2022 Arkansas School Safety Commission

Final Report

October 1, 2022

UofA
UNIVERSITY OF ARKANSAS SYSTEM
CRIMINAL JUSTICE INSTITUTE

September 30, 2022

Dear Governor Hutchinson:

On behalf of the 2022 Arkansas School Safety Commission, I am honored to present you with our final report. Thank you for your continual passion for the children of Arkansas and for allowing us the opportunity to contribute to your vision of making Arkansas's schools safer.

We are very grateful to all the individuals who presented to the Commission. A very special thank you is extended to the students and parents who provided us with their invaluable testimony. We heard you and your perspectives were instrumental in the framing and completion of many recommendations included within this report.

The work of this Commission could not have been possible without the support of Speaker Sheppard and Secretary Johnny Key. A very special thank you is extended to Ms. Angela Scaife from the Arkansas Department of Education. Her hard work and dedication are tremendously appreciated and were instrumental in helping us to meet your expectations.

I am tremendously grateful for the exceptional work of my fellow Commission members. Their commitment and passion for the safety of our children is remarkable and unmatched. I am humbled to have had the privilege to work alongside them.

It is our intent that this report will assist you in fulfilling your vision of keeping our children safe and providing them with the opportunity to reach their full academic potential. Thank you, as always, for your extraordinary leadership and the opportunity to serve you.

Sincerely,

Dr. Cheryl P. May
Chair
2022 Arkansas School Safety Commission

26 Corporate Hill Drive, Little Rock, AR 72205-4538 / (501) 570-8000 / (501) 565-3081 Fax / www.cji.edu

Table of Contents

Introduction

On March 1, 2018, Governor Asa Hutchinson, in the wake of the horrific school shooting at Marjory Stoneman Douglas High School in Parkland, Florida (February 14, 2018 with 14 students and three staff murdered and 17 others wounded), signed an executive order forming the Arkansas School Safety Commission (Commission). Governor Hutchinson's 2018 Proclamation is presented in Appendix A. The 18 members that served on the original Commission are provided in Appendix B. Governor Hutchinson appointed Dr. Cheryl May, Director of the University of Arkansas System's Criminal Justice Institute (CJI), as Chair of the Commission.

As required, the Commission provided Governor Hutchinson with a final report which included 30 recommendations (best practices) on November 30, 2018. A list of the original 30 recommendations of the Commission is presented in Appendix C.

On May 24, 2022, an attacker entered the Robb Elementary School in Uvalde, Texas and murdered 21, including nineteen nine, ten and eleven-year-old students and two veteran teachers, and injured as many as 17 others. To complete the critical task of preventing Arkansas schools from experiencing tragic events such as the one that occurred in Uvalde, on June 10, 2022, Governor Hutchinson signed an executive order (see Appendix D) to reconvene the Arkansas School Safety Commission (2022 Commission) and appointed 24 individuals to serve as members. A list of the 2022 Commission members along with their subcommittee assignments is presented in Appendix E.

The 2022 Commission is tasked with the following duties:

1) Review the Commission's Final Report published in November 2018;
2) Provide an update on the status of school safety across Arkansas;
3) Update the analysis of the safety of K-12 schools throughout the state taking into consideration the physical and mental health of students;
4) Determine which findings and recommendations from the previous report have not been remediated and achieved;
5) Identify any new recommendations of best practices in school safety that have been developed since the Commission's final report in November 2018;
6) Submit an initial report and recommendations to The Governor on August 1, 2022 and
7) Submit the final report of the Commission's findings and recommendations to the Governor no later than October 1, 2022.

As 2022 members of the Arkansas School Safety Commission, we are tremendously grateful for Governor Hutchinson's leadership and his continuous passion, commitment, and dedication to making sure all of Arkansas's students are in safe and secure environments and given the opportunity to reach their true academic potential. We are grateful for the opportunity to contribute to fulfilling his vision.

As Arkansans, we continue to be mindful of the profound pain and loss we experienced as a result of school shootings in our state. Since 1997, we have lost 6 students and one teacher and 13 students, teachers or staff have been wounded. In addition to Stamps High School (1997; 2 wounded) and Westside Consolidated Middle School near Jonesboro (5 fatalities and 10 wounded), three other school shootings have occurred, all since the Commission completed its work in November of 2018. On April 1, 2019 a 14-year-old eighth-grade student at Prescott High School shot and injured a 14-year-old fellow eighth grader. On April 24, 2019 a 14-year-old student at Concord High School shot himself and ended his own life in a restroom adjacent to the school cafeteria. On March 1, 2021 a 15-year-old student, in a premeditated attack, shot and killed a fellow 15-year-old classmate at Watson Chapel Junior High School. Our state's history of school violence and the heinous shootings at Robb Elementary School, Sandy Hook Elementary School, Columbine High School, Marjory Stoneman Douglas High School, Santa Fe High School and unfortunately many others, illustrate the real vulnerability of our children in schools.

As members of the 2022 Commission, we are committed to working tirelessly to honor the victims of these tragedies and improve the recommendations of the original Commission to further help Arkansas schools develop school safety strategies to prevent, mitigate, respond to and recover from events of violence.

As required, the 2022 Arkansas School Safety Commission Interim Report was submitted to Governor Hutchinson on July 29, 2022.

This report will present the progress which has been made in implementing the 2018 School Safety Commission recommendations and present the new 2022 Commission recommendations. As in the 2018 Commission Final Report, the order of presentation does not represent or reflect any priority as to the importance of the recommendations of one over another. Each of the recommendations are equally important in helping to ensure the safety and security of our school students, staff and teachers. There is not one solution that if implemented alone will end the potential of violence in our schools. Comprehensive school safety strategies that emphasize prevention, protection, mitigation, response and recovery should be implemented!

While this report provides school safety best practices for school districts, the 2022 Commission was very mindful of the potential implementation cost that could be incurred

by districts. In order to reduce the cost, a concerted effort was made to provide many free high-quality resources that districts can use to implement the Arkansas School Safety Commission recommendations.

We applaud the superintendents, staff and teachers for their efforts to make Arkansas schools safe learning environments free of violence. Unfortunately, because we are living in unprecedented times, we must ask them to do even more. Their commitment and dedication to our children are sincerely appreciated.

2022 Arkansas School Safety Commission Activities

The inaugural meeting of the 2022 Arkansas School Safety Commission was held on June 14, 2022, in Room 151 at the Arkansas State Capitol. We are grateful to Speaker Sheppard and his staff for their extraordinary support that allowed Commission meetings to be live-streamed so our discussions can be seen by the public. We are also tremendously appreciative of Secretary Key and his staff for their relentless support of our activities. We are grateful to DESE staff who provided public access to our discussions through the live streaming of full Commission meetings. A very special thank you is given to Ms. Angela Scaife for her continuous extraordinary support of our efforts.

During the 2022 Commission's initial meeting, Chair May organized members in to the five original subcommittees and assigned the following individuals as chairs of each subcommittee:

- **Ms. Lori Poston:** *Mental Health and Prevention*
- **Secretary A.J. Gary:** *Audits, Emergency Operation Plans and Drills*
- **Sheriff Tim Helder:** *Law Enforcement and Security*
- **Chief Chris Chapmond:** *Intelligence and Communications*
- **Director Tim Cain:** *Physical Securities*

Please refer to Appendix E for a list of members assigned to each subcommittee. In addition, Chair May invited several subject matter experts (SMEs) to assist Commission members in their subcommittee work. SMEs bring additional valuable knowledge and experience to each subcommittee. While non-voting members, SMEs have made valuable contributions to our discussions. We are tremendously grateful for their time and input. A list of SMEs is also provided in Appendix E.

Full Commission meetings have been held on June 14th, June 21st, June 28th, July 5th, July 12th, July 19th, July 26th, August 9th, August 16th, August 30th, September 6th, September 13th, September 21st, and September 27th. All subcommittees have met regularly on the Wednesday, Thursday or Friday following each full 2022 Commission meeting. During full Commission meetings, presentations were provided by key stakeholders to demonstrate the

significant progress made and/or identify free school safety resources available to school districts. A list of the presenters are provided in Appendix F. We are especially grateful to the three students (Mr. N'nambi Islam, Little Rock Southwest Magnet High School, Ms. Mary Emily Wrzensinski, Hamburg High School, and Mr. Webb Storer, Jonesboro High School) who spoke with us on July 19th. We are also very grateful to the four parents who spoke with us on August 30th (Ms. Dee Blackwell, Fort Smith School District, Ms. Elizabeth Vazquez-Rodriguez, Stuttgart School District, Mr. Scot Erwin, Perryville School District, and Ms. Charlene Kirk, Little Rock School District). We are very grateful to each of them for their open and honest dialogue. We heard you!

We are particularly grateful to the Investigative Committee on the Robb Elementary Shooting of the Texas House of Representatives and their release of the Interim Report 2022. This report provides an accurate account of the tragedy at Robb Elementary School on May 24, 2022. We applaud their work and release of this important candid report and vow the information shared will be used to better ensure the safety and security of school students in Arkansas. This report will be referenced repeatedly in the presentation of 2022 Commission recommendations.

As with the original 2018 Arkansas School Safety Commission, we further emphasize the importance that all school districts, regardless of size, implement **Comprehensive** school safety strategies and ensure the layering of these actions, policies, and procedures. There is not one solution that if implemented alone, will end the potential of violence in our schools. As indicated in the Robb Elementary Shooting Report numerous systemic failures at the school and in the actions of the responding law enforcement personnel contributed to the school's lack of preparation for and response to a potential armed attacker on campus. While the school had many of the right school safety policies and procedures in place, a culture of non- compliance contributed to a "relaxed vigilance on campus". While Arkansas has passed numerous school safety laws since the 2018 Commission report, we must make sure there is accountability at the state, district, school, and staff levels to ensure our schools are vigilant in following these laws and their established safety and security policies and procedures. The Robb Elementary Shooting Report clearly demonstrates that if we do not insist on this accountability, the lives of our students are at risk.

Since the conclusion of the work of the 2018 Commission, two critical articles concerning school shooters have been published by the U.S. Secret Service National Threat Assessment Center (NTAC). **Both studies indicate that school shootings are preventable.** The information provided in these studies were critical in guiding the development and use of policies, procedures, tools, and programs to best ensure the safety of our schools. In 2019, NTAC published their research on targeted school violence[1] and closely examined 41

[1] https://www.secretservice.gov/sites/default/files/2020-04/Protecting_Americas_Schools.pdf

incidents in K-12 schools that occurred between 2008-2017.
Key information from this report is provided below:

- No clear profile of a school attacker
- Most were current or former students.
- More than 80% were males.
- Most were 7th graders to seniors in high schools.
- Many were absent from school before the attack and some were suspended.
- Many were treated poorly by peers in-person and not just online; badly bullied.
- They were grieved in some way.
- Some sought fame.
- Others were suicidal.
- Had a history of discipline issues.
- Had negative home life factors.
- Had prior contact with law enforcement.
- Their behaviors concerned others but was not reported.

In 2021, the National Threat Assessment Center (NTAC) published their research on 67 averted attacks[2]. Striking similarities can be seen between school attackers and students who plotted attacks. According to NTAC, these include:

- Both had histories of contact with law enforcement and of school discipline.
- Both had mental health issues (such as harming themselves and depression) and were bullied.
- Intended or committed suicide.
- Both used drugs or alcohol.
- Both were impacted by negative factors at home, such as parent's substance abuse, domestic violence, child abuse, parental incarceration or parental mental health issues.

Because of the importance of the report's key findings and implications, they are being listed verbatim below.

❖ **"Targeted school violence is preventable when communities identify warning signs and intervene.** In every case, tragedy was averted by members of the community coming forward when they observed behaviors that elicited concerns."

❖ **"Schools should seek to intervene with students before their behavior warrants legal consequences.** The primary function of a threat assessment is not criminal

[2] https://www.secretservice.gov/sites/default/files/reports/2021-03/USSS%20Averting%20Targeted%20School%20Violence.2021.03.pdf

investigation or conviction. Communities should strive to identify and intervene with students in distress *before* their behavior escalates to criminal actions."

- **"Students were most often motivated to plan a school attack because of a grievance with classmates.** Like students who perpetrated school attacks, the plotters in this study were most frequently motivated by interpersonal conflicts with classmates, highlighting a need for student interventions and de-escalation programs targeting such issues."

- **"Students are best positioned to identify and report concerning behaviors displayed by their classmates.** In this study, communication made about the attack plot were most often observed by the plotter's friends, classmates, and peers. Schools and communities must take tangible steps to facilitate student reporting when classmates observe threatening or concerning behaviors. Unfortunately, many cases also involved students observing concerning behaviors and communications *without* reporting them, highlighting the ongoing need for further resources and training for students."

It should also be noted that in almost one-third of the cases (21/67), a SRO played a role in disrupting the attack plot.

Status of School Safety in Arkansas

This section of the report will focus on the significant progress made in the implementation of the 30 recommendations of the 2018 Arkansas School Safety Commission. While this progress will be listed by Commission subcommittee topics, there have been significant accomplishments that do not fit neatly under a single recommendation or even under a topic. These notable accomplishments will be described below.

In 2017, The Arkansas Center for School Safety (the Center) was formed under the umbrella of the University of Arkansas System's Criminal Justice Institute (CJI) through a Memorandum of Understanding executed by Commissioner Johnny Key and Dr. Cheryl May. The Center was established to build the capacity of educators, leaders, and law enforcement professionals to meet the safety needs of children in public schools in Arkansas. Funding for the Center included federal and state grants as well as one-time monies from Governor Asa Hutchinson and Arkansas Attorney General Leslie Rutledge. In addition, the Center promotes and supports school safety statewide through training, education and resources for school district and law enforcement personnel. During the 92nd General Assembly of 2019, thanks to the support of Governor Hutchinson and the Arkansas legislature, CJI received base funding for the Arkansas Center for School Safety. Acts 620 and 648 of 2021 identified the Center as the state school safety clearing house, expanded access to private schools and established a 16-member advisory board,

including 8 Governor-appointed members. Dr. Cheryl May, Director of CJI and the Center, provided a presentation to the 2022 Commission about the training and resources available through the Center on June 21, 2022. A copy of Dr. May's presentation, as well as all presentations to the Commission and subcommittees, are provided in Appendix G.

In 2019, Governor Hutchinson requested the Arkansas Center for School Safety (the Center) work with the Arkansas Division of Elementary and Secondary Education (DESE) and other key stakeholders to develop the 2019 School Safety Assessment and determine how well school districts have done in implementing the Commission's initial 30 recommendations.

The Center contracted with UA Little Rock's Survey Research Center to administer the 106- question survey developed. An incredible 97% response rate was achieved. The results of the 2019 School Safety Assessment will be presented throughout this report.

The results of the 2019 School Safety Assessment were used to identify key implementation gaps and the foundation upon which proposed legislation was written and passed. The school safety legislation passed in 2019 and 2021 are detailed in Appendix H. We are very appreciative of DESE's Safe Schools Committee and their efforts in assisting with the framing of many of these pieces of legislation.

In order to get a more accurate picture of the status of school safety in Arkansas, a 99-question survey was developed by the 2022 Arkansas School Safety Commission and again funded by the Arkansas Center for School Safety and administered by UA-Little Rock's Survey Research Center. The results of the 2022 School Safety Assessment prompted the development of several new recommendations included in this report.

Mental Health and Prevention Progress

As stated in the 2018 School Safety Commission Report, prevention efforts are critical in reducing the prevalence of school violence. These include early identification of at-risk students and detection of emerging threats. In the following section, progress related to the previous Mental Health and Prevention recommendations of the Commission will be presented.

Recommendation 1: Every school district should conduct school climate surveys across all campuses, and develop and implement an action plan based on the findings of the school climate survey.

Based on the 2019 School Safety Assessment, 60% of responding schools reported utilizing a School Climate Survey to assess their strengths and vulnerabilities, and to improve their awareness of potential risk factors related to bullying or other issues that negatively impact school climate. A positive school climate includes strong and caring relationships, physical and emotional safety from violence, bullying and substance misuse, and consistent and fair disciplinary policies. A thorough assessment of school climate in each building, with subsequent action planning by the building administration and other pertinent staff members, is highly recommended to ensure the identification of problem areas, and planning to address any identified issues is completed in a timely and an effective manner.

As a result of a state-wide climate survey roll-out by the Arkansas Division of Elementary and Secondary Education (DESE), 63% of school districts chose to use the High Reliability Schools Level 1 survey beginning in 2019. Data were not readily available for alternative platforms used for school climate surveys or implementation of action plans. In the 2022 School Safety Assessment, however, only 104 districts indicated they conducted a climate survey in the last 3 years and only 47 identified High Reliability Schools as the instrument they used.

Acts 620 and 648 of 2021 mandate that school site safety assessments are conducted by school districts every three years, the first no later than August 1, 2024. Conducting climate surveys are now included as part of the required comprehensive school safety assessment process.

Recommendation 2: All school districts should implement a positive climate program that deters bullying behaviors, and promotes social-emotional learning and positive peer relationships.

In the 2019 School Safety Assessment, 60% of schools identified that they utilize a specific Social-Emotional Learning curriculum in their districts. Arkansas has historically ranked near the top in the nation in regard to the prevalence of bullying in our schools. Creating a culture in schools where positive peer relationships are taught and reinforced is a crucial piece of addressing bullying and other harmful behavior in our schools.

The Arkansas Division of Elementary and Secondary Education (DESE) and others have developed innovations that support the work of implementing a positive climate program in schools. A summary of several key positive climate programs are provided below.

G.U.I.D.E. for Life (Growth, Understanding, Interaction, Decisions, and Empathy)

This program is the work of 96 educators, representing 44 districts across the state. G.U.I.D.E. for Life serves as social/emotional learning standards, guiding instruction as academic standards have shaped core instruction. Counselors and educators can provide K-12 students with a five-step process to ensure personal success. The five-step process includes:

1) Growth: (Manage Yourself)
    a) Develop problem-solving skills.
    b) Practice mindfulness.
    c) Persevere.
2) Understanding: (Know Yourself)
    a) Increase self-awareness.
    b) Know your strengths and weaknesses.
    c) Develop critical thinking skills.
3) Interaction: (Build Relationships)
    a) Treat others with respect.
    b) Communicate effectively.
    c) Seek out and offer help when needed.
4) Decisions: (Make Responsible Choices)
    a) Consider personal beliefs, safety, and the situation.
    b) Think through potential consequences.
    c) Put your best self forward.
5) Empathy: (Be Aware of Others)
    a) See other perspectives.
    b) Value the feelings of others.

c) Appreciate diversity.

The Guide for Life Program provides a free social/emotional learning curriculum for K-12 Arkansas schools. While thirty-three districts use some or all components of the curriculum, all school counselors have been trained for use with students. A monthly newsletter is sent to approximately 1300 counselors with a Guide for Life section highlighting social/emotional learning and podcast topics. Additional training is available upon the request of a school or district. Plans for future impact include helping districts with integrating social/emotional learning into the core curriculum.

THRIVE Arkansas

The Division of Elementary and Secondary Education's THRIVE Arkansas is a collaborative project funded through the American Rescue Plan to support districts while developing and sustaining a multi-tiered support system to assess behavioral and mental health needs across a school and create systems to support all students.

The project goals are as follows:

1. To increase coordination of efforts that support behavior and mental health services and programs.

2. Increase capacity in developing and sustaining evidence-based multi-tiered systems of support that address behaviors through a system of positive behavioral supports.

3. Develop the infrastructure that will best support the needs of the whole child.

In 2021, Act 1084 supported schools in utilizing "evidence-based positive behavior supports." THRIVE Arkansas launched in June of 2022, focused on providing training and support to schools in implementing school-wide positive behavior supports. In July 2022, the first cohort was trained, consisting of 93 schools representing 53 districts from across the state. The initial target group is district leadership. As part of the development process, they will be charged to return to their districts and create the district-wide framework, including building-level leadership teams for further implementation. THRIVE Arkansas is funded with American Rescue Plan funds and is currently funded through 2024. Two additional cohort training sessions will begin in January 2023. The additional cohorts could potentially impact 200 more schools. Subsequent training will need to take place to build capacity in teachers, counselors, and support staff.

Project A.W.A.R.E (Advancing Wellness and Resiliency in Education)

Project A.W.A.R.E. is a project which supports school districts in efforts to provide mental health care awareness and trauma-informed practices (funded through the Substance Abuse and Mental Health Services Administration (SAMHSA) AWARE State Education Agency Grant).

The project goals are as follows:

1. To increase coordinated referrals, mental health services and programs, and follow-up for children.

2. Increase outreach and engagement among youth, families, schools, and communities to increase awareness, mental health identification, and implementation of services and programs.

3. Develop the infrastructure that sustains mental health among youth and maintain mental and behavioral health services when federal funding ends.

Some of the components of AWARE are:

- Provided Mini-Grants to districts to directly support Mental Health
- Promoting the use of the SHAPE Assessment (School Mental Health Assessment)
- Arkansas Aware Podcast

Project AWARE is funded by a 5-year SAMHSA grant, and is presently in year 4. Just prior to the completion of this report, DESE was notified Project AWARE was funded for another 5 years. Almost 250 trainings have been conducted with school personnel, community members, and others including Mental Health First Aid, trauma and resilience, adverse childhood experiences (ACEs), and teacher wellbeing. 48 new Mental Health First Aid trainers were added this past year, increasing the total number of trainers to over 150 across the state.

There have been 88 Arkansas AWARE Podcast episodes produced. They are free and available to anyone in an effort to spread the project's impact and improve mental health support for children in Arkansas and beyond. This gives teachers and others easy access to information to support their professional growth, offer support, and covers topics relevant to mental health.

Since 2019, Arkansas AWARE has awarded 69 mini-grants to schools across the state to help equip them to better meet the mental health needs of their students.

Trauma Resource Initiative for Schools (TRIS)

The UAMS Trauma Resource Initiative for Schools (TRIS) partners closely with DESE to offer trauma awareness and trauma-informed care training for school staff. These trainings focus on the prevalence of childhood trauma, its impacts on child development/school success, and steps school staff can take to create a school environment in which children with experiences of trauma are more likely to succeed. Funded by a 3-year grant from the Blue & You Foundation, the TRIS trained more than 2,500 teachers and other school staff in the first grant year (2021-2022).

TRIS utilizes the best-practice framework disseminated by the National Child Traumatic Stress Network (NCTSN), called the *NCTSN System Framework for Trauma-Informed Schools*. According to the NCTSN, a trauma-informed (TI) school system is one in which all members of the school community are equipped to recognize and respond to the impact of trauma on students and others in the school system, understanding that trauma impacts emotions, behavior and the ability to succeed academically. The framework is rooted in a multi-tiered approach for the early identification and support of students with learning and emotional/behavior needs related to trauma. Within each of these tiers are trauma-informed practices and strategies designed to create a trauma-informed learning environment, build skills in students that support resilience, support staff well-being and reduce secondary trauma, enhance partnerships with families, strengthen organizational policies and procedures, and address needed community partnerships.

Recommendation 3: All school districts should provide access to training in Youth Mental Health First Aid for all personnel who interact with students. Additional school personnel training may include: Adverse Childhood Experiences (ACEs), Trauma-Informed Schools, Drug-Endangered Children, and Social-Emotional Learning.

In response to this recommendation, there have been some significant progress made in Arkansas:

- Act 551 and 622 of 2021 requires all school resource officers to complete YMHFA training every four years.
- Act 620 and 648 of 2021 requires all school counselors to complete YMHFA training every four years.
- To date, the Arkansas Center for School Safety staff has trained 756 SROs and school counselors.
- DESE's Project AWARE has trained over 2,500 educators, counselors, and community members in YMHFA

The 2022 Commission heard from administrators from Greenbrier School District about the impact of Youth Mental Health First Aid in their district. They are determined to go beyond the requirements from Acts 620 and 648 of 2021 and train other staff. They have two certified YMHFA trainers within the district. Below please find comments from Dr. Benish, Director of Mental Health Services & Behavioral Services for the Greenbrier School District:

Positive mental health and well-being is associated with increased academic success, better attendance rates, positive relationships, good problem-solving skills, and overall resilience just to name a few. But many of our students need help developing and maintaining a healthy mindset. School is naturally a good location for mental health support because our children and youth spend a majority of their time there. Many mental health difficulties begin during the school ages. From research we know that the onset of about half of all diagnosable mental illness occurs before adulthood with about a third occurring before the age of 14. Positive mental health is the foundation for learning in many cases. In Greenbrier, we are committed to making a difference by implementing a comprehensive system of mental health support in our schools. Our children come first and we are committed to educating and supporting the whole child academically, behaviorally, socially and emotionally.

Our goal is to develop and maintain a comprehensive system of support that includes early identification and makes school based mental health services easier to access for our families and youth in Greenbrier. Education and awareness of mental health difficulties are vital to the process. With programs like Youth Mental Health First Aid (YMHFA), we are providing that knowledge and equipping adults with the skills they need to recognize the signs and symptoms of mental health difficulties early on. With this program, our staff learn about warning signs of mental illness and substance abuse. They become familiar with common mental health disorders and learn how to intervene to get youth the help they need both as symptoms arise and in crisis situations.

Educating our staff with Youth Mental Health First Aid has a broad impact. We are dispelling myths about mental illness and reducing the stigma associated with it. Our staff commonly report feeling increased confidence to intervene and better knowing how to help our young people after receiving the training.

Since 2019, we have acquired trainer certification for two counselors, two directors and one intern who have conducted about 20 trainings in the district. We have trained approximately 395 participants, both school staff and community members who fill various roles in a young person's life including teachers, administrators, counselors, resource officers, bus drivers, custodians, computer technicians, school board members, parents, youth pastors, and administrative staff. It is our goal that all staff who work with children and youth receive training in this very important program and we are very close to reaching

that goal.

– *Dr. Tricia Benish*
Licensed Psychologist
Director of Mental Health & Behavior Services,
Greenbrier School District

CJI's Maltreatment and Drug Endangered Children Initiative

According to the National Threat Assessment Center reports, both school attackers and students who plotted attacks were impacted by negative factors at home such as a parent's substance abuse, domestic violence, child abuse and parental incarceration. According to the Investigative Committee of the Robb Elementary Shooting, the parent of the Uvalde attacker was struggling with a substance use disorder. The Maltreatment and Drug Endangered Children Initiative of the Criminal Justice Institute (CJI)focuses on the early identification of children who are maltreated. A very large percentage of these children live in homes where parents are engaged in illicit drug activities including substance abuse. These children are referred to as drug endangered children and are most commonly neglected, but are also at-risk of physical and sexual abuse. According to the Children's Bureau, 73% of children who died from maltreatment suffered neglect. Early identification of children at risk of maltreatment in this initiative are identified through collaboration between local and county law enforcement, child welfare workers, community correction professionals and schools. Through information sharing between law enforcement and child welfare, histories of domestic violence and substance abuse, which often go undiscovered, can be identified. Once at-risk children are identified, children and families are provided opportunities for needed services. The ultimate goal of this initiative is to the break the cycle of child and drug abuse in these families through early intervention. Local and county law enforcement, Arkansas Division of Children and Family Services, Arkansas Division of Community Correction and schools are the critical partners in this initiative. Currently this initiative has been implemented and successful in 7 counties.

