Mark Archer, Phillip Noel, and Executive Director Curtis Sutton.

The Tennessee Emergency Communications Board (TECB) is pleased to announce that the Tennessee Statewide Cybersecurity Assessments and Penetration Testing Program was selected for the 2022 "ASTORS" Homeland Security Awards Program.

The ASTORS awards recognize "industry leaders of Physical and Border Security, Cybersecurity, Emergency Preparedness – Management and Response, Law Enforcement, First Responders, as well as federal, state, and municipal government agencies in the acknowledgment of their outstanding efforts to keep our nation secure."

In the wake of several cybersecurity attacks that targeted government entities, TECB partnered with Mission Critical Partners (MCP) on a new project focused on assessing the cybersecurity status of the state's 142 public safety answering points (PSAPs). A total of 139 assessments were completed across the state. The assessments gave greater visibility into Tennessee's 911 infrastructure and provided PSAPs with an understanding of their baseline status and increased awareness of vulnerabilities. For more information on the award, click here.

GEOGRAPHIC INFORMATION SYSTEMS (GIS)

Emergency service boundaries are important for i3 functionality. Three boundaries (Law, Fire, and EMS) have been deemed necessary in order to cut over to an i3 implementation. Now is the time to start reviewing the service boundaries you have for geometry and attribute fitness. These boundaries should match the external boundaries of your Emergency Service Number (ESN) polygons to ensure a seamless fit when integrated into the statewide composite. Section 4 of the GIS Data Standards for NG9-1-1 also addresses the attribution and naming conventions when submitting to the True North spatial interface.

If you have questions or need assistance creating or modifying your service boundaries, please contact True North Support at support@tngeo.com or James Wood at jameswood@missioncriticalpartners.com.

As a reminder, you should be receiving error report e-mails from True North regardless of whether there are errors. If you are not receiving these e-mails at least twice a week, please contact True North Support at support@tngeo.com.

Continued on Page 2

I'VE REQUESTED TEXT-TO-911 SERVICES. WHAT'S NEXT?

The Tennessee Emergency Communications Board (TECB) has set a deadline of June 30, 2023 to have all emergency communications districts (ECDs or districts) provide Text-to-911 service statewide, or risk delayed receipt of up to 50% of state-provided funding until the service is implemented. Any district that is not live with Text-to-911 today needs to prepare quickly and get on the testing schedule.

Text-to-911 can be delivered to the public safety answering point (PSAP) in different ways — over-the-top (internet) or over the Emergency Services IP Network (ESInet) connection provided by AT&T. The best and preferred way is over the ESInet, but many call-handling systems are not capable of this method, so internet-based delivery will be required. Districts must work with TECB to better understand their target solution as soon as possible so that proper planning and scheduling can occur.

The process to deploy Text-to-911 is fairly straightforward. Once a district has requested the service, AT&T will file the necessary paperwork with Intrado for deployment of the service. Intrado is the text control center provider for AT&T. When ready, a Intrado project manager will reach out to the PSAP/ECDfor a project kickoff call and to begin gathering data. Several questions about the call-handling system will need to be answered, so the provider should be brought into the discussions. Eventually, a test date will be scheduled, and all parties will be asked to participate until testing is successfully completed. Given the approaching deadline and the demand for resourcing, it may take up to a few months to complete this process; however, once complete the PSAP is considered "text ready." At this stage of the deployment, the ECD/PSAP will need to register with the FCC and send a Request for Service (RFS) letter to the wireless carriers that provide service within their jurisdiction. Intrado and TECB have a list of contacts at each carrier, as well as a template RFS document that can be used. The carriers will schedule testing, then work with the ECD/PSAP to negotiate a go-live date. Given the process with the carriers could take an additional couple of months to complete, districts are urged to begin the process as soon as possible.

Do I need to hire additional staff, and how much training is needed?

The overwhelming consensus within the industry is that Text-to-911 really isn't as popular as once expected. The public tends to call 911, rather than text, so as a result, PSAPs typically find very little text traffic to process. Even the largest PSAPs within the state of Tennessee only receive a couple of texts per day on average, while the smallest may only receive a couple per year.

Nonetheless, training is necessary, and operational procedures should be documented to account for situations like texter not responding, when to dispatch or not dispatch to a location, when to apply a mental health response, how to handle texts in different languages, etc.

For any training-related questions, ECDs should reach out to the TECB training coordinator Jennifer Schwendimann to discuss. She can be reached via email here.