One important element of the Maltreatment and Drug Endangered Children Initiative is the PAYcheck (Protecting Arkansas Youth) Program. Often times there are negative experiences in a student's life outside of school that can have an impact on their behavior at school and far too often the school is not aware of any of these events. The PAYcheck program is designed to increase the communication between local schools and local and county law enforcement, children and family services and community correction and reduce the trauma experienced by children in these homes. If a child's parent is arrested, for example, a notification is set to the school indicating the child has been traumatized. It does not provide the circumstances of the trauma. This notification alerts school

personnel and if the child acts out or has difficulty with completing assignments, they are brought to the attention of the school counselor rather than disciplined. In order to reduce the amount of trauma experienced by the student, and ensure they are not further traumatized in school, CJI will be working with DESE and UAMS to develop and deliver trauma informed response training for school and law enforcement professionals. Dr. Cheryl May has received support for statewide implementation of the PAYcheck program from DESE (Secretary Johnny Key), the Arkansas Division of Children and Family Services, the Arkansas Association of Chiefs of Police and the Arkansas Sheriff's Association. This voluntary program is on target to be launched in early 2023.

Recommendation 4: All school districts should establish a behavioral threat assessment team, following best practices for team composition and process and require all team members receive basic and advanced behavioral threat assessment training through the Arkansas Center for School Safety.

Since the releasee of the 2018 Commission report, the following have occurred:

- The Arkansas Center for School Safety (the Center) received a Bureau of Justice Assistance (BJA) Stop School Violence Grant in 2019 to provide Basic and Advanced Behavioral Threat Assessment (BTA) training, as well as an online basic threat assessment course, tool kit, and draft policy. The Center recently received notification of a 24-month no cost extension for this grant award.
- Basic BTA - 11 classes delivered (351 attendees) with 88 school districts participating.
- Advanced BTA - 2 class delivered (47 attendees) with 24 school districts participating.
- In 2019, 45% of school districts indicated they utilize an anonymous school safety reporting system.
- However, only 28% of school districts indicated having a behavioral threat assessment team. Of those who reported having a BTA team, 66% indicated that all team members completed training in at least basic behavioral threat assessment.

The Mental Health/Prevention subcommittee heard presentations from Fort Smith School District and Springdale School District regarding their anonymous tip lines and behavioral threat teams and processes.

Based on our review of the information from districts that have successfully created a mechanism for anonymous or confidential reporting of concerning situations or behaviors at school, all behavioral threat assessment teams must meet national best practices for team composition, processes and training.

Behavioral Threat Assessment Team training is currently available FREE to all schools through the Arkansas Center for School Safety. This training is best practice in Arkansas, and is necessary for all identified team members. The Commission heard a presentation from Cindy Marble, a former Special Agent with the Secret Service, regarding Behavioral Threat Assessments. She does extensive training nationally regarding assessing threats in schools. She shared the critical pieces of a thorough threat assessment, including identification and definition of the concerning behavior, to determine what causes may be there. This allows identification of needs and intervention prior to threats occurring, which is the best possible outcome. She shared specifics about a court case[3] in California involving a behavioral threat assessment process that was not conducted appropriately, which involved inadequate response to bullying. The school was found 54% liable, as the threat assessment process did not involve a team, nor was there any recommendation of services for the student.

Recommendation 5: The Arkansas Department of Education should review roles and responsibilities of school counselors to provide increased time with students for provision of counseling and social-emotional learning, as well as referral to community resources as appropriate.

Act 190 of 2019 mandated that all school counselors must spend 90% of their time in direct service to students. The Commission's intent behind this recommendation was to appropriately utilize time that counselors spend with students each day, to ensure the best use of their specific skills and training to benefit students in the schools they serve. We do recommend ongoing monitoring by school administration, to ensure the appropriate use of counselor time. This recommendation has been accomplished.

Recommendation 6: A coordinated crisis response team should be developed to mitigate the emotional impact of any traumatic event that impacts a district.

The 2018 Arkansas School Safety Commission recommended a designated process be implemented utilizing trained personnel from across the state to respond to critical incident events in an organized and efficient manner.

Thanks to a DESE 2019 BJA Stop School Violence grant, staff members from the Arkansas Division of Elementary and Secondary Education (DESE) and Arkansas Center for School Safety (the Center) have researched and reviewed crisis response training

[3] https://cases.justia.com/california/court-of-appeal/2022-f079926.pdf?ts=1648231252

models. DESE recently received notification of a 12-month no cost extension for this grant award. The National Organization for Victim Assistance (NOVA) was recently designated as the crisis response model which will be utilized to train teams who can provide critical education and emotional first aid training in mass casualty, natural disasters or other events which impact Arkansas schools and communities.

Law Enforcement and Security Progress

Recommendation 1: No campus should ever be without an armed presence "AT ALL TIMES" when staff and children are attending class or a major extracurricular activity.

While 84% of school districts indicated they have armed presence on all campuses in the 2019 School Safety Assessment, discussion pertaining to the accuracy of this survey question generated the need to clarify the definition of "campus". In 2018, the intent was to have armed security within each building, i.e. Elementary School, Middle School, Junior High School and High Schools. It is believed that school districts did not fully understand the intent of this question. As a result, a more descriptive question was included in the 2022 School Safety Assessment. With initial reports and anecdotal evidence, we believe that most school districts do not have an armed presence on every school campus. Either districts could not afford the cost of School Resource Officers (SROs) or Commissioned School Security Officers (CSSOs) or the district was opposed to arming additional personnel (SROs or CSSOs). In the 2019 School Safety Assessment, while 79% of districts indicated having at least one SRO, only 20% of the districts indicated they had an SRO on all campuses. In 2019, only 20 districts indicated that they have established CSSO programs. Compounding this issue further, if there is an armed presence, it is periodically interrupted due to the SRO (if only one) having responsibilities elsewhere in the district, or other responsibilities within the community that remove them from the school.

Recommendation 2: If financially practicable, schools should ideally have at least one SRO for each campus.

Progress Made. Based on data from the Arkansas Center for School Safety, there are now at least 460 SROs throughout the state, in 223 total school districts. The number of SROs has increased significantly since the initial survey conducted by the Commission (315). However, at the time of the initial school safety assessment, only 20% of districts indicated they had SROs on all campuses.

This recommendation dovetails with the first requiring armed security on every school campus within a district. Because this recommendation states, if financially practicable, the committee is signaling that this is an important goal, but it is not as crucial as having

some form of armed security in every school. Obviously having a school resource officer on a campus does provide armed security, but it also provides the campus with a valuable tool. When properly trained, a SRO can build bridges between students and the police that can be incredibly beneficial in helping to provide and increase the level of security for the school.

We recognize that a SRO can be a powerful mentor and role model for the students they serve. They can also play an important role when schools are training staff to recognize and react to security threats. If funding can be found, placing a SRO on every school campus is recommended.

Recommendation 3: School districts should execute a Memorandum of Understanding (MOU) with their partnering law-enforcement agencies that identify the roles and responsibilities of SROs and other critical elements.

Acts 551 and 622 of the 2021 regular session requires a school district that accepts a SRO to enter into a memorandum of understanding with the law enforcement agency having jurisdiction. The University of Arkansas System's Criminal Justice Institute and Arkansas Center for School Safety (the Center) in collaboration with other key stakeholders including DESE's Safe Schools Committee developed a model MOU that must be used by school districts when obtaining the services of a SRO from a local or county law enforcement agency. School districts that form an institutional police department must use this model MOU to develop mirroring policies and procedures for any officers on campus during the instructional day (SROs). A copy of the model SRO MOU can be found at www.arsafeschools.com.

Recommendation 4: SROs whose primary assignment is within the school should receive specialized training.

Acts 551 and 622 of 2021 also include training requirements for all SROs. These include, a 40-hour basic SRO course, Youth Mental Health First Aid certification every four years, a SRO refresher course every five years after completing the basic SRO course and 12 hours of continuing education in school safety annually. In addition, superintendents and administrators with direct supervision responsibilities of a SRO must take a course on SRO roles and responsibilities. The Arkansas Center for School Safety (the Center) provides all needed courses (in-person and online) for SROs or administrators (www.arsafeschools.com) to meet these requirements. The Center is responsible for ensuring compliance in these laws and a district can lose the ability to use a SRO if these training requirements are not met. For clarification, auxiliary and part-time officers in schools as well as those who are members of institutional police departments are also legally considered SROs and must complete all required SRO training.

Recommendation 5: If a school district authorizes the use of the Commissioned School Safety Officer (CSSO) program, that policies, protocols, training, and selection go above the minimum standards required, to include standard psychological exams, random drug screening, extensive firearms handling training, and regular training with local law-enforcement.

The CSSO program was authorized legislatively through Act 393 of 2015. Since the 2018 Commission recommendations, there has been a significant increase in the use of these programs. According to the 2022 School Safety Assessment, the number of school districts using CSSO programs have quadrupled, with 528 CSSOs across the state. Unfortunately, 60% of the districts using CSSOs, do **not** implement enhanced requirements (standard psychological testing, standard drug screening and training regularly with local law enforcement).

The Arkansas State Police (ASP) is the regulatory agency that manages the Commission School Security Officer (CSSO) program. The ASP require new CSSOs to complete 60 hours of training encompassing active shooter training, live fire training, medical, and weapon retention. The ASP requires CSSOs to receive 24 hours of annual training encompassing the same curriculum as required in the initial 60-hour training. A background check is required every other year because CSSOs are required to renew their credentials on a biannual basis.

It is critically important for local law enforcement agencies to train with their public school and the school's CSSOs. The Commission's CSSO model with enhanced requirements is an economical way of placing armed security within every school, in all of Arkansas's school districts and urges school leaders to consider a hybrid approach using CSSOs and SROs in order to provide every school with armed security redundancy.

Recommendation 6: Schools should consider strategies that layer and build redundancy for optimal security.

This recommendation is meant to stress the importance of designing a district's plan for armed security to include, a method of insuring that, in the event the individual(s) providing armed security are absent, there is another person available to provide the armed security detail for the day. The 2018 Commission's rationale for this recommendation was also to point out that, when possible, a school should have multiple people assigned to armed security on any given day. Layering and redundancy speak to the critical need to not only have armed, trained personnel (SROs and/or CSSOs) present

in each building, but to have multiple in each building for "layering". When utilizing SROs redundancy means having plans in place to have "substitutes" step in when they are absent, just like when a teacher calls in sick.

Schools are best served with law enforcement providing security, but this may be a struggle to accomplish given the level of funding necessary to provide every school with a resource officer and the current retention and recruitment issues facing law enforcement agencies across the state.

Recommendation 7: Arkansas's Commission on Law Enforcement Standards and Training (CLEST) should study the feasibility of school districts being allowed to establish their own law enforcement agencies.

Act 629 of the 2019 regular session gave school districts the ability to form an institutional law enforcement agency, thereby creating a school police department. Since that time, at least **16 school districts have developed their own police departments**. When the commission was gathering information to develop the 2018 report, Commission members heard from several school leaders that believed this model would best serve their districts. There have been several successful agencies established in larger school districts throughout the state.

Audits, Emergency Operations Plans and Drills Progress

The Audits, Emergency Operations Plans and Drills Subcommittee met regularly to discuss the progress achieved in meeting previous recommendations from the 2018 Arkansas School Safety Commission. Below is a description of the progress made in implementing these recommendations and include the results from the 2019 and 2022 surveys.

Recommendation 1: All districts should be required to form District Safety and Security Teams.

The 2022 School Safety Assessment results indicated that 75% of school districts reported they had a District Safety and Security Team. While those schools that have formed these teams are applauded, there is tremendous inconsistency in how frequently the teams meet. These teams, if staffed with appropriate personnel, and tasked with reviewing district Emergency Operations Plans and security policies and procedures, would help create a culture of compliance with security protocols.

District Safety and Security Teams should meet at least two (2) times a year to evaluate

and update security policies and procedures. Districts need to ensure the routine evaluation of security procedures on each campus for: Perimeter doors closed and locked, classroom doors closed and locked, staff wearing ID badges, visitor logs/badges, and drills completed. Steve Vera with the Bentonville School District reported to the subcommittee that the results of his monthly security audits are part of the annual evaluation for principals. In addition, the District Safety and Security Teams should meet at least one (1) time a year with local emergency manager, fire and police to review their Emergency Operations Plans. Encouragingly, in the 2022 School Safety Assessment, 70% of districts indicated that they have a district security director/liaison.

Recommendation 2: Each campus should also designate one current staff member as a School Safety Coordinator.

According to the Arkansas Center for School Safety (the Center), 97% of school districts have reported through compliance forms that they have a School Safety Coordinator. It was determined through discussions that many of the districts did not, however, have one for each campus (i.e.: Elementary School, Middle School, Junior High School and High School). There is apparently some confusion regarding the Safety Coordinator duties/responsibilities and how they interact with the District Safety and Security Team. According to the 2022 School Safety Assessment, school safety coordinators are being assigned to 60% of elementary and high schools.

The designated School Safety Coordinator on each campus should ensure compliance with security policies and procedures and be a member of the District Safety and Security Team. Thanks to a 2019 Bureau of Justice Assistance (BJA) grant, the Criminal Justice Institute/the Arkansas Center for School Safety has been working with key stakeholders to develop the curriculum for a School Safety Coordinator Academy. This one-day, in-person, course will be available in the fall of 2022 and delivered regionally across the state. Topics to be included in the curriculum include emergency operations planning, school safety laws, incident command and best practices, compliance and accountability, responsibilities and coordination with local and county law enforcement as well as fire and county emergency managers.

Recommendation 3: The ADE's Safe Schools Committee membership should be expanded.

Completed. Act 809 of 2019 was passed to expand the membership of DESE's Safe Schools Committee. This committee was initially formed following the shooting at Westside Middle School in 1998. In 2014, the Safe Schools Committee began to meet regularly, typically every two months. Dr. Cheryl May, Director of the Criminal Justice Institute has chaired this committee since 2014. The Safe Schools Committee is charged

with the following responsibilities pursuant to Ark. Code Ann. § 6-15-1301(c):

1) To develop model policies and procedures that may ensure a safe and productive learning environment for students and school employees for recommendations to school districts. The procedures shall focus on ensuring the security of students and school employees and shall include techniques for prevention, intervention, and conflict resolution;
2) To recommend to the State Board of Education any necessary rules for ensuring a safe school environment; and
3) To recommend to the House Committee on Education and the Senate Committee on Education any necessary legislation for ensuring a safe school environment.

Act 809 of 2019 added the following positions to the Safe Schools Committee:

- Director of the Criminal Justice Institute or designee
- Director of the Arkansas Division of Emergency Management, or designee
- Director of the Arkansas Public School Resource Center, or designee
- Director of the Arkansas Rural Ed Association, or designee
- A Chief or a Sheriff
- Arkansas State Fire Marshall
- A school psychologist

Recommendation 4: Schools should modify their fire drills to include additional time for the teacher to evaluate the situation by looking, listening and observing prior to evacuating classrooms.

The 2019 School Safety Assessment showed that 72% of schools reported that they have modified fire drills to include time for teachers to evaluate the situation before evacuating classrooms. The percentage of districts in the 2022 survey that have modified their fire drills increased to 78%. This topic will be an element of the School Safety Coordinator Academy training being developed by CJI. The development of training for teachers is also being considered.

Recommendation 5: Comprehensive school safety assessments should be required to be conducted every three years and reviewed by the school board and school administration.

Acts 620 and 648 of 2021 requires all public school districts and open enrollment charter schools to conduct a comprehensive school safety audit every three years, with

the first audit due by August 2024. It has come to the subcommittee's attention that there is confusion about the use of the terms "assessment" and "audit". Assessments are an overall evaluation of the safety and security of the campus/building. Audits, on the other hand, are conducted regularly (for example weekly or monthly) to evaluate whether safety and security policies are being followed. It should be noted that while the language used in Acts 620 and 648 is audit, in retrospect, the intent is an overall evaluation and therefore, the language should have been "assessment." Modifications should be made to Acts 620 and 648 to reflect the change in the language from "audit" to "assessment".

According to the 2022 School Safety Assessment, 73% of districts indicated that the comprehensive school safety "assessments" required in Acts 620 and 648 of 2021 have been completed. However, only 104 districts have indicated they have conducted a climate survey in the past three years. Culture and climate surveys are a required component of the comprehensive school safety assessments. Consequently, until culture and climate surveys are conducted, comprehensive assessments are in fact not completed. Eighty percent of comprehensive school safety assessments were conducted by district staff.

Recommendation 6: School nurses and staff should be trained in efforts that enhance the emergency medical response within schools.

Given the continuous rise in the number of opioid overdose deaths in the U.S. and Arkansas, in 2019, the Criminal Justice Institute (CJI) and the Arkansas Drug Director's Office partnered with the Arkansas Department of Education and the Arkansas School Nurses Association to provide naloxone training and naloxone kits to school nurses. To date, 899 school nurses representing 215 school districts (81%) have completed training and been provided with naloxone kits. CJI is currently working to replenish kits that have expired Narcan and train and provide naloxone kits to additional school nurses. These efforts are supported through a grant received from the Substance Abuse and Mental Health Services Administration.

Bleeding is the number 1 cause of preventable death. Act 245 of 2019 requires that each public school provide a bleeding control training as a component of a health course to be taught to students in grades nine through twelve (9-12). Thanks to the efforts of several individuals, especially Clayton Goddard, school staff have been trained and Stop the Bleed kits made available. According to the 2022 School Safety Assessment, the number of school districts with "stop the bleed" type kits has increased to 206 (79% of districts).

Intelligence and Communications Progress

Recommendation 1: Each school district should support, establish, and maintain a comprehensive, common communication plan to be utilized by school officials, students, parents, law enforcement, and other stakeholders.

School districts across the state use a number of software and technology applications to communicate information to school officials, students and parents. According to the 2022 School Safety Assessment, 92% of school districts have a communication plan that is used to notify school officials, students, and parents of an ongoing critical incident. Social media platforms, email systems and phone notifications were the top three platforms used for staff, students and parents. School communication efforts with local law enforcement and other key stakeholders in the event of a critical incident is, however, unfortunately, unclear.

During Intelligence and Communication subcommittee meetings, there were several discussions and presentations by subject matter experts that explained the processes being used in various districts to share information. None of the subject matter expert presentations included a platform that delivered information directly to law enforcement. A written example of a communication plan from any school district that could be used as a model or example to demonstrate how various schools are fully implementing this recommendation was not presented. It is believed that the intent of the recommendation was to have a comprehensive communication plan that allowed for information to be shared to all the potential stakeholders. It appears that an effort has been made to communicate effectively with staff, students and parents but unclear the exact level or effort being made to communicate with law enforcement. According to the 2022 School Safety Assessment, 70% of school districts indicate that they have direct communication with local law enforcement through a radio system. However, when asked if the radio systems were AWIN compatible, 84% of the districts did not respond, potentially indicating they did not know if they were AWIN compatible.

Recommendation 2: School districts should have systems that enable direct communication with local law enforcement.

Based on the 2019 School Safety Assessment, 70% of the school districts indicated they have a communication plan that allows instant communication with law enforcement. Examples of direct communication systems include, but are not limited to, emergency alert systems, radios for school officials that are programmed with law enforcement frequencies and/or school district camera systems that can be accessed in real time by

law enforcement.

Information from a number of school district security personnel, (Hot Springs, Cutter Morning Star, Fountain Lake, Jessieville, Mountain Pine and Lakeside), was obtained to determine if they had direct communication with their law enforcement partners. Those that had an SRO assigned to the district stated that they utilized the SRO's radio for direct communication. Others stated that they did not have radio communication and gave responses for direct communication capabilities as being a cell phone or an application/software that sent an emergency alert via text message.

The intent of this recommendation was that school personnel would have the capability to communicate effectively and directly with law enforcement during a critical incident. It was also recognized that in a critical incident the SRO may not be in a position to relay information between school staff and responding law enforcement personnel. This creates a need for communication capabilities beyond the single SRO radio. School administrators need access to direct lines of communication with law enforcement. This will allow pertinent information to be shared and once incident command is established it allows for better command and control across all fronts.

It is recognized that emergency alert systems may be sufficient in sending initial information of a developing event to local law enforcement personnel, but the need for direct radio communication is imperative in navigating a critical incident.

Arkansas Code § 6-15-1302 allows for school districts to install communications equipment that is interoperable with the Arkansas Wireless Information Network (AWIN) system. The Rogers Police Department and Rogers School District formed an alliance that allowed for communication between the two entities via the AWIN system. Secretary A.J. Gary and Penny Rubow from the Arkansas Division of Emergency Management provided a presentation to the subcommittee concerning AWIN capacities and coverage limits. According to the 2022 School Safety Assessment, only 29 school districts indicated that they have radio systems that are part of the AWIN statewide system. The AWIN system has the capacity and coverage allowing for the largest portion of the State to utilize the program, but this does not seem to be the accepted path for communication for school districts. It is unclear if this is a cost issue or lack of knowledge.

Secretary Gary provided a follow-up presentation focusing on a possible statewide buildout of the AWIN system for use by the school districts. This would include the addition of numerous new towers across the state and use of bi-directional amplifiers inside school buildings to increase efficiency. The cost associated with the statewide buildout would exceed $90,000,000.00 or $207 per student. The cost estimate includes radios,

towers, and bi- directional amplifiers for all school districts. The proposal and presentation were for informational and planning purposes only.

Recommendation 3: School districts, in collaboration with local and other law enforcement agencies, should implement and expand strategies to promote reporting, to include anonymous reporting, of suspicious activity/behavior and threats.

Referred to Mental Health Subcommittee

Recommendation 4: Students, staff, and parents should be educated on how to recognize and report signs of at-risk behavior and potential threats.

Referred to Mental Health Subcommittee

Recommendation 5: An analysis should be conducted to determine how the Arkansas State Fusion Center (ASFC) could be more effectively utilized to receive and disseminate information pertaining to threats against schools. In addition, the ASFC could provide timely and relevant information to schools and other appropriate entities pertaining to school safety.

Recommendation 5 has not been achieved, but work is being done to accomplish this goal. A presentation from the Arkansas Fusion Center discussed ongoing efforts to develop partnerships with various vendors to explore social media monitoring and how they can interact with local school districts from an intelligence standpoint.

In addition, we know that there is ongoing discussion on how to incorporate a DESE staff member into the fusion center organizational structure to ensure information sharing. There is also an effort to work more closely with Arkansas Center for School Safety to help disseminate critical information.

There is much work yet to be done but progressive steps are being taken to improve intelligence gathering capabilities and information sharing among various stakeholders.

Physical Security Progress

Recommendation 1: State agencies should work with the federal Readiness and Emergency Management (REMS) for Schools Center Training Assistance Office, to develop a customized, state-level school bus safety initiative for use by districts, schools, and transportation office.

This recommendation was not achieved. No initiative exists between REMS and Arkansas agencies.

Recommendation 2: State leaders should engage the Arkansas congressional delegation and other federal partners to encourage the U.S. Department of Education to allow Title IV formula block grants to include use by schools for infrastructure improvements to support safe and healthy schools, including physical security remedies.

This recommendation was not achieved. There is a limited amount of funding for Title IV. Therefore, it didn't seem cost effective to pursue this option.

Federal funding is, however, available through the Office of Community Oriented Policing Services (COPS Office) School Violence Prevention Program. This program is authorized under the Students, Teachers, and Officers Preventing (STOP) School Violence Act of 2018 (34 U.S.C. § 10551 et seq.). The COPS Office School Violence Prevention Program (SVPP) provides funding directly to states, units of local government, Indian tribes, and their public agencies to improve security at schools and on school grounds in the recipient's jurisdiction through evidence-based school safety programs. This grant does require a 25% match. However, waivers for the match amount can be requested.

There are also certain items (electronic door access, cameras, doors) eligible for districts to purchase with their ESSER funds (with proper ESSER justification: contact tracing).

Recommendation 3: Districts should create an online facility profile within a panic button alert system for each new campus or facility in the district and conduct annual reviews to update facility profiles where needed.

Status: This recommendation was achieved. Acts 620 and 648 of 2021 required a public school shall have a panic button alert system or other means of emergency communication with law enforcement if funding is available. Funding from state was made available for one year, but no funding has been available since. Dr. Cheryl May worked with the state Office of Procurement to establish guidelines for a Request for

Qualifications (RFQ) for emergency response systems. ADE publishes a list annually of vendors who meet the RFQ for emergency alert systems. Per Acts 620 and 648 of 2021 schools are required to provide current floor plans and pertinent emergency contact information to appropriate first responders and update annually. However, according to the 2022 School Safety Assessment, 48 school districts indicated they have not accomplished this goal despite being required by law to do so by October 1, 2021.

Recommendation 4: Districts should review and assess the efficacy of upgrading any old style "crash bar" exterior door egress hardware with the newer "touch bar" type exit devices.

This recommendation has been partially achieved. Per the Division of Public School Academic Facilities and Transportation's (DPSAFT) facility manual "touch bar" type exit devices are now required on new construction. The 2019 School Safety Assessment, however, indicated that only 24% of districts indicated they reviewed and assessed the efficiency of upgrading old style "crash bars" exterior doors and updated to newer "touch bar" devices. School districts are strongly encouraged to upgrade to touch bar exit devices.

Recommendation 5: Prior to installation or contracting to installation of temporary door barricade devices designed to preclude intruders from entering any classroom or learning space of a school building, information pertaining to the project should be uploaded into the Division of Public School Academic Facilities and Transportation's (DPSAFT) web-based project submission tool for review.

This recommendation has been achieved. DPSAFT rules require districts to enter projects into master planning tool and require districts to submit drawings.

Recommendation 6: The state's Academic Facilities Partnership Program should be revised to allow districts to submit eligible campus safety and security upgrade projects for state financial assistance.

This recommendation has been achieved. Partnership Warm, Safe, and Dry Systems Replacement Facility Projects for Safety - Partnership Rules allow for project applications to be submitted to the Division for safety upgrades. "Eligible safety upgrades shall include original installations of the following: secure entrance vestibule, ballistic-rated glass/films, CCTV, Electronic Access controls on doors, intruder locksets, and may include reinforced hallways adjunct to student occupied areas, fully enclosed walkways between buildings, permanently installed screening technology, visitor management systems, hallway security/fire doors, and vehicle barriers." In two Partnership project cycles, 24 security project applications from 18 districts have been submitted at an

approximate cost of $24.1 million.

Recommendation 7: The Arkansas Public School Academic Facility Manual should be revised to provide specific safety and security measures for school districts to consider in the design and construction of new public school academic facilities.

This recommendation has been achieved. Arkansas School Facility Manual Security and Safety (Section 8000) - The Division of Public School Academic Facilities and Transportation now has a section in its facility manual for Security and Safety, which contains requirements and guidelines for new construction. Requirements include standards for Locking Systems / Hardware, Access Control, Communication Systems, Site and Perimeter, Video Surveillance, and Building Systems.

New Commission Recommendations Presented by Subcommittee Topic

General Commission Recommendations

The following recommendations do not fit neatly in any of the Commissions' subject topics and are, therefore, considered "General Commission" recommendations. A list of all Commission recommendations is provided in Appendix C.

Recommendation 1: A school safety unit should be formed in the Division of Elementary and Secondary Education to better ensure school districts are appropriately implementing school-safety related laws, provide support to districts in the implementation of school safety recommendations and assist schools in identifying gaps and needed resources to fill these gaps.

Justification: The Division of Elementary and Secondary Education (DESE) currently has only one school safety-specific position, DESE School Safety Coordinator, that works with the Arkansas Center for School Safety, school administrators and staff and other key school safety stakeholders to identify school safety needs and assist districts in meeting these needs. Since the work of the Arkansas School Safety Commission began in 2018, the need for school safety assistance for Arkansas's schools has dramatically increased. Given the new best practices being identified by the 2022 Commission, that need is further expanded.

Furthermore, in light of the circumstances of the Robb Elementary School shooting, compliance and accountability have become key issues for the 2022 Commission. We must ensure districts are complying with school safety laws and are strongly encouraged to implement the school safety best practices of the Commission. The DESE is uniquely positioned to fulfill this role. However, it is impossible for one person to effectively meet these needs.

Recommendation 2: The Arkansas legislature should consider recurring funding for school districts to implement the Arkansas School Safety Commission Recommendations.

Justification: Thanks to Governor Hutchinson and the Arkansas legislature, $50 million in state grants will be available to school districts to meet the Commission recommendations. We applaud the Governor and legislature for providing this much needed funding that will directly impact the safety of Arkansas's school students. This one-time money will be valuable in meeting many of the physical as well as law enforcement and security recommendations of the Commission.

The 2018 and 2022 School Safety Commissions have, however, made numerous recommendations that require recurring funding to implement. School districts being provided ongoing funding to meet many of the personnel and other school safety needs identified by the Commission as best practices is a priority. We agree that any new recurring funding should be identified and used for only the implementation of the Commission recommendations. Furthermore, this funding should not be used to pay for school safety strategies already in place, but rather used only to enhance, and expand the school safety preparedness capacity of our school districts.

School districts are also strongly encouraged to apply for federal grand funding to meet their school safety needs. In late June, the Bipartisan Safer Communities Act became law. This law expanded the funding available for the school safety needs of school districts and law enforcement. In particular, an additional $1 billion in funding for Title IV, $300 million additional each for the Community-Oriented Policing Services and Bureau of Justice Assistance's Stop School Violence grants, $500 million each for school based mental health services grant program and school-based mental health services professional demonstration grant and $28 million for school-based responses to student trauma. These grants will be beneficial in providing additional funding for physical security upgrades, school resource officers, anonymous reporting systems, behavior threat assessments, school safety training measures and mental health services.

According to the 2022 School Safety Assessment, 87% (216/249) of the responding school districts indicated they have staff capable of completing a federal grant application. Thirty-three school districts indicated they do no have staff capable of completing federal grant applications. The 2022 Commission strongly recommends that school districts work collaboratively, individually or through the education services cooperative, to assist school districts in applying for federal school safety grants.

Recommendation 3: Additional funding should be provided to the Arkansas Center for School Safety in order to build the capacity of the Center to provide training and resources to assist school districts and law enforcement agencies meeting school safety related laws and recommendations.

Justification: The Arkansas Center for School Safety (the Center) is the state school safety clearing house and was established to build the capacity of educators, leaders and law enforcement professionals to meet the safety needs of children in public and private schools. The Center has long provided critically needed free school safety training to administrators, school staff, teachers and law enforcement professionals entrusted with student safety. The Center has been instrumental in assisting school districts meet the requirements of school safety laws and implement the 2018 Arkansas School Safety Commission Recommendations.

Currently, there are three full-time staff within the Center. In addition to the school safety training provided, the Center is also responsible for ensuring school districts comply with Acts 551 and 622 focusing on the implementation of the School Resource Officer program. Additional funding for staff and program costs will be needed to continue and expand the training and resources available to districts to continue to comply with the current and new school safety laws and implement the 2018 and 2022 Arkansas School Safety Commission recommendations/best practices.

Recommendation 4: School districts should be required to include the implementation status of the Arkansas School Safety Commission recommendations in their annual report to the public.

Justification: The recommendations of the 2022 School Safety Commission are developed as best practices. Many recommendations may never become requirements through legislation or rule but remain essential considerations for districts. Including the implementation status of school safety recommendations in a school district's annual report to the public will promote an ongoing culture of school safety among stakeholders and the community. Based on survey data from the 2019 School Safety Assessment, there has not been full implementation of the 2018 Commission best practices due to a myriad of reasons, such as lack of funding, feasibility and sometimes lack of support at the local district level. Another barrier to implementation may be complacency over time. Districts are already required to provide an annual report to the public that includes several items, such as academic goals and proposals to correct deficiencies. A district should include an annual update on progress toward school safety recommendations or the reason for lack of progress. This information would inform state and local leadership of needs and promote assistance to districts in correcting deficiencies in those identified areas.

Recommendation 5: The Division of Elementary and Secondary Education's Safe Schools Committee should investigate the feasibility of developing a school safety award/recognition program for school districts that incentivizes the implementation of the Arkansas School Safety Commission recommendations.

Justification: By implementing a voluntary system that publicly recognizes school districts for implementing and maintaining the Arkansas School Safety Commission recommendations, districts will be more likely to develop sustainable plans of adherence to the best practices adopted by the Commission.

Furthermore, school districts that are recognized for prioritizing school safety preparedness will be able to share their achievements at their annual public meeting. This should establish another level of public confidence that the district is taking seriously their charge to not only educate, but to create a culture of safety for students and employees.

Physical Security

Recommendation 1: The legislature should change the language in Arkansas *Code§ 12-13-109* to "keep all exiting doors and classroom doors closed and locked during school hours, with the exception of transition times. No person shall be impeded from building egress per the current State Fire Prevention Code and the ADA Standards for Accessible Design."

Justification: *The legislature needs to modify language in Arkansas Code§ 12-13-109 (2020). Currently, it requires teachers to "...keep all doors and exits unlocked during school hours." Arkansas Code§ 12-13-109 (2020) states, "It shall be the duty of the Director of the Division of Arkansas State Police, his or her officers, and deputies to require teachers of public and private schools and all educational institutions to have one (1) fire drill each month **and to keep all doors and exits unlocked during school hours."** The underlined requirement contradicts the previous two subcommittee recommendations requiring all exterior and classroom doors to remain closed and locked.*

Subsequently, the Physical Securities subcommittee added the following (underlined) language, recommending the legislature change Arkansas Code§ 12-13-109 (2020) to the following: ...to keep all exterior doors and classroom doors closed and locked during school hours with the exception of transition times (to allow for limes between classes and before-and-after school). No person shall be impeded from building egress. per the current State Fire Prevention Code. The Physical Securities subcommittee and state fire marshal share the concern of following the fire code and addressing fire and easy egress; hence, the language addressing egress was included in the subcommittee's recommendation.

The legislature needs to change the language in Arkansas *Code§ 12-13-109* to "keep all exiting doors and classroom doors closed and locked during school hours, with the exception of transition times. No person shall be impeded from building egress per the current State Fire Prevention Code and the ADA Standards for Accessible Design."

Recommendation 2: Districts should, at a minimum, install electronic access controls for high-frequency-use exterior doors.

Justification: Ideally, electronic access controls should be installed on every exterior door. However, such a recommendation must be balanced with fiscal resources; therefore, the language of the recommendation is written to focus on installing electronic access controls for high-frequency use exterior doors. Additionally, electronic assess has several benefits, e.g., it takes the human error element out, thereby tremendously reduces human error; it provides additional important data to monitor, showing name, date, and time every time anyone comes enters and/or departs; and when combined with a camera system, electronic

access controls can help improve accountability. Understanding that budgets may not allow for electronic assess controls on all doors, it is recommended, at a minimum, to install access controls on high-frequency-use exterior doors. Additionally, the Division of Elementary and Secondary Education will be requiring construction of all new schools to use electronic access control on all exterior doors.

Recommendation 3: District campuses should have security cameras that are accessed by designated individuals, including law enforcement, during a critical incident.

Justification: Security cameras would allow for quicker response time for first responders and in case of an active shooter event, time is of the essence. Security camera systems extend the ability to guide first responders to the exact location on campus. Furthermore, local law enforcement's access to security camera footage should only occur during critical events. Such access by law enforcement during critical incidents is extremely helpful for identifying the location both outside and inside.

Recommendation 4: District campuses should have one secure visitor point of entrance with ideally a secured vestibule, when allowable.

Justification: Each district campus should have one visitor point of entrance. The language, "if feasible, a secured vestibule at main entrance" was included as it may not be feasible to do, due to how the current building is built. Vestibules are however, required by the Division of Elementary and Secondary Education for construction of new school buildings. It allows for a more effective controlled access point, improves the overall security of the building, and allows more efficient monitoring as there is only one entrance for visitors.

Recommendation 5: All exterior doors to school buildings must remain closed and locked.

Justification: According to the Texas House Investigative Committee Report on Uvalde (Report), Robb Elementary had a culture of non-compliance with safety policies requiring doors to be kept locked. The report also indicated that staff consistently used colored rocks to prop open exterior doors. The intruder was able to enter Robb Elementary through an unlocked, exterior door because the lock on that door did not function properly. In contrast, in Gaston Alabama, in June 2022, the perpetrator could not get into the school building because the exterior doors were closed and locked. Another example of an attacker entering through exterior doors was an incident, according to the police report in May 2018, at Santa Fe High School. The attacker was able to get into the building through the exterior doors and activated the fire alarm prompting students to exit into the hallway. It is imperative that exterior doors must remain closed and locked at all times.

Recommendation 6: Require district campuses to use a visitor management system.

Justification: Knowledge of who is inside the building and screening people who come into building to help control access and prevent unauthorized personnel from getting inside building. This measure will serve as a multi layered approach in the following areas: (1) Preventing access to unauthorized people from entering the building; (2) written record of visitors inside the building; (3) service to parents and other stakeholders in the community. This measure will provide direction from other campus related questions that will minimize them from wondering around different areas of the campus.

Recommendation 7: All classroom doors to school buildings must remain closed and locked.

Justification: According to the Texas House Investigative Committee Report on Uvalde, teachers at Robb Elementary commonly left interior doors unlocked for convenience. Consequently, the intruder was able to enter a classroom of an unlocked classroom door at the elementary school. Obviously, if an intruder is unable to enter through the classroom door, it makes it more difficult for the intruder to harm students. Additionally, it buys time for first responders, law enforcement to get there. It is imperative that all classroom doors remain closed and locked at all times. This would include adjacent doors. At Uvalde, the intruder gained access to room 112 through an adjacent door in classroom 111.

Recommendation 8: All school districts should utilize a grand master key system ensuring that each campus has a master key.

Justification: This allows for quick and easy access for authorized school personnel. It is critical that multiple authorized personnel have quick and easy access to every space on the campus to prevent a potential threat to students or staff. During a potential threat to students or staff, precious time cannot afford to be lost searching for keys to gain access to a room.

Recommendation 9: Every district should provide master key(s) access to local law enforcement for use during a critical incident.

Justification: Allows for law enforcement to gain access to the school as quickly as possible in response to a critical incident. Each district needs to decide how best to provide the master key(s) to their local law enforcement. Precious time cannot afford to be lost searching for keys to get access. According to Texas House investigative committee report on Uvalde it states that "...officers spent a great amount of time seeking a master key..." (bottom of page 46), "While Sgt. Coronado was outside, his body camera recorded several people commenting on the need to find a master key to the classrooms."(page 56), "Much of

this time was spent by Chief Arredondo on the phone with Constable Field. He issued a series of additional requests for equipment and support, including snipers, a master key, and breaching tools, repeatedly referencing the need for a key and breaching tools before they could attempt to enter the classrooms with the attacker." (page 56). It is critical that law enforcement have quick and easy access to every space on the campus in response to a critical incident.

Recommendation 10: District campuses need to protect any glass that allows vision or access into the classroom from the corridor.

Justification: Any glass between the corridor and classroom provides accountability for students and teachers during a normal school day. The purpose for installing shatter resistant film on the glass is to provide protection from threats outside the classroom. Shatter resistant film on any glass at a classroom door or window is the most economical product to deter an active shooter from gaining access into a classroom. At Marjory Stoneman Douglas High School in Parkland, Florida, the shooter killed and injured numerous students by shooting through the vision panel on multiple locked doors.

Recommendation 11: District campuses should use covers on vision panels on classroom doors during lockdowns that also allow students a blind area to 'hide'.

Justification: This provides another layer of protection for students and teachers in the event of a threat from the outside of the classroom. Research shows that in active shooter incidents the attacker is looking for quick access and easy targets. When they cannot visually see targets, they move on to other potential victims. According to the 2022 School Safety Assessment, 53% of school districts do not use covers on vision panels.

Recommendation 12: District campuses should equip classroom doors with locks so that doors can be locked from the inside, allow for access from outside for authorized personnel, and allow for egress per the current State Fire Prevention Code and the ADA standards for accessible design.

Justification: Because of other potential threats such as fire and the threat coming from someone inside the classroom all three aspects need to be addressed. "Doors that lock from inside are most effective in securing a classroom, according to a 2015 report by the Sandy Hook Advisory Commission. Exterior locking doors may put teachers or others in the path of an active shooter by requiring them to go into the hallway to lock the door. In the February 2018 shootings at Marjory Stoneman Douglas High School, teachers were injured or killed while trying to lock their classroom doors from the outside. Even if doors have interior locks, they must be accessible from the outside to administrators and emergency personnel. Provide these individuals with keys or an exterior access method." (see articled linked). A

strong layer of security would be for all interior doors to contain access control systems. This would allow for all doors to be locked at the same time with one click of the mouse. With electronic access control keys become obsolete and doors can be unlocked with a badge or fob. NFPA 101 (life safety code) requires doors to be readily opened from the classroom side. Makeshift devices such as after-market locking and barricades, wedges, rope, and chains not only violate this rule, but can either slow down or prevent first responders from quickly entering a classroom, or they can be used by an intruder to trap people inside and keep first responders from getting in.

Recommendation 13: Add physical security items to existing Division of Public School Academic Facilities and Transportation's *(DPSAFT)* Maintenance & Operations facility inspection checklist.

Justification: DPSAFT will ensure school safety measures are in place & used appropriately. If deficiencies are discovered, DPSAFT will follow-up with the district providing those deficiencies for the district to correct within 30 days. Area Project Managers-Maintenance will add security/safety measures to their inspection forms. Data will be collected through a drop-down form that will include the following items: Date; perimeter doors secured *(Yes/No);* interior doors secured *(Yes/No);* staff wearing badges *(Yes/No);* visitor security *(Yes/No);* drills completed *(Yes/No).* The district will have 30 days to provide a written corrective action plan to address the deficiencies found during the DPSAFT maintenance inspection.

Recommendation 14: Dedicate at least 20 minutes of Division of Public School Academic Facilities and Transportation's (DPSAFT) 3-hour required annual bus driver training to bus security.

Justification: The bus drivers need clarity on bus security issues and the proper emergency response in the event of a critical incident and other bus security concerns. School bus drivers are now receiving annual bus training which includes security issues. This annual training has been proven effective by specific examples of how bus drivers can respond in crisis situations. One such example happened with the PCSSD, what is now the Jacksonville North Pulaski School District, on October 7, 2013. While loading students on the bus, a man waving a knife got on the school bus. The school bus driver used the training she received by keeping the man at the front of the school bus. The bus driver also kept the man occupied through conversation while at the same time keeping the students calm by reassuring them. Drivers are trained on how to make the public aware of a critical situation such as this one. DPSAFT has taken a proactive approach for school bus safety on the national level by participation in *"School Bus on the Lookout",* a training provided through TSA. Janet Clarke, DPSAFT Senior Transportation Manager, and SESPTC Board Program Chair, recently received training at

the Southeastern State Pupil Transportation Conference *(SESPTC)* held in Hampton, Virginia. Mike Simmons, DPSAFT Public School Program Coordinator, currently president-elect of the National Association of State Directors of Pupil Transportation Services *(NASDPTS),* will be officially named president of the NASDPTS this October in Washington D.C. and is regularly involved with federal agencies working to keep school bus transportation safe for all students.

Recommendation 15: Any doors on district campuses that have faulty locks must have a high priority work order entered immediately and the faulty locks must be repaired/replaced immediately.

Justification: According to the Texas House investigative committee report on Uvalde it states that *"Robb Elementary had recurring problems with maintaining its doors and locks. In particular, the locking mechanism to Room 111 was widely known to be faulty, yet it was not repaired. The Robb Elementary principal, her assistant responsible for entering maintenance work orders, the teacher in Room 111, other teachers in the fourth-grade building, and even many fourth-grade students widely knew of the problem with the lock to Room 111."*

Recommendation 16: District campuses should have shatter resistant film at school entrances, especially the main entrance.

Justification: The shatter resistant film will protect the students & staff members from an intruder gaining quick access into the rest of the building. It will slow down the intruder's ability to enter building and allow more time for first responders. At Sandy Hook the intruder shot through a plate-glass window next to Sandy Hook's locked front entrance in order to quickly and easily gain access to the school.

Recommendation 17: District campuses should have physical barriers such as bollards, landscaping, fencing, low walls, etc. at school entrances, especially the main entrance.

Justification: Physical barriers provide exterior protection for the building. It reduces the ability for an intruder to use a vehicle to drive into the building or the campus. According to the 2022 School Safety Assessment, 62% of school districts do not have physical barriers at main entrances of schools.

Recommendation 18: District campuses should have corresponding numbers on

classroom interior and on exterior surfaces (wall, door, or window) easily identifiable to first responders so that they can reference position of students and/or intruders.

Justification: When emergencies occur, the rapid response of emergency workers to the incident can be critical. Many schools have dozens of doors providing entrance and egress to their buildings. During an emergency it may be necessary for responders to gain access through the door or window closest to the emergency scene. Numbering external doors and windows can be extremely valuable to emergency responders and will also assist the students and staff in acclimating themselves in case of an emergency. Door and window numbers should follow the international fire code for building identification as stated below:

- Arabic numbers and/or alphabetical letters
- Visible from the closest road & driveway
- Contrasting in color to its background.
- Reflective material & visible in dark or smoky conditions
- Larger than 4 in. and 1/2 in. wide
- Interior doors will be marked at the bottom of the door, and on the top of the door from inside the classroom
- Regularly maintained.

Intelligence and Communications

Recommendation 1: School Districts should develop layered two-way communication access between staff members and administrative staff via various platforms to ensure information sharing and improve alert processes.

Justification: In numerous critical incidents after action reports revealed that lack of communication is a constant area identified as a failure or an area that needs improvement.

For many reasons, it is a fore gone conclusion that effective communication is needed during a critical incident. These reasons include the basic need to ensure a successful deployment of resources, to create an environment where pertinent information is being shared among all stakeholders, and creating a strategy that leads to a high probability of success. Lines of communication need to be successfully implemented from the start of the event through the conclusion.

As clearly outlined in the Robb Elementary Report, the lack of successful communication with staff throughout the campus lead to confusion and potentially cost lives. We know from the report that the administration and their law enforcement officials developed a written plan that outlined procedures to be taken during a critical incident and how the information would be shared.

The school used a cell phone and a computer application that depended on Wi-Fi to connect to their cell phone or the staff member had to check their computer for the alert. Certain staff members had radios that were capable of communicating with the administrative office but it is unclear how many staff members had access or used the radio to relay information. The school also had a standard intercom system.

Continuing with the concept of layering, it is recommended that each school district campus have multiple ways to communicate critical information. The ability to reach the masses from a single platform such as an intercom system is imperative. The initial notification that an attempt at mass murder is occurring allows for the staff and students to take appropriate immediate action. These announcements then need to be supported with additional methods of communication that relays critical information.

The cell phone applications are commonly used but for them to work successfully in a brick, mortar and steel building the Wi-Fi must be sufficient. The value of most of these applications is that any staff member with the application that has access to their cell phone can initiate the alert. The Robb Elementary report indicated that staff did not always carry their cell phones and that the Wi-Fi was not sufficient throughout the building for it to work effectively. For these type applications to be effective a culture of maintaining cell phones is critical and ensuring that Wi-Fi is sufficient needs to be a requirement.

Radio communication is a key component in relaying information between staff members. Traditionally, radios may be limited in number and only assigned to certain staff. The assignment and use of these radios should be carefully thought out. Radio assignments to staff that are outside building or staff that have the authority to implement emergency protocols is essential. We know that the staff member that was outside and witnessed the Uvalde shooter jump the fence had access to a radio and notified the office. It is unclear how the Robb Elementary radios were used beyond that point.

The ability for staff members and administration to effectively communicate immediate threats is extremely important in saving lives. These lines of communication should be capable of going up and down the chain of command. The teacher in the classroom needs the ability to share information directly with administrative staff members, the coach on the field needs the ability to pass information of a developing situation on the exterior of the facility and administration needs the capability to deliver critical information to all personnel in a clear and concise method.

There are a multitude of communication platforms that allow for effective and rapid passing of information. A specific type of device or applications not being recommended. However,

the need for a layered communication plan that allows for two way, immediate and effective passing of critical information that will help save lives is stressed.

Specific information pulled from the Robb Elementary Report supporting a comprehensive use of a communication plan:

1) Other factors delayed the reporting of the threat to the campus and to law enforcement: Low quality internet service, poor mobile phone coverage, and varying habits of mobile phone usage at the school all led to inconsistent receipt of the lockdown notice by teachers. If the alert had reached more teachers sooner, it is likely that more could have been done to protect them and their students. (*Robb Committee Report, pg. 6*)

2) The active shooter policy outlined a series of preventative safety measures that served as the "primary preventative strategy" to address "problems of violence, vandalism, disruptions and fear."

    a. RADIOS – Key staff have been provided RADIOS to support campus communication processes. (*Robb Committee Report, pg. 16*)

3) Raptor Alert System

4) School district witnesses also testified to another effect of the rising prevalence of bailouts. The alert system does not differentiate its signals between bailouts and other kinds of alerts, such as an active shooter situation. The series of bailout-related alerts led teachers and administrators to respond to all alerts with less urgency—when they heard the sound of an alert, many assumed that it was another bailout. Raptor Technologies supplied the alert system Uvalde CISD used. Uvalde CISD had used Raptor's software to screen campus visitors for approximately 10 years. In the fall of 2021, Mueller viewed a presentation on Raptor's emergency management alert system, and he gathered the Uvalde CISD principals, who agreed that they needed it. Uvalde CISD purchased the software in October 2021, and the first Raptor alert occurred on February 8, 2022. By March 2022, as Uvalde CISD was implementing the Raptor alert system, there was a high volume of alerts. By utilizing the Raptor mobile phone application, any Uvalde CISD employee could activate an alert. Staff at a school campus typically would first learn about a bailout from an external source. Then they would decide, depending on the proximity of the threat to the school, whether to initiate a "secure" alert or a "lockdown" alert. The Committee received evidence that Uvalde CISD employees did not always reliably receive the Raptor alerts. Reasons included poor wi-fi coverage, phones that were turned off or not always carried, and employees who had to log-in on a computer to receive a message. (*Robb Committee Report, pgs. 23 and 24*)

5) Robb Elementary Coach Yvette Silva was outdoors at that time with a group of third graders, and she spotted the backpack being tossed over the fence followed by a person dressed in black climbing over it. She then saw the person raise a gun and

begin to shoot. Coach Silva thought the attacker was shooting at her, and she ran from the field toward her classroom. She used her school radio to report: "Coach Silva to office, somebody just jumped over the fence and he's shooting." She ran toward a group of third graders on the school playground to tell them to lock down. She expected to then hear an announcement of a lockdown, but she did not hear one right away. Meanwhile, the attacker proceeded to the fourth-grade teachers' parking lot, continuing to fire his gun.

6) As the attacker approached the school and as law enforcement responders were arriving, staff at Robb Elementary were beginning to lock down, based mostly on word-of-mouth reports of an armed man on campus. Principal Mandy Gutierrez had just finished an awards ceremony and was in her office when she heard Coach Silva's report over the radio. She attempted to initiate a lockdown on the Raptor application, but she had difficulty making the alert because of a bad wi-fi signal. She did not attempt to communicate the lockdown alert over the school's intercom. By phone, she called and spoke with Chief Arredondo, who told her, "shut it down Mandy, shut it down." She told head custodian Jaime Perez to ensure that all the doors were locked. She initially locked down in her own office, but she later moved to the cafeteria. (*Robb Committee Report, pg. 44*).

Recommendation 2: School Districts should develop capabilities to monitor communication platforms, on school owned devices, to include social media outlets as it relates to threats or triggering phrases used by potential active attack suspects.

Justification: According to the 2021 Secret Service Averting Targeted School Violence Report, 67 school attacks were prevented. Of those 63 or 94% of the plotters of school violence shared their intentions about carrying out the attack in a variety of ways. This included verbal statements, electronic messaging, and online posts through various platforms. In 43%, the would-be attackers documented their intentions in journals, documents, videos, and audio recordings.

Based on the research conducted by the Secret Service, 11 of the averted cases involved a form of social media. The platforms that were used included Snapchat, MySpace, Omegle, Twitter, and YouTube. In addition, the Robb Elementary shooter utilized social media platforms such as Instagram and Yubo, revealing information that could have potentially assisted in averting the Uvalde shooting.

Locally, the subcommittee was presented with information regarding the Little Rock School Districts technology monitoring program and the success that they have seen from its use. The system is used with every LRSD device that has internet capabilities and monitors communications, photos, chats over all LRSD devices and then alerts school officials when any of the following areas of concern are identified; self-harm, depression, suicidal ideation, substance abuse, pornographic content, unhealthy relationships, threats of violence or

bullying/cyberbullying. The Little Rock School District system reviewed 93,870 items and spent 806-man hours in the process. In that review, the system, added by human intelligence, identified 77 incidents that were deemed immediate response situations. That is 77 interventions or potential averted incidents.