WEARABLE PERSONAL SAFETY DEVICES

A number of body-worn personal safety products, or 911 panic buttons, exist that enable the user to summon help in a variety of ways. When first introduced to the public, these tools were initially marketed to elderly users as a means to provide safety in their homes. Accessibility to emergency responses permits the elderly continued independence and the ability to remain in their homes rather than be moved to assisted living or other options.

In recent years, wearable technologies have expanded marketing to address workplace safety concerns and provide coverage options for those working in isolated conditions or even in teaching and medical professions. The early options—pendants, wristbands, and panic buttons—have been extended to numerous other solutions.

Applications compatible with smart watches and phones come in a variety of cost options, making them accessible to anyone. The increasing impact of that availability is being felt across the 911 industry with each new wearable technology that enters the market. Wearable technology has configuration capabilities that permit specific recipients to be notified based on the user's preference, such as parental notifications from children arriving home from school. Unfortunately, many users utilize the default 911 notification when better-suited recipients may have been identified. And why not? 911 is always there! This complicates the 911 environment by delivering activations that may not require an emergency response and taxing already strained staffing resources.

A solution to this issue is a robust public education program. Whether education comes from the vendor directly to the user or from local 911 authorities, education is the key component. Recommendations for public education options include:

- Targeted outreach via school systems for school-age users and parents
- Senior outreach programs to assisted and senior living communities
- Use of social media
- Local government websites
- Regular public community meetings
- A brief mention on municipal mailings, such as utility or tax bills, that would provide an option for public education

Ultimately, technology will continue to expand, impacting the 911 ecosystem, and requires informing users about the impact of their wearable technology on local resources, to help ensure awareness and responsible usage of these lifesaving tools.

Continued on Page 3

WHAT IS PHISHING?

Phishing is a form of social engineering in which a malicious person (aka "bad actor") poses as a trustworthy colleague or organization to lure a victim into providing sensitive information, money, or access to a computer network. The lures typically come in the form of an email, but they can also occur via text message or even a phone call. When successful, this technique could result in a data breach, loss of service, identity fraud, malware infection, or ransomware.

How is phishing different from spam?

Phishing is targeted at a person or organization, whereas spam is blindly sent to a list of email addresses or phone numbers. Both can have the same result, but spam is much easier to recognize and block with spam filtering products due to the volume and consistent format of the messages received. Phishing is usually a single email or text message appearing to be from a trustworthy source to a small number of recipients.

What should I look for; how would I know if I received a phishing message?

First of all, never provide any personal information like credit cards, Social Security numbers, or passwords to anyone over email or text. Second, always be wary of clicking any links or opening attachments in email—first make sure the person that sent it to you is legitimate. If you receive a text message or phone call that seems suspect, or an urgent request to wire-transfer money, be sure to call and talk with the person they claim to be or confirm their legitimacy with colleagues or management before engaging in conversation or opening links that may have been sent.

The most common way that phishing attacks are carried out is over email, so this is where people should be the most vigilant.

Usually, the bad actors will create an email address that looks similar to a legitimate email address; therefore, before opening any attachments or clicking links, people should first look closely at the email address itself, not just the first and last name. By inspecting the full email address, you may be able to spot a difference with the real/correct address (e.g., .net instead of .com, a zero instead of the letter O, j instead of i, n instead of m, etc.). Also note that phishing messages typically have a subject that entices the user into opening the email, so look out for keywords like "important," "bonus," "layoffs," "corporate reorganization," etc.

Remember, phishing is a social engineering technique, so attackers will try different methods with different people until they're successful. They may be very direct and request the victim open a link or attachment, or they may start with an innocent conversation, without links or attachments. They often include something personal so as to seem authentic, perhaps something they found on social media about the victim or whoever they're impersonating. However the attack is delivered, the victim will eventually receive a link or attachment to open, and if/when they do, the organization will suffer the consequences.

The Cybersecurity and Infrastructure Security Administration (CISA) collected data from phishing assessments it has executed. Here are some interesting statistics:

- 80% of organizations had at least one person fall victim to a phishing attempt by CISA's assessment team.
- 70% of all attached files or links were not blocked by network protection services.
- 84% of people receiving a malicious email either replied with personal information or opened a malicious attach ment or link. (And they did so within the first 10 minutes of receiving the message.)
- Only 13% of targeted employees reported the phishing attempts.

STAY IN TOUCH WITH TECB!

TN Department of Commerce & Insurance | Tennessee Emergency Communications Board

500 James Robertson Parkway | Nashville, Tennessee 37243
tn.gov/commerce/emergency-communications

/TennesseeCommerceAndInsurance
/TNCommerceInsur
@tncommerceinsur
@TDCI