It is well documented that no real profile can be built for the attacker in these incidents but we know that there are several common factors. Many of these factors can be identified by review of the subject's social media platforms. Traits such as; attackers having interests in violent topics, their relationships socially and romantically, and they are often victims of bullying. Having the ability to monitor devices being used at school or through the use of the districts internet system is critical. It is just as important that once the potential suspects are identified that law enforcement have the means and investigative knowledge in monitoring and collecting evidence from the social media platforms in a legal and ethical manner.

The Uvalde shooter social media foot print was large and gave clues to his intent and specific time frames:

1) Finally, the attacker developed a fascination with school shootings, of which he made no secret. His comments about them coupled with his wild threats of violence and rape earned him the nickname "Yubo's school shooter" on that platform. Those with whom he played games taunted him with a similar nickname so often that it became a running joke. Even those he personally knew in his local chat group began calling him "the school shooter" after he shared pictures of himself wearing the plate carrier he'd bought and posing with a BB gun he tried to convince them was real. None of his online behavior was ever reported to law enforcement, and if it was reported by other users to any social media platform, it does not appear that actions were taken to restrict his access or to report him to authorities as a threat. (*Robb Committee Report, pg. 33*)

2) While a vague idea for a school shooting appears to have been in the attacker's mind as early as late 2021, he began to pursue his evil plan in early 2022 after a falling-out with his mother. A blowout argument between them was livestreamed on Instagram, and several members of their family viewed it.

3) Online interactions involving the attacker continued to foreshadow a tragedy. In March 2022, in an Instagram group conversation, a student told him that "people at school talk [expletive] about you and call you school shooter." Later, the attacker began referencing a timeline. On April 2nd, he asked in a direct message on Instagram, "Are you still gonna remember me in 50 something days ?" After the answer, "probably not" he retorted with, "Hmm alright we'll see in may ".The attacker often connected those dates with doing something that would make him famous and

put him “all over the news,” and many of those with whom he chatted suspected his cryptic deadlines meant violence. For example, in a May 14th conversation he simply wrote “10 more days,” leading to immediate speculation that he meant he’d “shoot up a school or something” or commit “mass murder” on that date. On May 17th, a friend told him that an acquaintance of theirs was “telling everyone u shooting up the school.” The attacker also began sharing photos of his rifles, including with total strangers. Those in his Snapchat group claimed they believed the guns were fake (despite the attacker posting the receipt) because he had tried to pass off a BB gun as real the year before. For those with no reason for doubts, the context often made the shared images disturbing, such in late April when a friend proposed visiting the attacker in Uvalde:

4) In the last days before the shooting, the attacker saved news stories and other information about the mass shooting in a Buffalo, N.Y. supermarket on May 19, 2022. He also spent time with his cousin’s son, who attended Robb Elementary. After playing the children’s videogame Roblox, the attacker elicited from him details about his schedule and how lunch periods worked at the school. On the eve of the shooting, the attacker began contacting numerous people with vague but ominous messages about doing something the next day. In one Snapchat exchange with a German teenager he had befriended, he commented: “I got a lil secret.” When she became curious, he told her it was “impossible for today” because he was still waiting for something “being delivered Monday 23 by 7 pm.” His order of 1,740 hollow points arrived later that day. Prior to the shooting, the attacker had no criminal history and had never been arrested. He is not known to have espoused any ideology or political views of any kind. Private individuals alone knew the many warning signals. (*Robb Committee Report, pgs. 37 and 38*)

Recommendation 3: Law enforcement agencies are encouraged to develop educational programs and build relationships within their communities to encourage reporting and to identify suspicious activity by those with the intent to commit harm.

Justification: According to the Secret Service, prevention can be challenging, but with preparation and collaboration communities can succeed. School districts cannot be left to bear the full responsibility of prevention and intervention. Law enforcement must be more proactive in their approach to identifying, comprehensive intelligence collection and investigated those that wish to commit mass murder.

The cases included in the 2021 U.S. Secret Service, Averting Targeted School Violence report includes cases that were averted through various means. The cases included in the study are only a sample of the tragedies prevented every day across our country. The cases

represented in the study affirm that bystanders coming forward to report concerning behavior can save lives. The study further establishes how public safety professionals must be deliberate in how they encourage and facilitate bystander reporting.

Once the public is educated to the need and process of reporting suspicious activity and relationships are developed that allow for the sharing of intelligence the law enforcement response must be to the appropriate degree of investigation, assessment and management.

In 13 of the 67 averted attacks, the attackers warned friends and other peers about the impeding attacks by telling them details of something that was going to happen. The plotters made specific statements to their peers that they should not come to school on certain dates. Critical information is being shared by the attackers to people within our communities. The data supports that the information is there and that obtaining that information is critical in averting future events.

In 75% of the averted events, the plots were solely detected based on the suspect's communication with others within their community.

This approach would be very similar to the Federal Bureau of Investigations approach to potential terror investigations post 911. Federal investigators built relationships with flight schools to identify suspicious activity and developed a culture that built trust and the reporting of potential criminal behavior. They did the same type thing following the Oklahoma City Federal Building bombing. This proactive approach to involving the public by educating them of the need, what to look for and how to report can be one of the best preventative tools we can develop.

Suspicious activity committed by the mass murderer in Uvalde, Texas as related to us in the Robb Elementary Report:

1) The attacker began wearing black clothes, combat boots, and long, unkempt hair. He was active on several social media platforms, including TikTok, Instagram, YouTube, and the French livestreaming platform Yubo. He networked with local peers in ongoing group chats on Snapchat, and he played a range of videogames, including the Call of Duty and Grand Theft Auto series. Most of his usernames and even his email address reflected themes of confrontation and revenge. The attacker began to demonstrate interest in gore and violent sex, watching and sometimes sharing gruesome videos and images of suicides, beheadings, accidents, and the like, as well as sending unexpected explicit messages to others online. Those with whom he played videogames reported that he became enraged when he lost. He made over-the-top threats, especially towards female players, whom he would terrorize with graphic descriptions of violence and rape. His online interactions grew more

manipulative and controlling as the year wore on, and he presented a more commanding personality online than he did in person. He pretended to a greater level of maturity than he had, searching the internet for information on sexual practices mentioned by others in conversation. The attacker wrote about his difficulty connecting to other people or feeling empathy for them; he said he was "not human," and he called others "humans," apparently intending it as an insult. Later internet usage suggests he may have wondered if he was a sociopath and sought out information on the condition. His internet research resulted in him receiving an email about obtaining psychological treatment for sociopathy. The attacker became focused on achieving notoriety. He believed his TikTok and YouTube channels would be successful. The small number of views he received led him to tell those with whom he interacted that he was "famous," that they were mere "randoms" by comparison, and that they were lucky to interact with him. On Yubo, the attacker spoke enviously of publicity given to a murderer and animal abuser whose story became widely known after a Netflix documentary. In late 2021, he shared a video online that showed him driving around with "someone he met on the internet" holding a clear plastic bag that contained a dead cat, which he discarded in the street and spit on while his driver laughed. The video then showed the attacker wearing a tactical plate carrier, went on to show him dryfiring BB guns at people, and ended with footage of emergency services responding to a serious car accident, which he claimed his driver had caused. The attacker got a job in late 2021. (*Robb Committee Report, pgs. 33 and 34*)

2) Meanwhile, the attacker's planning and preparation became more focused. The Committee received extensive documentation compiled and created by the Bureau of Alcohol, Tobacco, Firearms and Explosives in the course of its investigation of the attacker's purchases. He began buying more firearms accessories beginning in February 2022, including 60 30-round magazines, a holographic weapon sight, and a Hellfire Gen 2 snap-on trigger system. On March 23, 2022, a suspicious person dressed in all black with a backpack was seen canvasing Robb Elementary, but no one ever identified the person. As soon as the attacker turned eighteen on May 16, 2022—just one week before the shooting on May 24, 2022—he was finally able to purchase guns and ammunition. An online retailer shipped 1,740 rounds of 5.56mm 75-grain boat tail hollow point to his doorstep, at a cost of $1,761.50. He ordered a Daniel Defense DDM4 V7 (an AR-15-style rifle) for shipment to a gun store in Uvalde, at a cost of $2,054.28 (including tax and transfer fee). On May 17, 2022, he bought a Smith and Wesson M&P15 (also an AR-15-style rifle) at the same store in Uvalde, at a cost of $1,081.42. He returned the next day for 375 rounds of M193, a 5.56mm 55-grain round with a full metal jacket, which has a soft core surrounded by a harder metal. He returned again to pick up his other rifle when it arrived on May 20, 2022, and he had store staff install the holographic sight on it after the transfer was

completed.108 The owner of the gun store described the attacker as an "average customer with no 'red flags' or suspicious conditions"—just that he was always alone and quiet. The owner of the store remembered asking how an 18-year-old could afford such purchases (the rifles alone were over $3,000), and the attacker simply said he had saved up. Patrons of the store who saw him told 108 The exact cost of all magazines, sights, and a different story in FBI interviews, saying after the tragedy that the attacker was "very nervous looking" and that he "appeared odd and looked like one of those school shooters"; another described his all-black clothing as simply giving off "bad vibes." A background check was conducted, and the attacker qualified for the purchases. While multiple gun sales within such a short period are and were reported to the ATF, the law only requires purchases of handguns to be reported to yhe local sheriff. Here, the information about the attacker's gun purchases remained in federal hands. (*Robb Committee Report, pgs. 34 and 35*)

3) The attacker was at home with his grandparents on the morning of May 24th when he sent eerie online messages, including to an Instagram model he'd never met whom he had tagged in pictures of his guns the week before. "I'll text you in an hour," he wrote, "But you HAVE TO RESPOND. I got a lil secret. I wanna tell u" Evidence shows that the attacker had been getting in increasing conflicts with his grandmother, and she had threatened to remove him from her mobile phone plan. On the morning of May 24th, she called customer service to do just that. After a nearly hour-long FaceTime conversation with his online acquaintance in Germany, the attacker began texting her live updates: While these text messages have been circulated in media reports, those reports do not include a message deleted by the attacker's correspondent before the screenshot was taken. Just twenty-eight seconds after the attacker informed her that he had shot his grandmother and intended to "shoot up" an elementary school, the German teenager replied with a single word: "Cool." (Robb Committee Report 39 and 40)

Recommendation 4: Law enforcement should coordinate with school districts to ensure that there is limited access to existing law enforcement communication network, (radio systems) for critical incidents. We recommend for new radio systems that are being

developed by law enforcement to consider the school district as part of their initial buildout. Radio system use should be allowed with limited use during critical incidents only and be restricted to certain school administrators and staff.

Justification: The importance of proper communication has been identified as an area that needed improvement in a majority of the debriefs and after-action reports from a variety of critical incidents. The ability for critical information to be passed immediately from key stakeholders is imperative to saving lives.

It was noted that critical information was not being passed in the Uvalde incident. The Chief of Uvalde School District Department failed to even carry his radio and the lack of a proper communication plan with shared radios hindered the ability to communicate critical information from being passed regarding incoming 911 calls from victims injured in the classrooms.

Based on a presentation by subject matter experts we understand that school districts cannot be added as an entire entity based on limited capacity with the AWIN system. Therefore, the recommendation would be based on radios and access being limited to critical staff members. These staff members would be allowed to use the radio system during a critical incident to effectively and immediately communicate with first responders.

Not every jurisdiction will join the AWIN system. However an agreement is encouraged between all law enforcement agencies and schools located in their jurisdiction to share limited access to whatever the radio system may be.

Limited radio access should be allowed for school districts during critical incidents for existing communications systems and those that being built in the future.

From a buildout cost stand point we encourage that as law enforcement agencies build new radio systems they add the school district critical staff to the radio assignment list with the those selected having limited access to only be used during a critical incident. This will help limit the cost to school districts.

It is recommended that all radios that are purchased met P25 Compliant requirements as outlined by the Department of Homeland Security.

Following the tragic events from 9/11, legislation was passed to improve the interoperability of public safety communications systems and equipment. Congress mandated that new or upgraded equipment must be interoperable and meet certain interoperability standards. As a result, the Federal Government supported the purchase of P25 compliant LMR equipment through grants and policy, to ensure public safety systems can interoperate, regardless of

manufacturer. Purchasing P25 equipment ensures that digital LMR systems will be compatible with other, most importantly contiguous, P25 systems. Additionally, standards-based systems enable interoperable communications between emergency responders from various agencies, jurisdictions, and levels of government in the event they need to communicate during day-to-day incidents, large-scale emergencies, and disaster responses. Additionally, P25 standards provide a broader resource of competitive vendors providing more flexibility in purchasing equipment.

P25 is a suite of standards and specifications which enable interoperability among digital two-way land mobile radio (LMR) communications products provided by multiple manufacturers to support the mission critical public safety requirements. These standards provide a number of technical specifications for emergency communications equipment designed to ensure that equipment is interoperable, regardless of manufacturer. The P25 suite of standards, referenced as TIA-102 standards, is published by the Telecommunications Industry Association (TIA),1 a recognized American National Standards Institute standards development organization.

CYBERSECURITY

Since the 2018 Arkansas School Safety Commission completed its work, cybersecurity has become an important component of comprehensive school safety strategies. As a result of the COVID-19 pandemic and the need for schools to transition to virtual learning environments, the number of cyber-attacks on education institutions has dramatically increased. Due to the lack of consistent reporting requirements or practices for schools across the U.S., unfortunately, the exact number of cyber-attacks experienced by K-12 schools is not known. However, the number of publicly disclosed cyber incidents has increased significantly since 2019. The K-12 SIX 2022F cybersecurity report indicates that 1,331 cyber incidents have occurred in schools since 2016, with the majority of those attacks recorded for 2019, 2020 and 2021. During 2021 alone, 166 cyber incidents affecting 162 school districts have been reported nationally.

Why should cybersecurity now be included as an important component of school safety and security strategies? The primary reason hackers see schools as ripe targets is the rich personal information for students, staff and parents that are stored on their systems and the perception that schools have a lot of money. Furthermore, in response to the murder of students and school staff at Sandy Hook Elementary, Marjory Stoneman Douglas High School, Santa Fe High School, Robb Elementary School and unfortunately many others, school administrators, policy makers and state leadership across the county have encouraged the implementation of surveillance cameras, door access control systems, visitor management systems, and other software-based school safety solutions. The digital

nature of these systems makes them vulnerable to cyber-attacks.

Facility securities, such as cameras, monitors, and physical access control systems, are at risk for cyber threats. When schools install surveillance cameras and systems that integrate into their network, the school is open to adversarial, malicious attacks. Surveillance systems create potential entryways into the network; consequently, mitigating these risks requires a comprehensive approach. In the event of a malicious breach, an intrusion can spread through multiple cameras or areas of the network that controls door locks and security systems. Integration of cybersecurity planning enables schools to monitor and block network access from cyber intruders. Cyber attackers can gain access through these devices, however, they can also gain access to school networks in a variety of other ways. As a result, schools must have a comprehensive approach for securing their networks and data that addresses all potential attack vectors.

The most common type of cyber-attack occurring in schools is ransomware, a type of malicious software designed to block access to computer systems and/or publish personal data unless a ransom is paid. As a result of denial of access to student and parent data, schools become unable to continue daily business. According to Comparitech (June 23, 2022), in 2021, 954 schools and colleges were impacted by ransomware. According to Emsisoft, 1043 schools, including 62 school districts, were affected by ransomware in 2021. School ransomware attacks impacted close to 1 million students, with an average downtime of 4.26 days and average recovery time of almost 30 days, and an estimated cost of $3.56 billion nationally (Comparitech, June 23, 2022). For Arkansas specifically, there were three cyber-attacks impacting 8 schools and 9,104 students in 2021.

Of particular concern from the school safety and security perspective, is the unauthorized sharing of personal data for students, teachers, and parents accessed through a ransomware attack. Often personal data obtained through a ransomware attack is shared on the DARK web. This information can be used by online criminals for the purpose of identity theft, but also the information provided may be used to locate and groom victims of youth trafficking as well as victims of a child predator and identify children as targets for bullying and sextortion.

School districts, like institutions of higher education and local governments, are also perceived as being relatively easy targets because they do not yet have the cybersecurity infrastructure in place to protect their information from cyber criminals. According to the National Law Review, “school districts are appealing cyber targets for two main reasons: (1) school districts often have one of the largest budgets in the community, making them an appealing financial target; and (2) the data school districts store includes highly-sensitive student and employee personal information, including Social Security numbers, health information, and other pupil data. This information can be a gold mine to cyber criminals who are interested in identity theft or simply extorting money from a school district.” To

adequately address all these issues, school districts need to establish and maintain constant awareness of both physical and cyber threats.

As school districts focus on implementing cybersecurity best practices, two valuable resources are available to assist them. These resources are free! The National Cybersecurity Preparedness Consortium (NCPC) is a collaboration between the Criminal Justice Institute (University of Arkansas System), University of Texas-San Antonio, University of Texas A&M, University of Memphis and Norwich University. As early as 2004, in partnership with DHS/FEMA, the individual members of the NCPC have developed and delivered no cost DHS/FEMA certified online and face-to-face cybersecurity training courses to an array of states, counties, local jurisdictions and critical infrastructure components nationwide addressing cybersecurity and cyber terrorism concerns. The mission of the NCPC is to provide research-based, cybersecurity-related training and exercises to end users, IT personnel and leaders in local jurisdictions, counties, states and the private sector.

The consortium is organized around the Community Cyber Security Maturity Model (CCSMM) that emphasizes cybersecurity as being the responsibility of the "whole community". The whole community includes the public and private sectors as well as any individual within the community who accesses the Internet or a computer network. More information about the no cost FEMA certified training offered by NCPC is provided in Appendix G. Dr. Cheryl May is Chair of the National Cybersecurity Preparedness Consortium (www.nationalcpc.org) .

The Arkansas Department of Education, Division of Elementary and Secondary Education (DESE), currently provides a host of cybersecurity resources to schools. All the resources listed below are at no cost to the school or district:

- DESE supports a statewide strike team, Arkansas' Cyber Threat Response Team (CTRT). The CTRT is a group of regional IT professionals willing and ready to provide onsite support to whenever an Arkansas school district is faced with a cyber threat. (https://dese.ade.arkansas.gov/Offices/research-and-technology/cyber-threat-response-team)
- A standard data privacy agreement is provided as a template for districts to use and/or adopt to increase vendor accountability and better protect student data. (https://dese.ade.arkansas.gov/Offices/research-and-technology/privacy-awareness/step-2)
- Access to videos, posters, videos, games, and other learning opportunities to engage parents, students, and staff in keeping themselves and our kids safe and healthy online. (www.smactalk.info)

- Tabletop drills and other incident response preparation materials were created to provide districts with a starter kit in developing a cyber incident response plan. (https://dese.ade.arkansas.gov/Offices/research-and-technology/security-awareness/step-3).

Recommendation 1: School districts should require all school personnel, students, and other key stakeholders, such as school board members, who use district digital devices (desktops, laptops, Chromebooks, tablets, mobile phones, smart phones, etc.) to participate in cybersecurity awareness training annually and provide monthly ongoing reminders.

Rationale: According to K-12 SIX, internal and external actors are responsible for cybersecurity incidents. Internal actors include students, administrators, teachers and school board members who are not informed of how to avoid cyber incidents. Tech-savvy students without proper controls in place can disrupt or cause harm to others by inappropriately accessing and compromising school IT systems. As we see more and more students become integrated into a highly digital world, the threat of these potential actors will only continue to increase. Individuals are the weakest link in the cybersecurity chain and are susceptible to phishing attacks, social engineering schemes, etc. that can provide a gateway to malware being installed on vulnerable systems. To diminish these risks, cybersecurity awareness training is critical. While numerous states like Alabama, Colorado, Florida, Louisiana, Nebraska, Ohio, Texas, Pennsylvania, and West Virginia have laws or regulations requiring cybersecurity awareness training for all state employees, Arkansas does not.

According to the 2022 School Safety Assessment, only 21% of school districts reported that all staff have received basic cybersecurity awareness training. Because all staff and school stakeholders (including school board members) are regular users of technology and consequently, potential targets of cyber attacks, all stakeholders must receive cybersecurity awareness training on an ongoing basis. While there is no national standard identifying the frequency at which cybersecurity awareness training should be required for existing staff, all federal agencies, including the Cybersecurity and Infrastructure Agency (CISA), require all staff to take cybersecurity awareness training at least annually. At a minimum, the following topics should be covered: phishing, malware, strong and complex passwords, wifi, identity theft, online safety, and cybercrime[4]. Cybersecurity awareness training should also be required for all new hires within a very short period of time of onboarding. All schools should document when staff have completed the required training.

Quality cybersecurity training and awareness resources are openly available at no cost. The National Cybersecurity Preparedness Consortium (NCPC) provides free web-based, virtual and in-person cybersecurity classes specifically designed for end users, IT personnel and

[4] https://www.cisa.gov/publication/cisa-cybersecurity-awareness-program-toolkit

leaders. NCPC has free cybersecurity awareness online courses designed for end users. Two such web-based courses are *Cybersecurity in the Workplace* (2 hours; AWR-395W) and *Cybersecurity for Everyone* (4 hours; AWR-397W). Both are awareness level courses suitable for staff, but *Cybersecurity for Everyone* focuses on mobile devices and the Internet of Things (IoT). These free courses can be accessed on the NCPC website, www.nationalcpc.org. Districts can also opt-in to engage with DESE's free security awareness software that provides monthly phishing campaigns to assess a district's vulnerability to a phishing attack. Reports are provided regularly to monitor progress. DESE also provides security awareness videos and posters for use with school staff or students (https://dese.ade.arkansas.gov/Offices/research-and-technology/security-awareness/step-4).

In addition, educational service cooperatives (ESCs) employ a full time tech coordinator to serve the technology demands of the schools in their regional area. Each ESC Tech Coordinator can provide face-to-face security awareness training in their regional areas. According to the 2022 School Safety Assessment, of those districts making cybersecurity awareness training available for staff, 73% of the districts indicate this training is provided by district IT staff. The cybersecurity knowledge and experience of IT personnel across districts varies. Therefore, it is strongly encouraged that IT staff who do provide cybersecurity awareness training complete cybersecurity professional development. The NCPC offers the free online course, *Cybersecurity Fundamentals*. This course is designed specifically for IT personnel. Completing *Cybersecurity in the Workplace* and *Cybersecurity for Everyone* is also highly recommended. Other more advanced NCPC courses designed for IT personnel can be found at www.nationalcpc.org .

Cyber criminals change their tactics often. Therefore, it is also important that reminder cyber hygiene training and information about identified threats be made available on at least a monthly basis for all school stakeholders (leaders, teachers, staff, students, IT personnel, school board members) that use district digital devices. The Arkansas Division of Elementary and Secondary Education (DESE) provides a monthly security awareness newsletter, Security Awareness Insider, which provides cybersecurity tips and short training videos. In response to national or local cyber threats, special alerts are also provided through the Insider. Anyone can subscribe to these newsletters (https://arkansas.us18.list-manage.com/subscribe?u=3005d9da8e578c221bac88abf&id=bdca0c1c1a). However, it is recommended that district IT personnel be responsible for distribution of this newsletter to the staff in their schools.

Recommendation 2: School Districts should implement best practices in cybersecurity preparedness.

Rationale: The risk of cybersecurity incidents continues to increase for school districts across the country. On September 6, 2022, the FBI and CISA released a joint cybersecurity advisory for the education sector, especially K-12 institutions, concerning ransomware attacks by Vice Society actors. While this advisory identifies school districts with "limited cybersecurity capabilities and constrained resources" as most vulnerable, even large school districts with sufficient resources to develop a strong cybersecurity posture are vulnerable, as evidenced by the ransomware attack of the Los Angeles United School District (LAUSD) over the Labor Day weekend. While the LAUSD was well-prepared, the cyberattack still resulted in numerous challenges for them to overcome.

In addition to requiring annual cybersecurity awareness training for all end users, best practices in cybersecurity preparedness should include effective processes to back up all critical data, update and patch software immediately, manage passwords, authenticate authorized users and encrypt critical data. Each of these cybersecurity preparedness best practices will be discussed below.

- Data back-up: Ransomware has become a very lucrative criminal activity because the organizations that become victims of these attacks do not have at least a recent back-up of data critical to fulfilling their operational missions. According to Comparitech (June 23, 2022), the average downtime and recovery time for schools and colleges that were victims of ransomware in 2021 was 4.26 days and 29.73 days, respectively. The only way to protect school districts from losing valuable and sensitive student, staff and parent data and to ensure continued services is to conduct regular back-ups of all important data. Data back-up should, ideally, be conducted daily. Having these data stored off-site is critical so that, in the case of a network compromise, backed-up data is secure in an independent network. Off-site data back-ups are also crucial in the case of fire or a natural disaster that might physically damage a school's network.

  According to the 2022 School Safety Assessment, 86% of the responding school districts (241) indicated that they routinely back-up data and test for accuracy of the backed-up data. However, 48% of districts indicated these back-ups are stored on-site. On-site back-up is acceptable ONLY if a copy of the data is ALSO stored off-site. Having only an on-site data back-up system is unacceptable because the backed-up data are not secure in case of a network breach, fire or natural disaster. Data back-ups can be stored off-site using a Cloud service or by having an independent server at a physically different location. Unless organizations are extremely proactive in identifying and mitigating cyber threats, data should be backed up and maintained for different time intervals. Unfortunately, malware infections are far too often unrecognized until months after the initial infection. Consequently, if back-ups are accomplished daily and over-ride the previous data,

the data being saved may also contain the malware. Therefore, it is recommended that data be backed up at different time intervals. To the best of our knowledge, there are no free services available to provide off-site back-up services.

It is also important to ensure the integrity of all data back-ups. Testing the accuracy of backed-up data should be conducted regularly, i.e., quarterly, bi-annually or at least annually and if done appropriately, can discover any potential malware.

- Software Patches and Updates: Software patches and updates are typically conducted in response to identified vulnerabilities. New software vulnerabilities are continually emerging and are exploited by cyber criminals. Therefore, it is critically important that software patches and updates are installed by IT personnel immediately when they become available. A log documenting when software patches and updates are installed can provide a means for leadership to ensure these procedures are being accomplished by IT personnel in a timely fashion.

- Passwords: School district leadership and IT personnel should ensure that strong passwords are used by all individuals using district digital devices. Using strong passwords can prevent unauthorized access to electronic accounts and devices. Two of the most common passwords used are "password" and "123456". These are very weak passwords and should never be used. Best practices in password creation include randomness, uniqueness (all online accounts should have a different password) and length (the longer the better). School districts should train all users of digital devices and accounts to have complex passwords. Ensuring authorized access to accounts also requires that passwords change frequently. If an organization identifies persistent cyber threats, passwords should be changed immediately for all stakeholders having access to district digital devices.

- Multi-Factor Authentication (MFA): Multi-factor authentication (MFA) is a security technology that requires multiple methods of identity verification for users and provides an additional layer of defense against unauthorized access to accounts. Passwords can be easily compromised depending upon the tools available to cyber criminals. According to Microsoft, users who enable MFA are significantly less likely to get hacked. Even if a password is compromised, bad actors will be unable to meet the second authentication requirement to gain access. Many enterprise solutions, such as Microsoft 365 and Google, provide organizations the ability to implement MFA within the existing suite of business tools.

- Encryption: School districts should encrypt data and other end-point devices. Encryption sends messages in code, and the only person who can decode the

message is the person with the correct key. This is especially important for sensitive data. Emails can be intercepted and encryption ensures that the information cannot be hacked to slow or derail emergency response putting emergency responders and the public at risk. Data encryption can be difficult and expensive to implement.

- Limit Account Access: Account access and permissions are limited to specific job functions only. When accounts are not limited, an unexpecting staff member may execute harmful software onto the network, an employee from within may use their access to attack the organization from the inside, or loose permissions can be exploited by cyber criminals. Limiting individual permissions limits the potential for damages when an account is compromised.

- Secure Email Gateway (SEG): Districts should invest and implement a secure email gateway (SEG) software solution since email is the primary target used by hackers to obtain access to an organization's private data. A SEG acts as a filter between users, their email, and the internet. The SEG filter will scan incoming email for malicious software.

Recommendation 3: Establish a basic statewide school information sharing program for cybersecurity incidents and threats.

Rationale: Information sharing is an essential component of any basic cybersecurity preparedness program. The Arkansas legislature passed Act 260 in 2021, requiring that a public entity, or contractual provider of a public entity, disclose in writing an initial report of the known facts to the Legislative Auditor within five (5) business days after learning of the cybersecurity incident. However, it is uncertain whether this information is shared with key stakeholders. Sharing of information about potential cybersecurity threats is essential for effectively defending against cybersecurity risks and incidents. Consequently, it is highly recommended that school districts also be required to report cybersecurity threats and incidents to the Arkansas Division of Elementary and Secondary Education (DESE). As appropriate, DESE should share information about cybersecurity threats to school districts across the state. Responsive and timely communication provides DESE with the proper intel for analyzing statewide trends, assessing the threat, and relaying information to the appropriate stakeholders.

All school districts should also become a member of the U.S. DHS/CISA Multi-State Information Sharing and Analysis Center (MS-ISAC). MS-ISAC membership is free and provides a variety of no-cost cyber services to schools aimed at preventing and defending against potential cybersecurity risks (https://learn.cisecurity.org/ms-isac-registration). MS-ISAC's free services also includes cybersecurity incident response to state, local, tribal and territory (SLTT) communities, including school districts, and malicious domain blocking and

reporting (MDBR) that proactively blocks network requests from known harmful web domains. MDBR does not require any additional hardware or software.

Recommendation 4: School Districts should implement routine vulnerability scanning and testing.

Rationale: A critical element in preventing and defending against cybersecurity risks and incidents is the identification of weaknesses in the organization's network security, computers, servers and databases or flaws in software. To protect the organization from breaches and exposure of sensitive data, vulnerability scanning can detect and classify weaknesses and flaws and once identified, these vulnerabilities can be managed or eliminated. Vulnerability scanning is automated and should be done on a regular basis, i.e. weekly.

FREE vulnerability scanning is available to school districts through the Cybersecurity and Infrastructure Security Agency (CISA). Scans are conducted weekly and are accompanied by a report identifying any weaknesses or flaws that need to be addressed to reduce the risk of a cyber attack. To request these FREE services, send an email to vulnerability@cisa.dhs.gov with "Requesting Cyber Hygiene Services" in the subject line. According to CISA, once the request is received, scanning will start in several days and initial reports will be received by the organization in about two weeks. These reports should be used to manage any identified vulnerabilities.

In addition to vulnerability scanning, web application scanning, phishing campaign assessments and penetration testing should also be done, if practicable. Web application scanning is used to identify bugs and weaknesses in publicly accessible websites, while Phishing campaign assessments are conducted to determine the effectiveness of cybersecurity awareness training by identifying how susceptible staff are to phishing attacks. Phishing attacks account for a substantial percentage of successful cybersecurity breaches each year and are the primary gateway for ransomware attacks. FREE web application scanning and phishing campaign assessments are also conducted by CISA, with requests being made through vulnerability@cisa.dhs.gov .

Penetration testing is a simulated cyber attack on the organization's digital systems that is done to evaluate how secure the system is and identify potential weaknesses that could be exploited by a hacker. Penetration testing is not vulnerability testing and should only be done by well-trained and trusted personnel. The National Cybersecurity Preparedness Consortium, through CJI's Cyber Defense Initiative, has developed *Cybersecurity Proactive Defense*, a four-day instructor-led course focusing on penetration testing skills, defense analysis techniques, real-time response and threat mitigation steps. More information about this course, including prerequisites, can be found at

www.cybersecuritydefenseinitiative.org .

Recommendation 5: School Districts should Implement Third-Party Risk Management best practices to mitigate cyber threats.

Rationale: A third party is an entity that provides a product or service directly to you and/or an entity critical to maintaining your daily operations and can include partners, consultants, vendors, suppliers, and trusted non-profit and government partners. Third-party risk management is the act of identifying and addressing any type of risk (for example, financial, fraud, or cyber) that's associated with third-party entities.[5]

Between 2018 and 2019, security breaches increased by 11%, with a 67% between 2014 and 2018. A 2020 report noted that third parties were responsible for two of every three data breaches.[6] A 2022 annual report on K-12 cybersecurity indicates that 55% of K-12 data breaches are vendor-related and include third-party contracts with surveillance cameras and open-source software applications commonly used by schools.[7]

School districts should vet each vendor to ensure that all contracts with third-parties include data-sharing agreements and disclosures of any past cyber breaches. Third-party vendors should include suppliers, partners, contactors, or service providers.[8] Data breaches are becoming more common with several rising to national news. An example of a large-scale third-party data breach was with Target Corporation in 2013. Bad actors were successful because an employee of one of Target's Third Party HVAC vendors opened a phishing email and obtained credentials to breach Target's gateway server. Target paid $18.5 million in settlement claims[9] In this case, the HVAC vendor had more access to Target's networks than they needed. More recently, in January 2022, a New York City public school vendor's cyber breach jeopardized personal information for some 820,000 current or former school students.[10]

Additionally, External Dependency Management (EDM) assessments should be completed

---

[5] Third-Party Cyber Risk Management For Dummies®,
CyberGRX Special Edition
Published by
John Wiley & Sons, Inc.

[6] https://cybersecurity.att.com/blogs/security-essentials/third-party-risk-management-explained

[7] https://static1.squarespace.com/static/5e441b46adfb340b05008fe7/t/6228bfe3f412c818293e16e1/1646837732368/StateofK12Cybersecurity2022.pdf

[8] *Third Party Risk Management for Dummies (2022)*. John Wiley & Sons, Inc., Hoboken, New Jersey.

[9] https://www.nbcnews.com/business/business-news/target-settles-2013-hacked-customer-data-breach-18-5-million-n764031

[10] https://www.k12dive.com/news/data-breach-exposes-820k-new-york-city-students-information/621352/#:~:text=UPDATE%3A%20June%202%2C%202022%3A,in%20the%20nation's%20largest%20district.

as a component of third-party risk management. EDM establishes appropriate levels of controls to manage the risks that originate from or are related to an organization's dependence on external, or third-party, entities. To conduct an EDM assessment, the Cybersecurity and Infrastructure Security Agency (CISA) provides a free assessment framework and guide that includes utilizing a collaborative team approach with IT security planning and management staff, IT operations staff who manage configuration, leadership for continuity of operations plan in the district, and legal.[11] School district personnel can use the assessment by itself and as the first step in an improvement effort. The EDM Assessment focuses on the relationship between technology, facilities, and information and evaluates how to manage risks when using third-party services. The self-assessment evaluates how well a School District vets third-party vendors, how ongoing relationships with third-party vendors are managed, and how plans for managing breaches and incidents related to third-party vendors are managed.[12]

Recommendation 6: School Districts should develop a Cybersecurity Component within their Continuity of Operation Plans.

Rationale: Continuity of Operation Plans (COOP) are essential to ensure a district can continue to provide services due to natural or man-made disasters. A cyber-attack on the district can cause significant disruption for all of the following but not limited to: classroom instruction, phones, video cameras, automated door locks, HVAC systems, and bus location services. The ability to respond quickly to a cyber breach reduces the negative impact related to spreading of viruses, data loss, public image, instructional time, and potential physical security threats. A continuously updated and rehearsed Incident Response Protocol helps school districts to respond quickly to cyber breaches, thereby ensuring continuity of operations, security, and instruction. To this end, schools and districts should conduct annual table-top drills that include leadership, IT personnel, and key stakeholders to evaluate and be ready to implement their existing Incident Response Protocol. Samples of table-top drills, Incident Response Protocol, incident reports, and incident logs are available through DESE for districts to customize and reproduce as needed for getting started.

District and school leadership, Department of Information Systems K-12 field techs, members of ADE's Cyber Threat Response Team, law enforcement, forensic investigators, etc., need the ability to intervene quickly when a district is under attack and/or the technology director is inaccessible. In order to assist these agents in case of a breach, school districts should maintain an updated Site Notebook as part of their Incident Response Protocol. A Site Notebook should include information that is critical to maintaining the district's technology environment and include proper data mapping. Site notebooks

[11] https://www.cisa.gov/publication/external-dependencies-management-downloadable-resources
[12] https://www.cisa.gov/publication/external-dependencies-management-downloadable-resources

should be stored in a secure location as part of the district's continuity of operations and should be accessible by the superintendent and/or their designee.

District Incident Response Protocols should also include a communication plan to all school stakeholders (parents, students, school personnel, legal, law enforcement) in the case of a cyber breach. By communicating transparently with stakeholders, schools and districts can protect the individuals whose information has been breached, retain public credibility, and potentially obtain additional information about the suspected source of the cyber-attack. As part of this communication plan, districts should also provide direction and guidance for stakeholders on reporting potential cyber threats and breaches to the district.

Recommendation 7: School districts should ensure that particularly IT staff and leadership remain current and up to date in cybersecurity best practices.

Rationale: As a result of the constantly changing tactics, strategies and tools being used by cyber attackers as well as the development of new tools to respond to, mitigate and recover from ever evolving cyberattacks, it is critically important for all school staff to remain cyber knowledgeable and IT personnel to continuously enhance their cybersecurity skills. Cybersecurity is a field that has both extremely technical and very basic aspects to it. It is not possible to have a single, or even just a few courses provide all the knowledge individuals will need to know in order to effectively defend their systems and respond in the event of a cyberattack. IT/security administrators, end users and leaders all need different training and different levels of training. Multiple courses for each are required to ensure adequate knowledge to prevent, respond to and recover from cyberattacks. Furthermore, there are currently at least 500,000 open, unfilled cybersecurity positions in the United States alone. While academic programs like the ones at UA-Pulaski Tech and UA-Little Rock are offering degrees in cybersecurity and producing qualified graduates, they cannot, in the immediate future graduate enough students to meet the need in Arkansas. Consequently, individuals without cybersecurity education are being asked to perform many duties related to defending an organization's system from cyberattacks. Having access to cybersecurity training is critical in enhancing the cybersecurity knowledge and skills of the current workforce.

The National Cybersecurity Preparedness Consortium (NCPC), through funding from DHS/FEMA, offers FREE online and in-person cybersecurity training designed for end users, IT personnel and leadership. NCPC offers awareness, performance and management and planning level courses. Available courses can be found at www.nationalcpc.org. The most recent NCPC brochure is included in Appendix G. To maximize the number of NCPC in-person courses that can benefit Arkansas, the Criminal Justice Institute (a founding member of NCPC) is working to develop more NCPC certified instructors in Arkansas. In addition, NCPC is working to increase the number of these in-person courses which can also be

delivered virtually.

The U.S. DHS's Cybersecurity and Infrastructure Security Agency also provides FREE training on cybersecurity incident response (https://www.cisa.gov/incident-response-training) including cyber range training events and a series of one-hour webinars focusing on the cybersecurity topics such as ransomware, indicators of compromise, log management, web and email server attacks and creating a network map.

Audits, Emergency Operations Plans and Drills

Recommendation 1: Every campus must have a school safety coordinator, who is a part of the district school safety security team.

Justification: To clarify Recommendation 2 of 2018, as well as to include recommended duties of school safety security coordinators. Any individual who has interest in security and safety and risk management can obtain the position of school safety coordinator, e.g., school principal, campus custodian, etc., or other staff person designated by the principal. The school safety coordinator reports to the school principal, as the ultimate, primary individual responsible for building security remains with the principal and the school safety coordinator is assigned to the district safety and security team. School Safety Coordinator duties include conducting security audits, reviewing emergency operations plans, coordinating with law enforcement, fire, and emergency medical services during a campus event. The school safety coordinator is also responsible for tornado, fire, and earthquake lockdown drills under the direct authority and supervision of the school principal. The school safety coordinator should be trained through the Safe Schools Coordinator Academy and the school safety coordinator should be familiar with incident command through FEMA courses like ICS 100.

The FEMA ICS 100 Course, which is a free, basic course on incident command that provides a basic level of understanding and not intended to make safety coordinators emergency management experts. Regarding the School Safety Coordinator Academy, Dr. May shared that in the 2018 Arkansas School Safety Report, the 2018 Commission recommended that a school safety coordinator should be on every campus. Subsequently, in 2019, the Criminal Justice Institute (CJI) received a grant from the Bureau of Justice Assistance, which included the development and delivery of a course for school safety coordinators, which can be regionalized and starts in the Fall. Moreover, the school safety coordinator would be critically important in setting and maintaining the school safety culture and compliance for staff.

Recommendation 2: Security assessments must be conducted every three years using SITE ASSESS.

Justification: As it is required in the new laws that were passed, school districts are required to conduct a comprehensive school safety assessment every three years; however, the assessment, specifically the physical security of the assessment, varies by school district. The U.S. Department of Education has an excellent program, SITE ASSESS, which is also advocated by the National School Safety Clearinghouse (https://www.schoolsafety.gov/), which is part of the Cybersecurity and Infrastructure Security Agency. The subcommittee determined that there exists a need to standardize the way schools conduct the school safety assessment. The SITE ASSESS Program is free of charge. The SITE ASSESS Program is high quality, free of charge, and training resources are available through the Arkansas Center for School Safety. Thanks to the efforts of a small group of administrators and SROs lead by Superintendent Jeff Collum, an-Arkansas Specific version of SITE ASSESS has been developed. Additionally, the School Site Safety Assessment and Audit course will be changed from six (6) hours to four (4) for the convenience of school district staff attendance.

Recommendation 3: Schools should conduct routine, and unannounced safety checks, at least monthly, to evaluate safety and security policies and procedures.

Justification: This recommendation is to combat the issue of the culture of non-compliance demonstrated at Uvalde, related to their safety and security policies and procedures. Moreover, Uvalde had the correct safety and security procedures in place but failed to practice them. Therefore, the idea of the recommendation is that someone, potentially the school safety coordinator or school principal, or someone at the school, conduct regular audits. Specifically, physically checking to ensure exterior doors are locked when they should be, that classroom doors are closed and locked, staff and visitors are wearing ID badges, double-checking the visitor logs, checking to ensure cameras are appropriately working, and immediately address issues, if any. In addition to the monthly checks, school officials should conduct more frequent informal safety checks as part of school and classroom visits such as evaluations, hall monitoring, or other routine school business. Importantly, implementing this recommendation will help to create a culture of compliance.

Recommendation 4: Requires the school district and law enforcement

agency having jurisdiction over the local school district to conduct a full-scale critical incident exercise every three years. In addition, school districts should conduct tabletop exercises and lockdown drills at least annually.

Justification: To clarify the difference between a full-scale exercise and a normal lockdown drill. Requires a school district and law enforcement agency having jurisdiction over the local school district to conduct a full-scale active shooter exercise every three years. They are the most time consuming activity in the exercise continuum in our multi-agency, multi-jurisdictional efforts, in which all resources are deployed. This type of exercise is meant to test the specific plans of the whole community; they test collaboration among the agencies and participants, public information systems, community systems and equipment, emergency operation center is established by either law enforcement or fire services, and the Incident Command System (ICS) is activated. Participants include school staff, fire EMS, the local Office of Emergency Management (OEM), and other law enforcement agencies. Student participation is not required.

Require school district, law enforcement agencies to conduct an active shooter tabletop exercise every year, which are small group discussions that walk through the scenario and the courses of action in the school that a school will need to take before, during, and after an emergency to lessen the impact on the school community. The activity helps assess the plan and resources and facilitates and understanding emergency management and planning concepts. Participants include leadership from school staff, fire EMS, OEM, and other law enforcement agencies. Student participation is not required. The findings from these discussion-based exercises dictate what needs to be tested or stressed during the full scale.

Require school campuses to conduct annual lockdown drills, similar to tornado, fire, earthquake, etc., with student participation. As Acts 620 and 648 require annual lockdown drills, the recommendation is reduced to two recommendations in one.

Recommendation 5: To implement Community Emergency Response Team (CERT) training in Arkansas high schools.

Justification: In order to enhance school safety and resiliency in the event of an emergent event, either natural or manmade, it is the recommendation of this committee to establish FEMA-approved Community Emergency Response Team (CERT) training in the high schools. This training is designed to deliver immediate on-scene care and assistance to victims within the facility and prior to the arrival of professional responders. These CERT teams would be composed of a faculty or other designated staff advisor and a minimum of six high school students. The training would be provided as part of an appropriate curriculum offering such as a Health Science class or the ROTC program. The CERT

curriculum can be linked to existing student groups and does not have to be a separate program. Students who successfully complete the training would be qualified to serve on the CERT Response Team. The team would be outfitted with "CERT Responder Bags" that would include safety equipment for the responder as well as first aid and other response equipment.

The CERT teams can be a component of an overall campus Youth Safety Council composed of a staff advisor and student representatives from each high school grade level. The purpose of this Youth Safety Council would be to promote individual and community preparedness and safety initiatives for the school as well as the community as a whole. The Youth Councils can be a part of an existing youth group and do not have to be a separate organization.

Recommendation 6: To prepare for, respond to, recover from and mitigate threats to our schools it is our recommendation that every county has a full-time, qualified, and resolute local Emergency Manager.

Justification: The County Emergency Manager will work with local school districts to help prepare, respond, recover and mitigate threats. They assist the school districts on full-scale exercises, and tabletop exercises. The local Emergency Management Director is the conduit between local needs and state and federal resources during times of natural and manmade disasters. With a noticeable increase in these events across the state as well as an increase in daily duties and requirements being placed on the County Emergency Managers from countywide stakeholders, it is recommended that every county have a full-time, qualified, and resolute Emergency Manager. Currently, partial funding for the County Emergency Managers comes from federal funding in the form of an Emergency Management Performance Grant (EMPG), which may fluctuate year to year and is not a guarantee in years to come. By adequately funding the County Emergency Managers through dedicated and sustainable funding we will ensure that every county in the state, regardless of economic status is receiving a similar level of service in regards to their readiness levels, ability to coordinate with exercises and develop comprehensive preparedness plans.

Law Enforcement and Security

Recommendation 1: Campuses should always have an armed presence when staff and children are attending class or a major extracurricular activity.

This recommendation replaces the 2018 Commission Law Enforcement and Security Recommendation 1.

The Arkansas School Safety Commission continues to maintain that ideally, every campus/building where staff and students are present should have a School Resource Officer present. However, due to a number of factors (financial constraints of school districts and law enforcement agencies, as well as statewide staffing shortages in law enforcement) we encourage schools to consider other recommendations as presented in our 2018 report to achieve layering and redundancy.

The intent of the Arkansas School Safety Commission is to have armed security within each building (e.g., elementary, middle, junior high, senior high, etc.). Based on past events, armed responders located within school buildings reduces the time an active shooter has to freely target the innocent. To facilitate a rapid response, school districts should carefully consider the location of armed responders within its school buildings. Along with location, providing for the redundancy of armed responders cannot be over emphasized. Redundancy facilitates there never being a lapse in armed security during the school day. Having more than one armed responder within a building also increases the likelihood of quickly stopping the assailant.

With initial reports and anecdotal evidence, most school districts have an armed presence, however, not on every school campus. If there is an armed presence, it is periodically interrupted due to the school resource officer having responsibilities elsewhere in the district, or other responsibilities within the community that remove them from the school. (See Recommendation 5 for methods to help with layering and redundancy). There is also preliminary evidence that over the past four years, since the first report was released, school districts have increased the armed security, with the number of SROs increasing from 315 in 153 districts to 460 in 233 districts in 2022.

When reflecting upon the Uvalde, Texas school shooting, it is possible that had armed security personnel been inside the school when the attack began, the shooter may have been thwarted, perhaps before ever entering the school. The Commission believes very strongly that an armed responder in every school building is a must, and the best practice is to have more than one. School districts have multiple options to explore in their efforts to provide their students with armed security. Because of past efforts, schools can now choose

from, school resource officers (provided by city police or institutional police departments or county sheriff departments) or commissioned school security officers (CSSO). CSSO can be private security or school employees (such as coaches, maintenance directors, administrators, educators, etc.) that have been certified by the Arkansas State Police to carry a gun on campus. As in our 2018 final report, the 2022 Commission continues to strongly recommended that if CSSOs are used as a viable option for redundancy that schools require CSSOs to be given standard psychological exams, participate in random drug screening and regularly train with local law enforcement. Based on the results of the 2022 School Safety Assessment, there are 87 school districts using a total of 528 CSSOs. Unfortunately, 60% of districts using CSSOs have not adopted the enhanced requirements recommended by the Commission.

Recommendation 2: The Arkansas School Safety Commission recognizes Advanced Law Enforcement Rapid Response Training (ALERRT) as the standard active threat response training required for all law enforcement officers and commissioned school security officers in Arkansas.

The ALERRT center at Texas State University is one of the most widely accepted active attack programs in the nation. ALERRT was created at Texas State University in 2002 as a partnership between Texas State University, the San Marcos, Texas Police Department and Hays County, Texas. By 2013, ALLERT at Texas State was named as the National Standard in Active Shooter Response Training by the FBI.

Since 2002, ALERRT has been awarded more than $72 million in state and federal grant funding. The program has trained more than 130,000 law enforcement and fire personnel nationwide in force-on-force scenario-based training. The ALLERT program is also responsible for training over 200,000 in the Civilian Response to Active Shooter Events (CRASE) Avoid-Deny-Defend awareness program.

The ALERRT program is data driven and research based. The staff uses in-depth after-action lessons learned through partnerships with agencies who have been involved in some of the most highly published events related to active shooter situations. ALERRT established a criminal justice research department to evaluate and enhance the overall understanding of active attack events and assist in improving best practices.

Numerous state and federal agencies have accepted the ALERRT curriculum as their standard active shooter training. These states include, Texas, Mississippi, Alabama, Oklahoma, Iowa, Louisiana, Maryland, Georgia and Virginia. In addition, the New York Police Department, San Antonio Police Department, Miami Police Department, Memphis Police Department and the Atlanta Police Department are some of the major cities to adopt ALERRT as their standard. (Information obtained from the ALERRT website).

The Federal Bureau of Investigation has also accepted ALERRT has their standard of active attack training. In each of the 56 domestic field offices there are FBI Special Agent ALEERT trainers. During the past 18 months, the FBI Little Rock Field Office has trained approximately 1,000 people in the civilian response aspect of ALERRT training (CRASE). In addition, all FBI Special Agents and professional support staff are required to receive ALERRT training.

Based on the Uvalde event and the Robb School Report it should be noted that the ALERRT training program addresses most of the leadership and tactical failures identified.

The Level 1 basic course is the backbone of the law enforcement instruction and is designed to prepare the law enforcement officer to isolate, distract and neutralize an active shooter. The course covers shooting and moving, threshold evaluation, concepts and principles on team movement, setting up for and conducting room entries, approach and breaching areas, improvised explosive devices, and post engagement priorities of work. The course utilizes force-on-force scenarios as proof of instruction concepts. If these principles had been used in the Uvalde incident the outcome may have been much different.

In 2018, ALERRT merged the three primary first responder disciplines (Police, Fire, and EMS), and developed an integrated response that includes emergency medicine, coordinated command centers, stronger local, regional, state and national response preparedness and processes.

With the addition of the integrated response system the ALERRT program is now a three-prong approach in providing active shooter event survival skills. They teach law enforcement the approach of stop the threat prior to anything else, they provide a civilian response course that teaches our civilian populace the skills to survive from the time the active attack starts until law enforcement officers neutralize the threat and the integrated response system that allows for immediate on-site lifesaving procedures.

Additionally, ALERRT provides specific training in the following areas;

1. Active Shooter Incident Management- the course provides an overview of the incident command systems and the specific way to use the processes to integrate various stakeholders in the first hour of response to an active attack.

2. CRASE- this training platform focuses on civilians and is frequently requested by schools, businesses and hospitals. The civilian response to active shooter events provides resources in how to act if they are confronted with an active shooter event.

3. Civilian Response and Casualty Care-This course combines the civilian response to an active shooter with the Stop the Bleed Campaign, which empowers civilians to provide life saving medical aid before first responders ever arrive.

4. Breaching- the training provides hands on training to aid the first responder in approaching and breaching crisis site using traditional and non-traditional methods. The class discusses manual and ballistic breaching tools to gain immediate entry into a structure under extreme circumstances that demand immediate entry to save and protect lives.

5. Exterior Response to Active Shooters Events- The course is designed to prepare law enforcement for an open-air active attack encounter. It addresses tactics and techniques to be used in an exterior environment with and armed aggressor.

6. First Responder Medical- This is a train the trainer course that delivers a Tactical Medical for Patrol Officers course of study. This is a critical component in immediate life saving measures.

7. Solo Officer Rapid Deployment- the course provides the solo officer with knowledge, skills and mind set on how to isolate, distract, or neutralize an armed threat like an active shooter.

ALERRT provides the most comprehensive instructional approach to the active attack event as any program in the nation. ALERRT is funded through the Department of Justice Bureau of Justice Assistance and is the most widely accepted active shooter program in our region and on a national platform. The State of Arkansas currently has over 400 certified ALERRT trainers who can provide immediate instruction in the majority of the eight ALERRT platforms.

A key component to the ALERRT training program is that other than the equipment needed to conduct the training for the instructors all classes are free of charge to law enforcement and civilian entities.

Rule 10.5 of the Phase III training, as required by the Arkansas State Police for Commissioned School Resource Officers (CSSO), requires that sixteen (16) hours of active shooter training be provided to all new CSSOs. After the initial sixty (60) hours of training, CSSOs must annually receive twenty-four (24) hours of refresher or renewal training. Four (4) hours of ALERRT or similar training is a requirement of the refresher training, Rule 10.13. ALERRT active shooter training, or an approved equivalent, is the current required format as stated in Rule 10.5 of the Department of Arkansas State Police Rules for Licensing and Regulation of Private Investigators, Private Security Agencies, Alarm Systems Companies,

Polygraph Examiners, and Voice Stress Analysis Examiners. The School Safety Committee's recommendation is that ALERRT be made the sole training program for CSSO's sixteen (16) hour active shooter response training block under Rule 10.5, and the four (4) hour training block under Rule 10.13. The rationale behind this recommendation is to ensure all CSSOs have received the same uniformed training that is also being recommended as the standard for the responding law enforcement agencies. By utilizing ALERRT as the standard active threat response training across our state we believe the coordination between CSSO's and the multiple responding law enforcement agencies will be enhanced. By requiring the use of ALERRT as the training platform for all armed personnel responding to an active school threat, the failure of the responders to immediately and properly engage an assailant should now be eliminated.

Recommendation 3: School Resource Officers should have instant access to certain equipment in the event of an active killer situation.

Each officer should have within their "Go Bag", at a minimum, the following items:

- Level 4 Body Armor
- Ballistic Helmet
- Forcible Entry Tools
- Medical First Aid Trauma Kits

Each campus should also have one ballistic shield, one set of level 4 body armor, one ballistic helmet, breaching tools and additional 1st aid kits for easy access by Law Enforcement Officers (LEOs) or Commissioned School Security Officers (CSSOs) in the event of an incident. The CSSOs should receive proper instruction in the use of all listed items.

It is imperative that officers assigned to serve in our schools be equipped with up-to-date tools to be used when called upon to respond to an active killer. Upon review of the Virginia Tech attack where the attacker chain-locked a door, not having the right equipment to mitigate those circumstances created a lengthy delay in engaging the suspect. Also, in Uvalde, Texas, even though the door was unlocked, LEOs believed it to be locked and precious time was wasted trying to locate breaching tools. We've seen in recent school attacks, suspects are using assault rifles and other high-powered weapons. Consequently, there is a need to give first responders instant access to ballistic shields and helmets to protect themselves as they engage the attacker(s). Sadly, we've learned that in attacks at Sandy Hook, Virginia Tech, Uvalde, and other incidents, those that were not killed instantly, bled to death as they await trauma treatment. Consequently, having medical trauma kits is vital.

Recommendation 4: All school districts that have a Commissioned School Security Officer (CSSO) program should establish communications with the city and/or county law enforcement administrators that serve the school district. The district and the agencies should work cooperatively to develop plans that will address the joint response to an active school killer incident.

The Plans should address the following:

- Ensure that there are armed personnel on campus that will respond to an active killer incident.

- Provide the names, photos and information concerning where a school district's armed responders are typically located on campus.

- The school district and local law enforcement agencies should work together to offer training opportunities that would allow school personnel and law enforcement to train together. Joint training within school facilities utilizing ALERRT should be a priority.

- The joint training should address how law enforcement will enter the school buildings and link-up with the Commissioned School Security Officers (CSSOs). It should be made clear to all the CSSOs that when law enforcement officers arrive on the scene, the law enforcement officers will take command. Link-up and command should be based on ALERRT procedures.

- The district and the law enforcement agencies should work together to develop ways that allow for quick identification of CSSOs by visual and auditorial means.

- The school district and primary responding law enforcement agency should develop a means of direct communication via radio, which is to be used only in the event of an active killer incident.

As witnessed in the Uvalde incident initial armed responders were unable to engage the shooter. It was later determined that through the lack of uniform training, protocol and command and control the momentum of the priority of stopping the killing was lost. By creating a standard plan, based on advanced law enforcement rapid response training protocols if someone stops progressing forward to end the threat others on scene will push on in spite of indecision.

Furthermore, by communicating and training with the Law Enforcement Agency of jurisdiction the transition of incident command to law enforcement will be seamless. By providing vital information about CSSOs within the school district and establishing quick identification from protocol, friendly fire incidents can be avoided and valuable time will not

be wasted while trying to engage the killer.

As a final point, communication is paramount between the school district and law enforcement with jurisdiction. A radio (with police department frequency) would create a clear line of communication as the law enforcement agency is responding to an active killer incident.

Recommendation 5: Schools should develop strategies that layer and build redundancy for optimal security.

In 2018 the Commission identified several strategies where law enforcement officers or CSSOs could be utilized in layering and building redundancy. Some of these Include:

- Recruiting former certified law enforcement officers as SROs, as defined by the Arkansas Commission on Law Enforcement Standards and Training, or Commissioned School Security Officers;

- Collaborating with law enforcement and seek ways to increase law enforcement traffic and visibility on campus. For example, the Benton and Bentonville Police Departments have implemented a policy that directs law enforcement officers to conduct safety checks throughout the schools in their jurisdiction. These and other departments have also asked law enforcement officers to park their squad cars in the school's parking lot while they complete reports or visit schools during lunch;

- Using current or retired law enforcement officers as substitute teachers; and/or

- Allocating office space within the school for law enforcement officers to use during the day to complete reports and other administrative tasks.

The Arkansas School Safety Commission has strongly recommended armed security is to be provided for every classroom building. Districts should use multiple officers per site to ensure continuity of protection. This can be achieved by using a combination of school resource officers and commissioned school security officers. If a district and its jurisdictional law enforcement agency is unable to provide continuity of protection with their personnel, the Commission strongly recommends they work with other adjacent agencies to develop strategies that would provide the personnel needed to maintain uninterrupted protection. The 2022 Arkansas School Safety Assessment indicates the number of school districts utilizing CSSO programs have quadrupled since the initial 2018 Commission Report.

Recommendation 6: School Districts should adopt the Advanced Law Enforcement Rapid Response Training, (ALERRT), training and protocols designed for community members that address what to do when confronted with an active attack situation.

The Commission previously recognized ALERRT active attack training be adopted as the standard active attack training for all law enforcement officers in the State of Arkansas. To ensure that training is consistent across the state when dealing with an attack situation we are encouraging school districts to adopt the ALERRT training modules that are designed to incorporate community members. These three modules are the Active Attack Incident Command, Civilian Response to Attack Shooter Events, and Civilian Response and Casualty Care. (Additional training modules may be available in the future.)
The adoption of these training modules will ensure that the primary parties involved in an active attack event are trained to the same standards, processes and are familiar with the same terminology. A standardized training program will allow for mutual understanding of concepts and tactics required to survive, operate, and provide casualty care in an active attack situation.

1. Active Shooter Incident Management- the course provides an overview of the incident command systems and the specific ways to use the processes to integrate various stakeholders in the first hour of response to an active attack.

2. Civilian Response to Active Shooter Events (CRASE) - this training platform focuses on civilians and is frequently requested by schools, businesses and hospitals. The civilian response to active shooter events provides resources in how to act if they are confronted with an active shooter event.

3. Civilian Response and Casualty Care-This course combines the civilian response to an active shooter with the Stop the Bleed Campaign, which empowers civilians to provide lifesaving medical aid before first responders ever arrive.

The Criminal Justice Institute's Arkansas Center for School Safety should be the coordinator and custodian of all non-law enforcement training related to the ALERRT training for school districts.

Mental Health and Prevention

Recommendation 1: DESE and the Arkansas Center for School Safety should collaborate to develop and provide training to schools on analyzing data and creating action plans to effectively address needs related to school climate.

Based on the 2019 School Safety Assessment, 60% of responding schools reported utilizing a school climate survey to assess their strengths and vulnerabilities, and to improve their awareness of potential risk factors related to bullying or other issues that negatively impact school climate. Acts 620 and 648 of 2021 mandate that comprehensive school site safety assessments are conducted by school districts every three years, the first no later than August 1, 2024. Conducting climate surveys is now included as a component of the comprehensive school safety assessment process. However, the 2022 School Safety Assessment demonstrated that only 43% of school districts indicated they have conducted a climate survey in the past 3 years. Data from culture and climate surveys should be the foundation of the development of an action plan for transformation and include action steps for the implementation of evidence-based programs that develop and maintain a positive climate, encourage trauma-informed practices, deter bullying behaviors, and promote social-emotional learning and healthy peer relationships.

It was determined that schools could benefit from supplemental training regarding the action planning process and should include information about ways to analyze data obtained from climate surveys, how to create an action plan to address areas of concern or needs, and how to monitor progress toward identified goals. As stated in the 2021 US Secret Service/Homeland Security report, *Averting Targeted School Violence: A U.S. Secret Service Analysis of Plots Against Schools:*

> "Prevention and early intervention are paramount. The analysis of 67 averted school attack plots contained in this report demonstrates that there are almost always intervention points available before a student's behavior escalates to violence."

The implementation of this recommendation would move Arkansas schools closer to creating cultures that address the needs of all students, thus decreasing the use of punitive disciplinary practices while increasing a more restorative approach. Schools should become bully-free zones that teach positive social behaviors to replace negative ones. The 2020 CDC Youth Risk Behavior Survey indicates that 22.6% of high school students in Arkansas reported being bullied on school property. This percentage is higher than the national average (19.5%). School cultures should be trauma-responsive, helping students to utilize positive coping strategies to navigate through toxic stress. In *Averting Targeted School Violence: A U.S. Secret Service Analysis of Plots Against Schools,* it states:

> These types of "models of early intervention have been widely adopted in the school setting and can work in conjunction with a school's multidisciplinary threat assessment program. Positive Behavioral Interventions and Supports (PBIS) models are one such approach that provides a primary intervention for all students, with secondary and tertiary interventions to support students who may be experiencing distress. These collaborative approaches foster positive school climates and promote student emotional and physical well-being, thereby decreasing the impact of adverse experiences. Approaches that promote successful outcomes for all students will decrease the risk of harm to the school community."

The initial Commissioner's Memo announcing the statewide rollout of the use of Level 1 High-Reliability Schools (HRS) surveys occurred in January of 2019. Level 1 of the HRS framework addresses the factors considered foundational to the culture and climate of a school. These factors include building a safe, supportive, and collaborative environment. In January 2019, Secretary Key, Dr. Marzano, and several others were part of statewide communication to schools about HRS. In addition, every superintendent and principal received a copy of the books, *A Handbook for High-Reliability Schools* and *Leading a High-Reliability School*. Level 1 school climate surveys were provided to every school in the state at no cost. Thus far, there have been two survey windows per school year since that initial launch. In the 2022 School Safety Assessment, only 19% of school districts (47/251) in Arkansas indicated they use HRS. DESE has plans to continue providing access to the climate survey and the score report that would guide action planning through the 2022-23 school year. Arkansas schools also have access to the SHAPE assessment, through DESE's Project AWARE, which is available to help schools assess needs related to the mental health of students, and also provides resources that guide schools in action planning to meet these needs.

Based on the reports/presentations from representatives with DESE regarding current initiatives in Arkansas, such as THRIVE Arkansas, there is significant positive momentum in efforts to support our schools in creating positive, healthy cultures that best support students. As schools seek to build capacity in shifting the culture, they should utilize the resources provided by DESE. It is imperative that support for these initiatives continue so that these necessary efforts do not cease due to the end of a grant or time-limited funding. Supporting DESE in the creation of a state-wide network of support for schools is the best possible outcome to continue this essential work.

Recommendation 2: All school districts should have access to training and ongoing support for the implementation of evidence-based programs that develop and maintain a positive climate, encourage trauma-informed practices, deter bullying behaviors, and promote social-emotional learning (SEL) and healthy peer relationships.

There are multiple and complex risk factors implicated in school violence, ranging from childhood trauma (often including violence or abuse and neglect in the home), impulsivity/lack of self-control, lack of social skills and peer rejection, mental health concerns including suicidality, exposure to media violence and more. While some risk factors may be difficult for schools to influence, there are a variety of interrelated approaches schools can use to build a cohesive and supportive school environment that is designed to reduce these risk factors and increase protective factors in youth. For example, social-emotional learning programs can build important self-regulation/self-control skills as well as social skills such as conflict management, social problem-solving, anger management, and coping with rejection and disappointment.

Trauma-informed care approaches can assist school personnel in understanding and responding to the needs of children with experiences of trauma, increasing the likelihood they will be successful in school. Positive school climate initiatives focus on helping students feel a sense of belonging and can build trust between youth and adults. There is some evidence that restorative justice approaches to discipline can support a positive school climate, as opposed to zero-tolerance policies that run the risk of further marginalizing children already at high risk. Greater awareness of the mental health needs of students and access to mental health supports can support early identification of suicidal youth in school as well as address other mental health needs of high-risk students.

When schools work towards developing a positive culture and climate, the wellness of the staff should be a chief consideration. This stakeholder group is charged with meeting the social and emotional needs of others and, due to this, often experiences symptoms of vicarious trauma. These symptoms can leave staff members feeling overwhelmed. Thus, school districts should ensure staff members have access to meaningful professional learning experiences that assist with being aware of, monitoring, and managing their individual wellness.

In the 2019 School Safety Assessment, 60% of schools identified that they utilize a specific social and emotional learning curriculum in their districts. Arkansas has historically ranked near the top in the nation in regard to the prevalence of bullying in our schools. The 2022 School Safety Assessment revealed that 38% of responding districts indicated they have implemented a positive climate program. Of those districts, 95% reported the program they have implemented supports social and emotional learning and positive peer relationships. For the 62% of reporting schools who indicated they are not implementing a positive climate

program, being unaware of available tools, lack of funding and limited staff resources were the primary reasons cited.

Creating a culture in schools where positive peer relationships are taught and reinforced is a crucial piece of addressing bullying and other harmful behavior in our schools. The Arkansas Division of Elementary and Secondary Education (DESE) has worked to develop innovations that support the work of implementing a positive climate program in schools. To include G.U.I.D.E. for Life (Growth, Understanding, Interaction, Decisions, and Empathy), THRIVE Arkansas, Project A.W.A.R.E (Advancing Wellness and Resiliency in Education), Trauma Resource Initiative for Schools (TRIS), and Collaborative for Academic, Social, and Emotional Learning (CASEL).

Collaborative for Academic, Social, and Emotional Learning (CASEL)

In terms of available national resources, the Collaborative for Academic, Social, and Emotional Learning (CASEL) supports schools in the implementation of social-emotional learning initiatives (www.casel.org). CASEL offers a number of tools for schools seeking to increase social-emotional supports, including The CASEL Guide to SEL programs, which is designed to help educators and school administrators select an evidence-based SEL program that best meets the needs of their community (https://pg.casel.org/). Arkansas school teams can use this tool and related resources to support the quality implementation of well-designed classroom programs and school practices that will support social-emotional learning.

The Commission heard from several high school students who emphasized that early prevention, through teaching students healthy emotional development, key life skills, etc., is a key–yet under-recognized and under-resourced–aspect of preventing violence in schools by promoting and supporting students' mental health from the earliest stages of development. There was also discussion about the stigma associated with mental health issues and seeking treatment in schools. Establishing a culture that promotes the health and wellness of all and confronts stigma is crucial to optimal student mental health.

In summary, it is essential that schools have access to training and support to equip them to develop a positive climate and support the social and emotional needs of all children, including children with experiences of trauma or with emotional and behavioral concerns. It is cause for concern that the key initiatives in the state that provide this support are grant-funded and that the supports provided are therefore time-limited. It is critical that these initiatives receive ongoing support so that this important work can be sustained.

Recommendation 3: All school districts should provide access to training in Youth Mental Health First Aid (YMHFA) for all personnel who interact with students. All districts should also have, at a minimum, one YMHFA trainer, to promote sustainability and ongoing staff development. Additional school personnel training may include Adverse Childhood Experiences (ACEs), Trauma-Informed Schools, Drug-Endangered Children, and Social-Emotional Learning.

According to findings based on the 2018-2019 National Survey of Children's Health (NSCH) and the most recent data from the Behavioral Risk Factor Surveillance Survey (BRFSS), "Arkansas exceeds the national average of children with two or more ACEs — 27.1% in Arkansas vs. 20.5% nationally. The fact sheet also looks at the effects of ACEs: For example, 39% of children ages 10–17 in Arkansas with two or more ACEs are overweight or obese, compared to 37.2% nationally. Also, 41.6% of children ages 6–17 in Arkansas with two or more ACEs are bullied, picked on, or excluded by other children, compared to 34.2% nationally.

In Arkansas, there have been significant gains made since the release of the 2018 Commission recommendations. These include:

- Acts 551 and 622 of 2021 require all school resource officers to complete YMHFA training every four years.
- Acts 620 and 648 of 2021 require all school counselors to complete YMHFA training every four years.
- To date, Arkansas Center for School Safety staff has trained 756 SROs and school counselors.
- DESE's Project AWARE has trained 2500 educators, counselors, and community members in YMHFA

Acts 620 and Act 648 of 2021 implemented a requirement for all school counselors to be certified in YMHFA. The initial certification is required by September 1, 2024, and then at a minimum every 4 years thereafter. Schools are much better equipped to respond to the mental health needs of students when all adults who interact with students are prepared to respond in a supportive and informed way. In the 2022 School Safety Assessment, 47% of school districts responding indicated that 76-100% of their counselors have received this training. However, 59% of responding districts indicated that 0-25% of their staff who interact with students have received this training. 32% of responding districts indicated their staff has been provided training in ACEs, and 42% of responding districts indicated their staff has received trauma-informed schools training.

Among adults nationwide, those who had two or more ACEs are three times more likely to have attempted suicide and four times more likely to consider themselves alcoholics than adults who had no ACEs. The odds of those and other problems are considerably higher for adults who had more than two ACEs."

Feedback has been received from school leadership, who have seen tremendous success in broadening the availability of YMHFA to their staff, and in having district YMHFA trainers for continued growth and sustainability of YMHFA in the culture of their districts. To quote the Director of Mental Health and Behavior Services at Greenbrier Schools,

"Mental Health First Aid (YMHFA), we are providing that knowledge and equipping adults with the skills they need to recognize the signs and symptoms of mental health difficulties early on."

Because there are resources in Arkansas currently that make this training very accessible to schools, and the number of trainers has increased significantly, we feel schools have better access to this training than ever before. The schools that have trained staff beyond those required report a significant benefit for their staff and for their schools. Having school personnel trained in Youth Mental Health First Aid equips them to identify at-risk students and the potential need for services and supports. Earlier identification of needs leads to more quickly connecting students to the support they need.

Recommendation 4: All school staff who regularly interact with students should be required to take, at a minimum, the free online 1-hour Mental Health basic awareness class, "Basic Mental Health Awareness for Educational Staff" on an annual basis, if they have not been certified in YMHFA.

Classified staff interact with students on a frequent basis, and often observe behaviors or situations that may be indicative of more serious needs. However, there is presently no requirement for classified staff to receive any standardized Mental Health awareness training. It is imperative that ALL staff are equipped with basic knowledge of mental health awareness, and that this is a bare minimum way to meet this need. This course is free, and available online through AR Center for School Safety. If classified school personnel complete certification in YMHFA, they would not also be required to take this 1-hour online course in Basic Mental Health Awareness.

Recommendation 5: The AR Center for School Safety should coordinate a planning group to focus on the development and implementation of a statewide school safety anonymous or confidential tip line.

Over the past several years, the Commission Chair and other subcommittee members have investigated and studied models in other states for anonymous or confidential reporting of school safety concerns. The subcommittee evaluated the 2021 report, "School Safety Tip Line Toolkit" (Tip Line Toolkit), which reported that:

1. Just over half (51%) of public middle and high schools in the United States currently have a tipline in operation.
    a) most tiplines are relatively new. Sixty percent have been in operation for less
        i. than 3 years.

2. Principals perceive tiplines as an effective school safety strategy, addressing multiple threats:
    a) seventy-seven percent believed that their tiplines made them more aware of
        i. safety issues at their school.

    b) over 50% said that their schools' tiplines had prevented violent incidents.
    c) two-thirds believed that their tiplines allowed their schools to respond more
        i. effectively to bullying.

    d) seventy-three percent reported that their tiplines had prevented incidents of
        i. self-harm or suicide.

3. Over half of the tiplines are staffed or monitored 24 hours a day, 7 days a week, such that a staff member receives calls, texts, or other entries in real time.

4. Most are described as anonymous rather than confidential.

5. Most schools involve school administrators (89%) and law enforcement officers (56%) in their tipline programs, but only about 25% involve mental health professionals or students as active partners.

6. The most common challenges to operating a school safety tipline include the following:
    a) receiving tips with insufficient information to act on,
    b) raising student awareness and getting students to submit tips – identifying
        i. false or bogus submissions,
    c) receiving tips for situations that are considered out of scope, and
    d) raising community awareness.

Experts emphasized that punitive responses to reported or perceived threats, in contrast, can have the opposite effect, by deterring reporting and further alienating the most

vulnerable, at-risk students and families.

In the 2022 School Safety Assessment, 56% of reporting districts indicated they have a confidential or anonymous reporting system. These districts report that these mechanisms for reporting are 1) in person to a staff person, 2) by email and 3) by text. Of the 56% of districts who indicated the use of a confidential or anonymous reporting system, 16% indicate their system is "extremely adequate" and 53% indicate their system is "somewhat adequate". Those same districts were asked to indicate how effective they feel efforts are to raise awareness about what types of things to report: 35% indicated "very" effective and 49% indicated "moderately" effective.

The Commission heard directly from the state of Oregon regarding its approach to their student safety tip line, called "SafeOregon." The Commission learned that states that have implemented statewide systems required several years of planning, as well as significant and ongoing state funding, to initiate these systems in a sustainable way. In addition, several Arkansas school districts presented information regarding their district-specific approaches to anonymous or confidential reporting. Several barriers were noted to the implementation of such systems, including cost, raising awareness, promoting acceptance, privacy/confidentiality, etc. The Commission learned that school districts who are presently utilizing such systems are interested in the possibility of a statewide solution, whereby school districts could sign up, and participate actively in, the statewide system. In fact, 96% of Arkansas districts responding to the 2022 School Safety Assessment indicated they would be interested in using a state-wide anonymous/confidential tip line.

The role of the Center's Tipline planning group will be to research the most effective approaches to statewide confidential or anonymous school safety tip lines. This statewide tip line should facilitate the ability of Arkansas's students, parents, and community members to anonymously or confidentially report threats to student safety. In addition, the tip line should also serve as a means of support for students with a range of challenges. These might include bullying, harassment, concerns about suicide or self-harm, or other safety-related issues. While the tip line would not serve as a substitute for school counselors or mental health care, the school safety tip line will serve as another layer in a safety net for our students.

Recommendation 6: All school districts that utilize an anonymous reporting system MUST establish a behavioral threat assessment team, following best practices for team composition and process, and require all team members receive basic and advanced behavioral threat assessment training through the Arkansas Center for School Safety.

Having trained behavioral threat assessment teams is best practice in a process focused on identifying and preventing potential incidents that put students and school personnel at risk. For schools that utilize an anonymous or confidential reporting system, having this team not only established but trained according to best practices, is a crucial piece in responding appropriately to reports of potential risks that endanger students and/or school personnel.

Anonymous/confidential reporting systems have a defined process for triaging reports and determining the appropriate recipient of the reported information. For reports that are sent to a designee at the school, there must be a defined process for a response, to ensure that there is an appropriate investigation of the report, assessment of the student about whom the report is submitted, and that all appropriate personnel is involved in compiling relevant information related to the report. Without having a designated behavioral threat team and ensuring that all members of the team have been appropriately trained, crucial pieces of the process may be missed.

Presentations were heard from Fort Smith School District and Springdale School District regarding their anonymous tip lines and behavioral threat teams and processes. Based on a review of the information from districts that have successfully created a mechanism for anonymous or confidential reporting of concerning situations or behaviors at school, along with a defined process for behavioral threat assessment teams and processes, it is recommended that any district using an anonymous or confidential school safety tip line must have appropriately trained behavioral threat assessment teams that meet national best practices for team composition and processes.

Reports conducted by the Secret Service/National Threat Assessment Center consistently support the need for a well-trained, multidisciplinary team to respond to potential behavioral threats. In the above referenced Secret Service report, it states:

“When conducted properly, a threat assessment will involve providing robust interventions and support for students experiencing distress, thereby intervening with and de-escalating situations before they become violent. It should be noted clearly in any school threat assessment policy that the primary objective of a student threat assessment is not to administer discipline or to introduce students into the criminal justice system. While those responses may be necessary at times, especially in situations involving explicit threats, violence, or weapons, the primary objective of a student threat assessment should be providing a student with help and working to ensure positive outcomes for the student and

the community."

Recommendation 7: All school districts should establish a behavioral threat assessment team, following best practices for team composition and process, and require all team members receive basic and advanced behavioral threat assessment training through the Arkansas Center for School Safety.

Behavioral Threat Assessment Team training is currently available at no cost to all schools through the Arkansas Center for School Safety. This training is best practice in Arkansas and is highly recommended for all identified team members. Engaging families in the team and discussing needs can strengthen their engagement and commitment to the treatment process, add accountability, provide an opportunity to share successes and improvements, as well as revise the plan as needed to achieve the best outcomes.

The Commission heard a presentation from Cindy Marble, a former Special Agent with the Secret Service, regarding Behavioral Threat Assessments. She does extensive training regarding assessing threats in schools. She shared the critical pieces of a thorough threat assessment, including identification and definition of the concerning behavior, to determine what causes may be there. This allows identification of needs and intervention prior to threats occurring, which is the best possible outcome. In Cleveland v. Taft Union High School District et al., a 16-year-old high school student shot a fellow student while in class. The shooter was charged and sentenced to 27 years imprisonment. The injured student filed a civil suit against several school officials due to a behavioral threat assessment process that was not conducted appropriately, which involved inadequate response to bullying. The school was found 54% liable, as the threat assessment process did not involve a team, nor was there any recommendation of services for the student. We believe this supports the recommended best practice of designation of a multidisciplinary team, along with training in an approved model of threat assessment and plan development.

Based on the data reviewed, implementation of this recommendation is necessary to decrease the risk to students, and the school district, and increase the likelihood of appropriate response and intervention to help the student identified as a potential risk. Schools must have Behavioral Threat Assessment teams with the appropriate members who are appropriately trained.

Recommendation 8: Coordinated school crisis response teams should be developed at the state, regional, district, and campus levels to ensure effective crisis management and mitigate the negative impact of any traumatic event that involves schools.

This recommendation replaces the 2018 Commission recommendation 6 which discusses a designated process be implemented utilizing trained personnel from across the state. These individuals or teams would be tasked with responding to critical incident events in an organized and efficient manner. While this recommendation is focused on ensuring the training of school personnel, a multi-disciplinary approach to crisis response is recommended, including first responders, EMS, law enforcement, and mental health providers. Schools are encouraged to work with their local community and engage these partners as appropriate to their communities.

Since 2019, staff members from the Arkansas Division of Elementary and Secondary Education (DESE) have researched and reviewed crisis response training models. The National Organization for Victim Assistance (NOVA) was recently designated as the crisis response model which will be utilized to train teams who can provide critical education and emotional first aid training in mass casualty, natural disasters, or other events which impact Arkansas schools and communities. The 2022 Arkansas School Safety Assessment asked schools if a coordinated, statewide crisis response system would benefit their district, and 94% responded “yes”.

The DESE designee should serve as the point of contact collaborating with NOVA personnel, school districts, and other key stakeholders to provide crisis response training and services. NOVA provides disaster relief to victims of crime, victims of mass casualty events, or survivors of natural disasters in the form of crisis response. The goal is to assist victims and survivors to understand and normalize their reactions to increasingly abnormal situations and allow them to begin their physical and emotional recovery.

Crisis response is a key element of fulfilling NOVA’s mission to champion dignity and compassion for those harmed by crime and crisis. Trauma has common reactions but the cause of the trauma, from wide-area natural disasters to multiple victim crimes of violence, have different layers and dimensions. There are organizations that focus on crime victim advocacy and others that deal with disaster relief. NOVA is unique in that it incorporates extensive skill and experience in training a vast network of responders in a broad range of needs that stem from criminal, man-made, and natural crisis victimization.

NOVA'S long-term goal for the continued stabilization of an impacted community entails three primary tasks:

1. Provide direct services through individual and group crisis intervention sessions as well as family companioning during the immediate aftermath of a mass casualty or natural disaster;
2. Assist local officials and other decision-makers to plan for immediate and long-range care, comfort, and assistance for victims, first responders, and survivors within their communities;
3. Train and support local community caregivers who may be called upon to provide long-term assistance to their communities after NOVA has departed, enabling the community to be self-sustainable.

The first NOVA training will be held in the fall of 2022, thanks to a Bureau of Justice Stop School Violence grant awarded to DESE in 2019, with regional crisis response training scheduled to begin in October 2022. Information is being disseminated to school district administrators and key stakeholders within those districts ie: administrators, school counselors, school psychology specialists, school security directors, building and district crisis team leaders, or other personnel designated by the school districts. It should be noted that first responders in Arkansas are also NOVA trained across the state, and may be an additional resource for schools in the event of a crisis. The NOVA community crisis response model has been designated as the primary training process for schools in the State of Arkansas. There are other crisis response models and initiatives currently in place or available which can serve to enhance and expand the skill set of the NOVA-trained responder:

Project A.W.A.R.E (Advancing Wellness and Resiliency in Education)

Project A.W.A.R.E. is a project which supports school districts in efforts to provide mental health care awareness and trauma-informed practices (funded through the Substance Abuse and Mental Health Services Administration AWARE State Education Agency Grant).

PRePARE

The National Association of School Psychologists PRePARE curriculum provides relevant school personnel with comprehensive training on how to establish and serve on school safety and crisis response teams. The training integrates the roles of school staff members and community providers in terms of prevention, protection, mitigation, and response and recovery. Specific components are:

- Prevent and prepare for psychological trauma
- Reaffirm physical health and perception of security and safety
- Evaluate psychological risk
- Provide interventions
- Respond to psychological needs
- Examine the effectiveness of crisis prevention and intervention

It is important to note that the support available to schools in response to traumatic events is available for students and for school personnel. An appropriate, effective crisis response model will not differentiate the need, but offer support to meet the unique needs of all who may be affected.

Recommendation 9: DESE/School Health Services and The Division of Aging, Adult, and Behavioral Health Services (DAABHS) should convene a workgroup to identify and address gaps in current mental health supports for students in Arkansas.

As the needs of students for timely and appropriate mental health services and supports increase across our state and the nation, approximately 10% of schools in Arkansas report they do not have access to mental health services for their students. Despite an increase in telehealth services for treatment over the last few years, many students who need mental health evaluation and treatment still face significant barriers to access. Some of these barriers include workforce shortages in the mental health field, providers struggling to remain financially viable in rural areas, and varying payor-related regulations that create constraints on payment for services delivered in schools.

Potential steps for this workgroup should include: assessing the current state of available student mental health resources, identifying potential mental health-related resources for schools that lack access to mental health services for their students, and facilitating communication between schools and resources available in their areas. Additionally, work may be needed to find solutions to gaps in treatment coverage, ensure that all students in need of mental health services and support have access, and explore the quality of care issues that impact schools.

In discussing the appropriate partners to engage in this work, it is recommended that the group be co-convened and facilitated by a designee from DAABHS and a designee from DESE's School Health Services team. Additional partners should include representatives from behavioral/mental health agencies, Medicaid, Blue Cross Blue Shield, regional prevention agencies, and other partners as appropriate. This is to address the issues from various perspectives - providers, payors, and policymakers should partner with our educational system to ensure that identified gaps are appropriately addressed.

Recommendation 10: Districts should have access to a dashboard or similar system that would facilitate student data analysis for identifying at-risk behaviors, allowing for early intervention that could provide additional academic, social, or emotional support.

Having access to timely, relevant student data supports school personnel in identifying potential at-risk behavior in students. Schools who have a standardized process for gathering and analyzing student data are much more likely to appropriately identify needs and link students to appropriate supports. Not only can these data identify potential needs, they can also inform behavior planning and monitor student success.

Supporting data to consider includes, but is not limited to, attendance issues, behavioral referrals, loss of class credit, failing grades, poor reading skills, or other indicators of impaired functioning or concerning behaviors. School personnel should continue to receive appropriate training and resources to be able to identify and provide needed support for student mental and behavioral health needs.

As stated in the 2019 US Secret Service/Homeland Security report, Targeted School Violence: Protecting America's Schools U.S. Secret Service Analysis of Targeted School Violence, school attackers reported a variety of stressors before carrying out a school attack. Specifically, the report refers to academic and disciplinary stressors as follows:

> "Most attackers (n = 31, 89%) had experienced school stressors related to academic or disciplinary actions, including failing grades and school suspensions. More than half of the attackers (n = 21, 60%) had both academic and disciplinary issues. For seven of the attackers (20%), a disciplinary issue at school was the most recent stressor experienced prior to the attack.
>
> Every attacker included in this analysis (n = 35, 100%) exhibited concerning behaviors prior to their attack. In all but two of these cases (n = 33, 94%), concerning behaviors were displayed at school. Three-quarters of the attackers (n = 27, 77%) displayed concerning behaviors at home or in the community, and about three-quarters displayed them online (n = 26, 74%)."

The Commission encourages schools to use data to provide early interventions for students that would lead to positive outcomes for students. Data should not be used to label or target students in a negative way.

In Arkansas, school districts have access to THRIVE, which provides training and support to districts in implementing a multi-tiered system of support for students with a variety of needs.

The multi-tiered system involves the systematic use of data to most efficiently allocate resources in order to improve learning for all students, through integrated academic and behavioral supports. To ensure efficient use of resources, schools begin with the identification of trends and patterns using school-wide and grade-level data.

THRIVE participants are trained how to use a student dashboard available to everyone in the state at no cost. The training includes navigation through the platform as well as using trend data to determine areas of need for their campuses.

In situations where a Behavior Threat Assessment Team is convened to assess a potentially at-risk student, data found in this dashboard could provide a great deal of important information to guide this critical work.

Appendix A

STATE OF ARKANSAS
EXECUTIVE DEPARTMENT

PROCLAMATION

EO 18-03

TO ALL TO WHOM THESE PRESENTS COME – GREETINGS:

EXECUTIVE ORDER TO ESTABLISH THE ARKANSAS SCHOOL SAFETY COMMISSION

WHEREAS: The Governor has long held school safety as a priority, and he led a national study on school safety in 2012; and

WHEREAS: Recent events involving violence at schools around the country make it necessary for the issue of school safety to be addressed in a comprehensive manner in Arkansas; and

WHEREAS: Crime and violence remain issues in schools nationwide; and

WHEREAS: It is a matter of state importance to provide best practices regarding school safety to our local school districts; and

WHEREAS: Arkansans with backgrounds in education, mental health, and law enforcement possess the necessary expertise to propose and develop workable solutions to the issue of school safety;

NOW, THEREFORE, I, ASA HUTCHINSON, acting under the authority vested in me as Governor of the State of Arkansas, do hereby order the following:

(1) There is hereby created the Arkansas School Safety Commission (the "Commission"), which shall advise the Governor and the Department of Education on school safety across Arkansas.

(2) The Commission shall be composed of members appointed by the Governor and shall serve at the pleasure of the Governor. The chair of the committee shall be designated by the Governor. The Commission shall be composed of:

a) A representative of the Office of the Arkansas Attorney General;
b) The Director of the Arkansas Department of Emergency Management, or his or her designee;
c) A Public School Superintendent;
d) A Public School Teacher;
e) A Public School Counselor;
f) The Director of the Arkansas Division of Public School Academic Facilities and Transportation within the Arkansas Department of Education;
g) An advisor on school security from the Arkansas Department of Education;
h) A County Sheriff;
i) A former Federal law enforcement officer;
j) A Mental Health professional;
k) The Director of the Criminal Justice Institute;
l) The Director of the Arkansas Law Enforcement Training Academy or his or her designee; and
m) Additional citizens, as the Governor deems necessary, to represent the different geographic regions of Arkansas.

(3) The members of the Commission shall have the following duties:

a) To advise the Governor and the Department of Education on school safety across Arkansas;

b) Study and analyze the safety of K-12 schools throughout the state taking into consideration the physical and mental health of students;
c) To study the architecture and construction of school buildings as it relates to the safety of students and staff in those buildings, including prevention and response to active shooter threats;
d) Make recommendations to the Governor and the Department of Education on improvements or changes needed to increase school safety;
e) Consider any and all issues associated with school safety and should undertake school visits, visits with school resource officers, building principals, counselors, superintendents, and others to have a comprehensive view of this topic;
f) Consider assigning subcommittees with directions to consider several topics and report back to the full commission with recommendations to be considered;
g) The initial report and recommendation will be due to the Governor on July 1, 2018, with subsequent reports being submitted by the Chair of the Commission; and
h) The final report of the Commission's findings and recommendations shall be submitted to the Governor no later than November 30, 2018, at which time the work of the Commission will conclude.

(4) Upon request, the Department of Education may provide staff and other personnel to support the work of the Commission.

IN TESTIMONY WHEREOF, I have hereunto set my hand and caused the Great Seal of the State of Arkansas to be affixed the 1st day of March, in the year of our Lord 2018.

Asa Hutchinson, Governor

GREAT SEAL OF THE STATE OF ARKANSAS

Attest:

Mark Martin

Mark Martin, Secretary Of State

Appendix B

2018 School Safety Commission Members

Dr. Cheryl May - Chair
Director, Criminal Justice Institute (CJI)
University of Arkansas System

William Temple - Vice Chair
Retired Special Agent in Charge,
Federal Bureau of Investigation (FBI)

John Kaminar
Security and Lost Prevention Manager
Arkansas Department of Education (ADE)

Brad Montgomery
Director of Public School Academic Facilities and Transportation Arkansas Department of Education (ADE)

A.J. Gary
Secretary, Arkansas Department of Emergency Management (ADEM)

Tim Helder
Washington County Sheriff

Jami Cook
Director, Commission on Law Enforcement Standards and Training (CLEST)

Will Jones
Deputy Attorney General
Special Investigations Unit

Dr. David Hopkins
Superintendent
Clarksville School District

Dawn Anderson
High School Counselor
Hot Springs High School

John Allison
Teacher
Vilonia High School

Tom Jenkins
Chief Rogers Fire Department

Marvin L. Burton
Deputy Superintendent
Little Rock School District

Lori Poston
Child and Adolescent Therapist from Jonesboro

Dr. Margaret Weiss
MD, PHD, UAMS Professor Department of Psychiatry, and Director of Child and Adolescent Psychiatry

Ricky Hopkins
Parent
Prescott School District

Dr. Sterling Claypoole
Professor in Psychology at South Arkansas Community College and Parent of Students in El Dorado School District

Dr. Joyce Cottoms
Superintendent
Marvell-Elaine School District

Appendix C

2018 School Safety Commission Recommendations

Mental Health and Prevention

- Recommendation 1: Every school district should conduct school climate surveys across all campuses, and develop and implement an action plan based on the findings of the school climate survey.

- Recommendation 2: All school districts should implement a positive climate program that deters bullying behaviors, and promotes social-emotional learning and positive peer relationships.

- Recommendation 3: All school districts should provide access to training in Youth Mental Health First Aid for all personnel who interact with students. Additional school personnel training may include: Adverse Childhood Experiences (ACEs), Trauma-Informed Schools, Drug-Endangered Children, and Social-Emotional Learning.

- Recommendation 4: All school districts should establish a behavioral threat assessment team and process.

- Recommendation 5: The Arkansas Department of Education should review roles and responsibilities of school counselors to provide increased time with students for provision of counseling and social-emotional learning, as well as referral to community resources as appropriate.

- Recommendation 6: A coordinated crisis response team should be developed to mitigate the emotional impact of any traumatic event that impacts a district.

Law Enforcement and Security

- Recommendation 1: No campus should ever be without an armed presence when staff and children are attending class or a major extra-curricular activity.

- Recommendation 2: If financially practicable, schools should ideally have at least one SRO for each campus.

- Recommendation 3: School districts should execute a Memorandum of Understanding (MOU) with their partnering law enforcement agency that identifies the roles and responsibilities of SROs and other critical elements.

- Recommendation 4: SROs whose primary assignment is within the schools should receive specialized training.

- Recommendation 5: If a school district authorizes the use of the CSSO program, that policies, protocols, training, and selection go above the minimum standards required, to include standard psychological exams, random drug screening, extensive firearms handling training, and regular training with law enforcement.

- Recommendation 6: Schools should consider strategies that layer and build redundancy for optimal security.

- Recommendation 7: Arkansas's Commission on Law Enforcement Standards and Training (CLEST) should study the feasibility of school districts being allowed to establish their own law enforcement agencies.

Audits, Emergency Operation Plans and Drills

- Recommendation 1: All districts should be required to form District Safety and Security Teams.

- Recommendation 2: Each campus should also designate one current staff member as a School Safety Coordinator.

- Recommendation 3: The ADE's Safe Schools Committee membership should be expanded.

- Recommendation 4: Schools should modify their fire drills to include additional time for the teacher to evaluate the situation by looking, listening and observing prior to evacuating their classrooms.

- Recommendation 5: Comprehensive school safety assessments should be required to be conducted every three years and reviewed by the school board and school administration.

- Recommendation 6: School nurses and staff should be trained in efforts that enhance the emergency medical response within schools.

Intelligence and Communications

- Recommendation 1: Each school district should support, establish, and maintain a comprehensive, common communication plan to be utilized by school officials, students, parents, law enforcement, and other stakeholders.

- Recommendation 2: School districts should have systems that enable direct communication with local law enforcement.

- Recommendation 3: School districts, in collaboration with local and other law enforcement agencies, should implement and expand strategies to promote reporting, to include anonymous reporting, of suspicious activity/behavior and threats.

- Recommendation 4: Students, staff, and parents should be educated on how to recognize and report signs of at-risk behavior and potential threats.

- Recommendation 5: An analysis should be conducted to determine how the Arkansas State Fusion Center (ASFC) could be more effectively utilized to receive and disseminate information pertaining to threats against schools. In addition, the ASFC could provide timely and relevant information to schools and other appropriate entities pertaining to school safety.

Physical Security

- Recommendation 1: State agencies should work with the federal Readiness and Emergency Management (REMS) for Schools Center Training Assistance Office, to develop a customized, state-level school bus safety initiative for use by districts, schools, and transportation offices.

- Recommendation 2: State leaders should engage the Arkansas congressional delegation and other federal partners to encourage the U.S. Department of Education to allow Title IV formula block grants to include use by schools for infrastructure improvements to support safe and healthy schools, including physical security remedies.

- Recommendation 3: Districts should create an online facility profile within a panic button alert system for each new campus or facility in the district and conduct annual reviews to update facility profiles where needed.

- Recommendation 4: Districts should review and assess the efficacy of upgrading any old style "crash bar" exterior door egress hardware with the newer "touch bar" type exit devices.

- Recommendation 5: Prior to installation or contracting to installation of temporary door barricade devices designed to preclude intruders from entering any classroom or learning space of a school building, information pertaining to the project should be uploaded into DPSAFT's web-based project submission tool for review.

- Recommendation 6: The state's Academic Facilities Partnership Program should be revised to allow districts to submit eligible campus safety and security upgrade projects for state financial assistance.

2022 School Safety Commission Recommendations

General Commission Recommendations

Recommendation 1: A school safety unit should be formed in the Division of Elementary and Secondary Education to better ensure school districts are appropriately implementing school-safety related laws, provide support to districts in the implementation of school safety recommendations and assist schools in identifying gaps and needed resources to fill these gaps.

Recommendation 2: The Arkansas legislature should consider recurring funding for school districts to implement the Arkansas School Safety Commission Recommendations.

Recommendation 3: Additional funding should be provided to the Arkansas Center for School Safety in order to build the capacity of the Center to provide training and resources to assist school districts and law enforcement agencies meeting school safety related laws and recommendations.

Recommendation 4: School districts should be required to include the implementation status of the Arkansas School Safety Commission recommendations in their annual report to the public.

Recommendation 5: The Division of Elementary and Secondary Education's Safe Schools Committee should investigate the feasibility of developing a school safety award/recognition program for school districts that incentivizes the implementation of the Arkansas School Safety Commission recommendations.

Physical Security

Recommendation 1: The legislature should change the language in Arkansas *Code§ 12-13-109* to "keep all exiting doors and classroom doors closed and locked during school hours, with the exception of transition times. No person shall be impeded from building egress per the current State Fire Prevention Code and the ADA Standards for Accessible Design."

Recommendation 2: Districts should, at a minimum, install electronic access controls for high-frequency-use exterior doors.

Recommendation 3: District campuses should have security cameras that are accessed by

designated individuals, including law enforcement, during a critical incident.

Recommendation 4: District campuses should have one secure visitor point of entrance with ideally a secured vestibule, when allowable.

Recommendation 5: All exterior doors to school buildings must remain closed and locked.

Recommendation 6: Require district campuses to use a visitor management system.

Recommendation 7: All classroom doors to school buildings must remain closed and locked.

Recommendation 8: All school districts should utilize a grand master key system ensuring that each campus has a master key.

Recommendation 9: Every district should provide master key(s) access to local law enforcement for use during a critical incident.

Recommendation 10: District campuses need to protect any glass that allows vision or access into the classroom from the corridor.

Recommendation 11: District campuses should use covers on vision panels on classroom doors during lockdowns that also allow students a blind area to 'hide'.

Recommendation 12: District campuses should equip classroom doors with locks so that doors can be locked from the inside, allow for access from outside for authorized personnel, and allow for egress per the current State Fire Prevention Code and the ADA standards for accessible design.

Recommendation 13: Add physical security items to existing Division of Public School Academic Facilities and Transportation's *(DPSAFT)* Maintenance & Operations facility inspection checklist.

Recommendation 14: Dedicate at least 20 minutes of Division of Public School Academic Facilities and Transportation's (DPSAFT) 3-hour required annual bus driver training to bus security.

Recommendation 15: Any doors on district campuses that have faulty locks must have a high priority work order entered immediately and the faulty locks must be repaired/replaced immediately.

Recommendation 16: District campuses should have shatter resistant film at school entrances, especially the main entrance.

Recommendation 17: District campuses should have physical barriers such as bollards,

landscaping, fencing, low walls, etc. at school entrances, especially the main entrance.

Recommendation 18: District campuses should have corresponding numbers on classroom interior and on exterior surfaces (wall, door, or window) easily identifiable to first responders so that they can reference position of students and/or intruders.

Intelligence and Communications

Recommendation 1: School Districts should develop layered two-way communication access between staff members and administrative staff via various platforms to ensure information sharing and improve alert processes.

Recommendation 2: School Districts should develop capabilities to monitor communication platforms, on school owned devices, to include social media outlets as it relates to threats or triggering phrases used by potential active attack suspects.

Recommendation 3: Law enforcement agencies are encouraged to develop educational programs and build relationships within their communities to encourage reporting and to identify suspicious activity by those with the intent to commit harm.

Recommendation 4: Law enforcement should coordinate with school districts to ensure that there is limited access to existing law enforcement communication network, (radio systems) for critical incidents. We recommend for new radio systems that are being developed by law enforcement to consider the school district as part of their initial buildout. Radio system use should be allowed with limited use during critical incidents only and be restricted to certain school administrators and staff.

CYBERSECURITY

Recommendation 1: School districts should require all school personnel, students, and other key stakeholders, such as school board members, who use district digital devices (desktops, laptops, Chromebooks, tablets, mobile phones, smart phones, etc.) to participate in cybersecurity awareness training annually and provide monthly ongoing reminders.

Recommendation 2: School Districts should implement best practices in cybersecurity preparedness.

Recommendation 3: Establish a basic statewide school information sharing program for cybersecurity incidents and threats.

Recommendation 4: School Districts should implement routine vulnerability scanning and testing.

Recommendation 5: School Districts should Implement Third-Party Risk Management best practices to mitigate cyber threats.

Recommendation 6: School Districts should develop a Cybersecurity Component within their Continuity of Operation Plans.

Recommendation 7: School districts should ensure that particularly IT staff and leadership remain current and up to date in cybersecurity best practices.

Audits, Emergency Operations Plans and Drills

Recommendation 1: Every campus must have a school safety coordinator, who is a part of the district school safety security team.

Recommendation 2: Security assessments must be conducted every three years using SITE ASSESS.

Recommendation 3: Schools should conduct routine, and unannounced safety checks, at least monthly, to evaluate safety and security policies and procedures.

Recommendation 4: Requires the school district and law enforcement agency having jurisdiction over the local school district to conduct a full-scale critical incident exercise every three years. In addition, school districts should conduct tabletop exercises and lockdown drills at least annually.

Recommendation 5: To implement Community Emergency Response Team (CERT) training in Arkansas high schools.

Recommendation 6: To prepare for, respond to, recover from and mitigate threats to our schools it is our recommendation that every county has a full-time, qualified, and resolute local Emergency Manager.

Law Enforcement and Security

Recommendation 1: Campuses should always have an armed presence when staff and children are attending class or a major extracurricular activity.

Recommendation 2: The Arkansas School Safety Commission recognizes Advanced Law Enforcement Rapid Response Training (ALERRT) as the standard active threat response training

required for all law enforcement officers and commissioned school security officers in Arkansas.

Recommendation 3: School Resource Officers should have instant access to certain equipment in the event of an active killer situation.

Recommendation 4: All school districts that have a Commissioned School Security Officer (CSSO) program should establish communications with the city and/or county law enforcement administrators that serve the school district. The district and the agencies should work cooperatively to develop plans that will address the joint response to an active school killer incident.

Recommendation 5: Schools should develop strategies that layer and build redundancy for optimal security.

Recommendation 6: School Districts should adopt the Advanced Law Enforcement Rapid Response Training, (ALERRT), training and protocols designed for community members that address what to do when confronted with an active attack situation.

Mental Health and Prevention

Recommendation 1: DESE and the Arkansas Center for School Safety should collaborate to develop and provide training to schools on analyzing data and creating action plans to effectively address needs related to school climate.

Recommendation 2: All school districts should have access to training and ongoing support for the implementation of evidence-based programs that develop and maintain a positive climate, encourage trauma-informed practices, deter bullying behaviors, and promote social-emotional learning (SEL) and healthy peer relationships.

Recommendation 3: All school districts should provide access to training in Youth Mental Health First Aid (YMHFA) for all personnel who interact with students. All districts should also have, at a minimum, one YMHFA trainer, to promote sustainability and ongoing staff development. Additional school personnel training may include Adverse Childhood Experiences (ACEs), Trauma-Informed Schools, Drug-Endangered Children, and Social-Emotional Learning.

Recommendation 4: All school staff who regularly interact with students should be required to take, at a minimum, the free online 1-hour Mental Health basic awareness class, “Basic Mental Health Awareness for Educational Staff” on an annual basis, if they have not been certified in YMHFA.

Recommendation 5: The AR Center for School Safety should coordinate a planning group to focus on the development and implementation of a statewide school safety anonymous or confidential

tip line.

Recommendation 6: All school districts that utilize an anonymous reporting system MUST establish a behavioral threat assessment team, following best practices for team composition and process, and require all team members receive basic and advanced behavioral threat assessment training through the Arkansas Center for School Safety.

Recommendation 7: All school districts should establish a behavioral threat assessment team, following best practices for team composition and process, and require all team members receive basic and advanced behavioral threat assessment training through the Arkansas Center for School Safety.

Recommendation 8: Coordinated school crisis response teams should be developed at the state, regional, district, and campus levels to ensure effective crisis management and mitigate the negative impact of any traumatic event that involves schools.

Recommendation 9: DESE/School Health Services and The Division of Aging, Adult, and Behavioral Health Services (DAABHS) should convene a workgroup to identify and address gaps in current mental health supports for students in Arkansas.

Recommendation 10: Districts should have access to a dashboard or similar system that would facilitate student data analysis for identifying at-risk behaviors, allowing for early intervention that could provide additional academic, social, or emotional support.

Appendix D

STATE OF ARKANSAS
EXECUTIVE DEPARTMENT

PROCLAMATION

EO 22-09

TO ALL TO WHOM THESE PRESENTS COME – GREETINGS:

EXECUTIVE ORDER TO RECONVENE THE ARKANSAS SCHOOL SAFETY COMMISSION

WHEREAS: On March 1, 2018, pursuant to EO 18-03, Governor Hutchinson created the Arkansas School Safety Commission (the "Commission"), which advised the Governor and the Department of Education on school safety across Arkansas; and

WHEREAS: The Commission provided a final report on November 30, 2018, which outlined findings and recommendations to improve school safety throughout the state; and

WHEREAS: Schools across Arkansas have implemented many of the recommendations found in the Commission's Final Report, including but not limited to, conducting school climate and culture assessments, implementing positive climate programs, providing access to training in Youth Mental Health First Aid for personnel, ensuring that school districts have armed personnel present when staff and children and present, employing at least one School Resource Officer, forming District Safety and Security Teams, designating a staff member as a School Safety Coordinator, and many others; and

WHEREAS: Crime and violence remain issues in schools nationwide; and

WHEREAS: On May 24, 2022, an armed intruder entered Robb Elementary School in Uvalde, Texas, and murdered over 20 people, including 19 students aged 11 or under and two educators, and injured countless others; and

WHEREAS: It is crucial that the state remain informed of the status of school safety and ensure that school districts are properly equipped to prevent tragic events such as the one that occurred in Uvalde; and

WHEREAS: It is a matter of state importance to provide an updated analysis of best practices regarding school safety to our local school districts; and

NOW, THEREFORE, I, ASA HUTCHINSON, acting under the authority vested in me as Governor of the State of Arkansas, do hereby order the following:

(1) There is hereby reconvened the Arkansas School Safety Commission (the "Commission"), which shall advise the Governor and the Department of Education on the status of school safety across Arkansas.

(2) The Commission shall be composed of members appointed by the Governor and shall serve at the pleasure of the Governor. The chair of the committee shall be designated by the Governor. The Commission shall be composed of:

a) A representative of the Office of the Arkansas Attorney General;
b) The Director of the Division of Emergency Management within the Arkansas Department of Public Safety, or his or her designee;
c) A Public School Superintendent;
d) A Public School Teacher;
e) A Public School Counselor;
f) The Director of the Arkansas Division of Public School Academic Facilities and Transportation within the Arkansas Department of Education;
g) An advisor on school security from the Arkansas Department of Education;

h) A County Sheriff;
i) A former Federal Law Enforcement Officer;
j) A Mental Health professional;
k) The Director of the Criminal Justice Institute;
l) The Director of the Arkansas Law Enforcement Training Academy, or his or her designee; and
m) Additional citizens, as the Governor deems necessary, to represent the different geographic regions of Arkansas.

(3) The members of the Commission shall have the following duties:

a) Review the Commission's Final Report published in November 2018;
b) Provide an update on the status of school safety across Arkansas;
c) Update the analysis of the safety of K-12 schools throughout the state, taking into consideration the physical and mental health of students;
d) Determine which findings and recommendations from the previous report have not been remediated or achieved;
e) Identify any new recommendations of best practices in school safety that have developed since the Commission's Final Report in November 2018;
f) Submit an initial report and recommendations will be due to the Governor on August 1, 2022, with subsequent reports being submitted by the Chair of the Commission; and
g) Submit the final report of the Commission's findings and recommendations to the Governor no later than October 1, 2022, at which time the work of the Commission will conclude.

(4) Upon request, the Department of Education may provide staff and other personnel to support the work of the Commission.

IN TESTIMONY WHEREOF, I have hereunto set my hand and caused the Great Seal of the State of Arkansas to be affixed the 10th day of June, in the year of our Lord 2022.

Asa Hutchinson, Governor

Attest:

John Thurston, Secretary of State

Appendix E

2022 Commission Members

Dr. Cheryl May – Chair
Director, Criminal Justice Institute
University of Arkansas System

Arkansas Attorney General Leslie Rutledge
Arkansas Attorney General, or her designee

Secretary A.J. Gary
Division of Emergency Management
Arkansas Department of Public Safety

Dr. David Hopkins
Superintendent,
Clarksville School District

Donna Wilchie
School Counselor,
Conway School District

Tim Cain
Director, Division of Public School Academic Facilities and Transportation
Arkansas Department of Education

Crystal Green-Braswell
Office of Coordinated Support and Services, Division of Elementary and Secondary Education
Arkansas Department of Education

Tim Helder
Sheriff, Washington County

Bill Temple
Retired Special Agent,
Federal Bureau of Investigation

Dr. Laura Dunn
Director,
UAMS Psychiatric Research Institute

Secretary Jami Cook
Director, Arkansas Law Enforcement Training Academy
Secretary, Arkansas Department of Public Safety

John Allison
Teacher, Vilonia High School

Marvin Burton
Principal, Little Rock School District

Chris Chapmond
Chief, Hot Springs Police Department
President, Arkansas Association of Chiefs of Police

Patricia Gann
Deputy Director, Division of Aging, Adult, and Behavioral Health Services
Arkansas Department of Human Services

Bill Gossage
Deputy Chief of Staff, External Operations, Governor's Office

Linda Graham
School Psychologist,
Nettleton School District

Dr. Mike Hernandez
Executive Director, Arkansas Association of Educational Administrators

Bill Hollenbeck
Chief of Police, Fort Smith Public Schools

Ricky Hopkins
Parent, Prescott School District

Tom Jenkins
Chief, Rogers Fire Department

Lori Poston
Vice President of Clinical Services,
Northeast Region, Arisa Health

Courtney Salas-Ford
Chief Legal Counsel, Division of
Elementary and Secondary Education
Arkansas Department of Education

Paula Stone
Assistant Director, Children's Services,
Division of Aging, Adult, and Behavioral
Health Services
Arkansas Department of Human
Services

Joe Duboise
Training Supervisor,
Central Arkansas Law Enforcement
Training Academy

Members assigned to each subcommittee

Mental Health and Prevention

Ms. Lori Poston-Chair
Dr. Cheryl May
Ms. Crystal Green-Braswell
Dr. Laura Dunn
Ms. Patricia Gann
Ms. Linda Graham
Ms. Paula Stone
Ms. Donna Wilchie

Audits, Emergency Operation Plans and Drills

Secretary A.J. Gary-Chair
Dr. Cheryl May
Chief Tom Jenkins
Dr. David Hopkins
Mr. John Allison
Dr. Mike Hernandez
Director Tim Cain

Law Enforcement and Security

Sheriff Tim Helder-Chair
Dr. Cheryl May
Mr. Bill Temple
Chief William Hollenbeck
Dr. David Hopkins
Chief Chris Chapmond
Mr. John Allison
Attorney General Leslie Rutledge

Intelligence and Communications

Chief Chris Chapmond-Chair
Secretary Jami Cook-Former Chair
Dr. Cheryl May
Secretary A.J. Gary
Mr. Bill Gossage
Attorney Courtney Salas-Ford
Ms. Patricia Gann
Mr. Marvin Burton
Mr. Joe Duboise
Mr. Bill Temple

Physical Securities

Director Tim Cain-Chair
Dr. Cheryl May
Ms. Donna Wilchie
Dr. Mike Hernandez
Mr. Ricky Hopkins
Chief William Hollenbeck
Sheriff Tim Helder

Subject Matter Experts

Mental Health

Dr. Nikki Edge
Dr. Betsy Kindall
Superintendent Scott Spainhour
Ms. Judy Lattimore

Audits, Emergency Operation Plans and Drills

Superintendent Jeff Cullum
Dr. Bethany Swindell
Assistant Chief Bubba Jones
SRO Phil Blaylock
Mr. Bo Robertson
Mr. Erik Wright
Mr. Chad Johnston

Intelligence and Communications

Mr. Ray Girdler
Dr. Angela Kremers
Dr. Erin Finzer
Mr. Mark Kirby

Law Enforcement and Security

Assistant Chief Bubba Jones
Dr. Nancy Anderson

Physical Security

SRO Phil Blaylock
Mr. Ron Self
Mr. Clayton Vaden
Mr. Nathan Alderson
Mr. Tyrel Pace
Mr. Jason Black
Dr. Nancy Anderson

Appendix F

Non-Commission Member Presenters

Ms. Cindy Marble
Former Special Agent for the Secret Service
Topic: Behavioral Threat Assessment
June 28, 2022

Mr. Chad Johnston
Protective Security Advisor-Arkansas, Region VI, DHS/CISA
and
Mr. Mark Kirby
Cybersecurity State Coordinator-Arkansas, Region VI, DHS/CISA
Topic: Department of Homeland Security (DHS)/Cybersecurity and Infrastructure Security Agency (CISA) Security Programs
July 5, 2022

Ms. Hope Worsham
Elementary and Secondary School Emergency Relief (ESSER) Director
Arkansas Department of Education
Topics: THRIVE AR and SmartData Dashboards
July 5, 2022

Mr. N'nambi Islam, Little Rock Southwest Magnet High School
Ms. Mary Emily Wrzensinski, Hamburg High School
Mr. Webb Storer, Jonesboro High School
Topic: Students' Perspective on School Safety
July 19, 2022

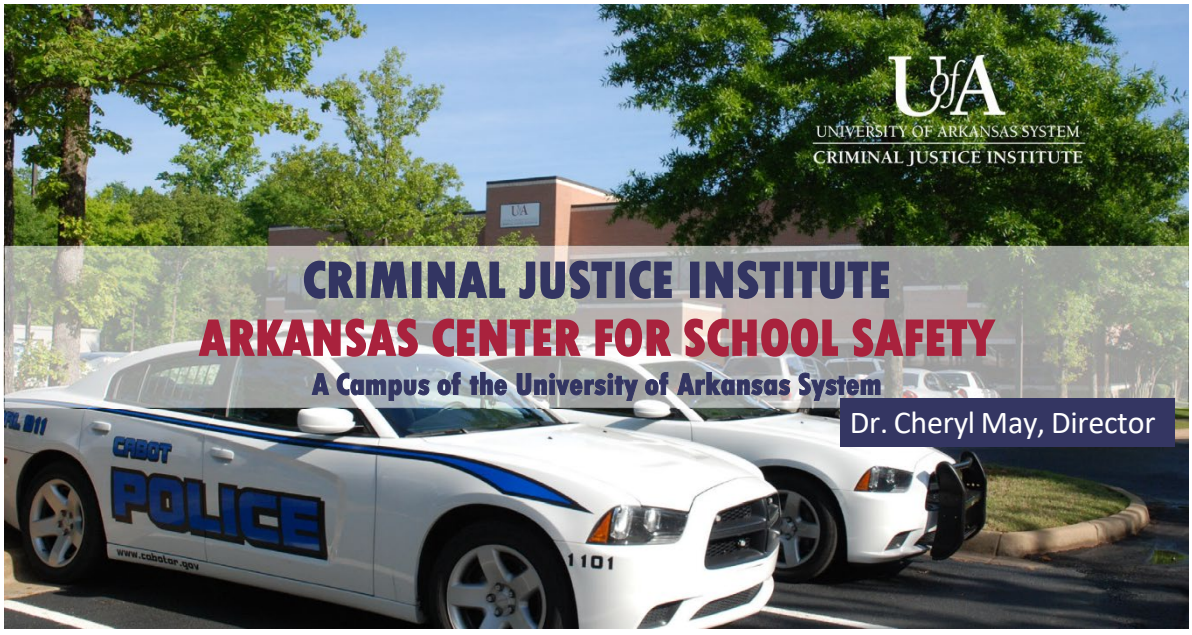
Ms. Dee Blackwell, Fort Smith School District
Ms. Elizabeth Vazquez-Rodriguez, Stuttgart School District
Mr. Scott Erwin, Perryville School District
Ms. Charlene Kirk, Little Rock School District
Topic: School Safety Perspective of Parents
August 30, 2022

Commission Member Presenters

Dr. Cheryl May, Director
Criminal Justice Institute
Topic: 2018 Arkansas Recommendations (30)
June 14, 2022
Topic: Arkansas Center for School Safety
June 21, 2022

Sheriff Tim Helder, Washington County
Chief Chris Chapmond, Hot Springs Police Department/President, Arkansas Association of Chiefs of Police
Topic: Advanced Law Enforcement Rapid Response Training (ALERRT) Uvalde Report
July 12, 2022

Appendix G



UofA
UNIVERSITY OF ARKANSAS SYSTEM
CRIMINAL JUSTICE INSTITUTE

AR Center for School Safety

- CJI Has a Long History of Providing School Safety Training and Resources for Arkansas
  - National School Safety Resource Center 2002
  - SRO and Educational Staff Training 2009 COPS
  - 2014 ADE Safe Schools Committee Reconvenes
    - Recommended Formation of the Arkansas Center for School Safety
- MOU Between CJI and ADE 2017
- 2019 Base Funding for CJI/ACSS from Governor Hutchinson and Legislators

2

UNIVERSITY OF ARKANSAS SYSTEM
CRIMINAL JUSTICE INSTITUTE

AR Center for School Safety

- 2019 Received BJA Grant with Focus on Behavioral Threat Assessments and School Safety Coordinator Academy (BBTA, ABTA, Toolkit, Policy)
- 2021 Act 620 & 648 Identified as State School Safety Clearinghouse with Governor Appointed Advisory Board and included private schools

- School Safety Programs-Online
  - School Site Safety Assessment (3hrs)
  - Autism Spectrum Disorders (7hrs)
  - Basic Mental Health Awareness (1hr)
  - Identifying and Preventing Bullying (3hrs)
  - Active Killer Response for Educators (2hrs)
  - Intro to Behavioral Threat Assessment (1hr)

3

UNIVERSITY OF ARKANSAS SYSTEM
CRIMINAL JUSTICE INSTITUTE

AR Center for School Safety

- School Safety Programs-Online
  - SRO Roles and Responsibilities (3hrs)
  - SRO Roles and Responsibilities for Admins (1hr)
  - Intro to Human Trafficking for Educators (2hrs)
  - Basic Mental Health Awareness for Educational Staff (1 hr)

4

UNIVERSITY OF ARKANSAS SYSTEM
CRIMINAL JUSTICE INSTITUTE

AR Center for School Safety

- School Safety Programs-In Person
  - Addressing and Preventing Adult Sexual Misconduct (7hrs)
  - Advanced School Threat Assessment (7hrs)
  - Suicide Prevention for Schools (6hrs)
  - Basic Behavioral Threat Assessment (7hrs)
  - Civilian Response to Active Shooter Events (4hrs)
  - Expect Respect: Promoting Healthy Relationships (6hrs)
  - Juvenile Takeover of Social Media (4hrs)
  - Planning, conducting and Analyzing EOPs (7hrs)
  - Resilience Strategies for Educators: Self Care and Peer Support (4hrs)

5

UNIVERSITY OF ARKANSAS SYSTEM
CRIMINAL JUSTICE INSTITUTE

AR Center for School Safety

- School Safety Programs-In Person
  - School Site Safety Assessments & Audits (6hrs)
  - Solo Engagement Response to an Active Killer (18hrs)
  - SRO Basic (40hrs)
  - SRO II Intermediate (28hrs)
  - SRO Refresher (16hrs)
  - Standard Response Protocol (John Michael Keys-8hrs)
  - Strategic Communications for Interacting with Juveniles (6hrs)
  - The Bully, the Bullied and the Not so Innocent Bystander (6hrs)
  - Understanding Juvenile Law (7hrs)
  - Youth Mental Health First Aid (8hrs)

6

UNIVERSITY OF ARKANSAS SYSTEM
CRIMINAL JUSTICE INSTITUTE

AR Center for School Safety

- 17th Annual AR Safe Schools Conference
  - July 18-20, 2022
  - ACSS
  - Arkansas Safe Schools Association
  - Governor's Office
  - Arkansas Division of Elementary and Secondary Ed
  - Arkansas Attorney General

7

UNIVERSITY OF ARKANSAS SYSTEM
CRIMINAL JUSTICE INSTITUTE

AR Center for School Safety

- SRO Certificate Levels
  - Level I: Basic SRO
  - Level II: Intermediate SRO
  - Level III: Advanced SRO
  - Level IV: Senior SRO

8

UNIVERSITY OF ARKANSAS SYSTEM
CRIMINAL JUSTICE INSTITUTE

AR Center for School Safety

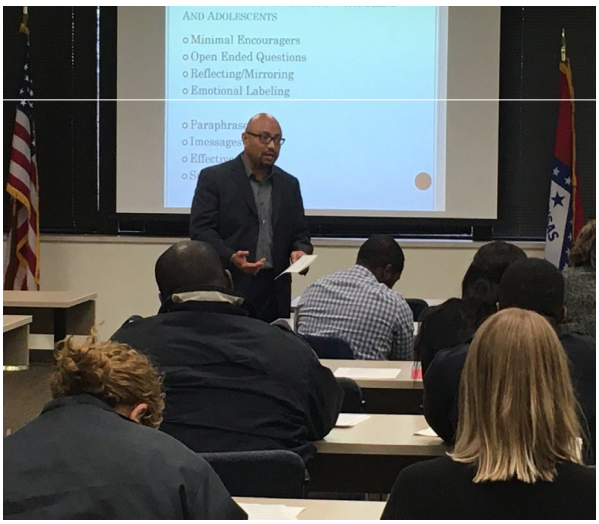
- FY22 Numbers thru May 31st
  - 3,609 Attendees (online and in-person)
  - Partnership with the Morgan Nick Foundation
  - Human Trafficking Awareness and Internet Safety
  - 14,957 Students
  - 602 School Staff

9

UNIVERSITY OF ARKANSAS SYSTEM
CRIMINAL JUSTICE INSTITUTE

AR Center for School Safety

WWW. ARSAFESCHOOLS.COM



10

UNIVERSITY OF ARKANSAS SYSTEM
CRIMINAL JUSTICE INSTITUTE

AR Center for School Safety

Ms. Vicki French 501-570-8098
vefrench@cji.edu

11

Thank you!

Dr. Cheryl May, Director

Email: cpmay@cji.edu
Phone: 501-570-8052
Website: www.cji.edu

National Cybersecurity Preparedness Consortium (NCPC)

July 11, 2022

DESE Summit

Dr. Cheryl May

Why is Cybersecurity in Schools Important

- In 2021, over 1,000 schools in the U.S. were affected by Ransomeware incidents.
- Schools are perceived as having lots of money. Range of ransomeware amounts were $100,000 to $40M
- Schools are ripe with a lot of personal information on students and parents
  - Identity Theft
  - Human Trafficking
  - Sextortion
  - It Is All About $$$$$$$

Slide 2

Introduction of the National Cybersecurity Preparedness Consortium (NCPC)

The NCPC's mission:

- To help State, Local, Tribe and Territory (SLTT) governments establish viable and sustainable programs to prevent, detect, respond to, and recover from cyber attacks
  - Public and Private Sectors
- To provide research-based, cybersecurity-related training, exercises and technical assistance to SLTT communities (everyone has a role).

Slide 3

Consortium Members

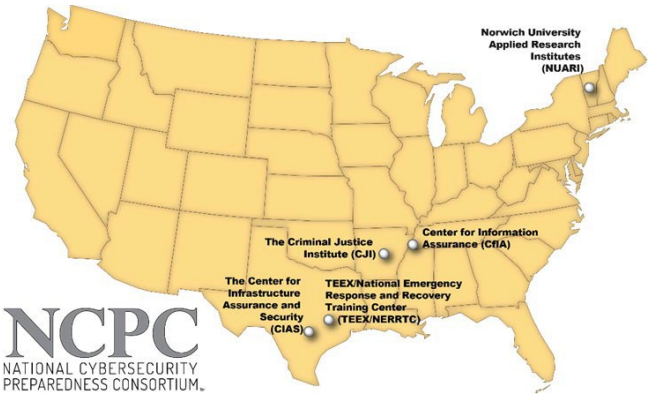
- National Cybersecurity Preparedness Consortium Members
  - Cyber Defense Initiative-CJI/UA System
    - Dr. Cheryl May, Consortium Chair
  - Center for Infrastructure Assurance and Security-University of Texas-San Antonio
  - Texas A&M Engineering Extension Service-Texas A&M University System
  - Norwich University Applied Research Institutes, Norwich University
  - Center for Information Assurance, Univ. Memphis

National Cybersecurity Preparedness Consortium

NATIONAL CYBERSECURITY PREPAREDNESS CONSORTIUM

Slide 4

NCPC Partners



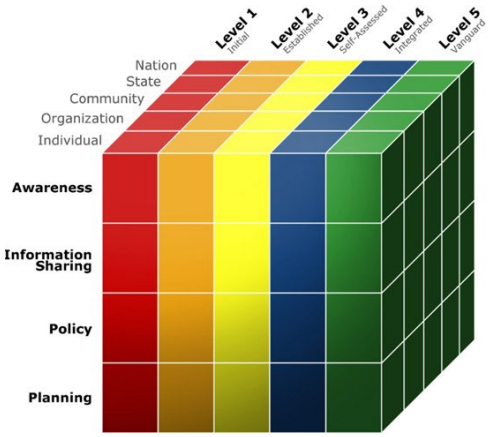
- Five Universities Working Collaboratively with Lanes
- Trained 113,606 from 2002 – September 30, 2021
- 48 Total Courses (and growing)
  - 33 Certified Courses
  - 15 Courses in Development
- Received Federal Appropriations in 2021 and 2022
- All NCPC Courses are Available Free of Charge!!

Slide 5

Organized Around the CCSMM

The Community Cyber Security Maturity Model:

- Framework for cybersecurity preparedness
  - Focusing first on low and no cost solutions
- Everyone has a role in cybersecurity from the individual, organization, community, state and nation
- Addresses all aspects of cybersecurity
- Incorporates other frameworks such as the NIST CSF, NICE, CMMC, EMP and others
- Provides a roadmap to improve cybersecurity posture



Slide 6

NCPC History

- NCPC-FEMA Partnership
  - 2013 1st NCPC CTG Grant
  - Lead Institutions
    - CJI, UTSA, NUARI
  - Course Development and Delivery
    - Based on annual FEMA Objectives such as:
      - Investigating Cybercrime
      - Internet of Things based attacks
      - End-User Awareness
      - Securing Critical Infrastructure (CI) and SCADA
    - All NCPC Courses are FEMA Certified/Continuously Updated!
    - And ADA Compliant (508 Compliance)

National Cybersecurity Preparedness Consortium

Slide 7

NCPC Capabilities

FEMA State, Local, Tribes and Territories (SLTT) Training

- Awareness
- Coordination and Planning
- Cyber Incident Response and Recovery
- Infrastructure Technical Training
- Cyber Threat Information Sharing

Slide 8

NCPC Capabilities

SLTT Training

- Individuals/End users
- IT Security Personnel
- Leadership

All These Groups MUST Be Involved in Establishing Your Cybersecurity Posture!

Slide 9

Target Audience

Leadership/Management

- Courses that are strategic to assist the organization/community to create and modify strategies and plans for long-term goals. Roles can be Chief officers, policy makers, risk mangers, mid-level management.

Leadership/Management - 20 Courses

Slide 10

Leadership/Management - 20 Courses

Awareness

- AWR-383 – Cybersecurity Risk Awareness for Officials and Senior Mgmt (Length – 4 hours)
  This is a non-technical course designed to develop awareness of cybersecurity risks for elected officials, appointed officials and other senior managers so that they are better informed to properly protect the jurisdiction/organization during a cybersecurity incident. It is designed to help officials and senior management work more effectively with their Information Technology (IT) departments to mitigate cyber threats.

Coordination and Planning

- AWR-384 – Community Preparedness for Cyber Incidents (Length – 12 hours)
  Community Preparedness for Cyber Incidents is a two-day, non-technical course designed to provide organizations and communities with strategies and processes to increase cyber resilience. Participants will analyze cyber threats and initial and cascading impacts of cyber incidents, evaluate the process for developing a cyber preparedness program, examine the importance and challenges of cyber related information sharing and discover low to no-cost resources to help build cyber resilience.

Slide 11

Leadership/Management - 20 Courses

Cyber Threat Information Sharing

- MGT-473 – Organizational Cybersecurity Information Sharing (Length – 16 hours)
  This course introduces fundamental cyber information sharing concepts that can be incorporated into a cybersecurity program for both inside and outside an agency or organization. It introduces the purpose and value of information sharing and how sharing can assist with cyber incident preparedness and response before, during and after a cyber incident occurs. It will identify types of shared cyber information; explore when to share information; and will explore attributes found when reporting cyber information.

Slide 12

Leadership/Management - 20 Courses

Cyber Incident Response & Recovery

- AWR-366W – Developing a Cybersecurity Annex for Incident Response (Length – 6 hours)

  This online course addresses the need for a strategic-level "how to" of responding to and sharing information about cybersecurity incidents through the cyber annex vehicle. At the end of this course, participants should possess the fundamentals needed to design and develop a cyber annex for states, locals, tribes and/or territories (SLTTs). It addresses what the annex is, how it is used, who should participate in the design, implementation and execution.

Technical Training

- AWR-418W – Cybersecurity Fundamentals (Length – 4 hours)

  Cybersecurity Fundamentals is an introductory level course designed for new and transitioning Information Technology professionals. Participants learn preferred network topologies and the uses of Intrusion Detection/Prevention systems; the use and maintenance of firewalls and anti-virus software; to recognize various types of network based attacks; to recognize social engineering attacks, both remote and in-person; and the importance of establishing policies, and disaster planning.

Slide 13

Target Audience

IT Security Personnel

- Courses that focus on developing skills needed to design, develop, implement and maintain cybersecurity. to protect themselves, their organizations and community's from data loss or cyber attacks. Roles can be IT, information security or cybersecurity professionals or those with technical responsibilities within the organization/community.

IT Security – 18 Courses

Slide 14

IT Security Personnel– 18 Courses

Awareness

- AWR-388W – Cybersecurity Awareness for Municipal, Police, Fire and EMS IT Personnel (Length – 2 hours)
  This course covers basic cyber awareness for Municipal, Police, Fire and EMS Information Technology personnel. Participants will increase their knowledge of threats specific to their jurisdiction and an understanding of the processes and procedures needed to develop a cyber-awareness program. This course focuses on the steps involved in being aware of cyber threats and effectively communicating the processes and procedures to protect users against common cyber threats. The participants will apply this knowledge by developing processes and procedures to integrate cyber awareness into routine operations.

Slide 15

IT Security Personnel- 18 Courses

Technical Training

- PER-256 – Comprehensive Cybersecurity Defense (Length – 32 hours)
  Comprehensive Cybersecurity Defense (CCD) is a basic-level course designed for technical personnel who monitor and protect our nation's critical cyber infrastructure. The course introduces students to cyber-defense tools that will assist them in monitoring their computer networks and implementing cybersecurity measures to prevent or greatly reduce the risk of a cyber-based attack. This course integrates hands-on computer lab applications to maximize the student's learning experience.

- PER-257 – Cybersecurity First Responder (Length – 32 hours)
  Cybersecurity First Responder (CFR) is an intermediate-level course designed for technical personnel who are first responders to any type of cyber-based attack against our nation's critical cyber infrastructure. Blended learning methods are utilized, to include a balance of classroom lecture, hands-on laboratory exercises, and the use of cyberterrorism response tools against real world simulated cyber-attacks. Students learn the proper steps of an incident response to include incident assessment, detection and analysis, and the containing, eradicating, and recovering process from a system or network-based attack.

Slide 16

IT Security Personnel - 18 Courses

Technical Training

- PER-382 – Malware Prevention, Discovery, and Recovery (Length – 32 hours)
  Malware Prevention, Discovery, and Recovery (MPDR) is an intermediate-level course is designed for technical personnel who monitor and protect our nation's critical cyber infrastructure. Students learn how to recognize, identify, and analyze malware; the remediation process to eliminate the malware; and proper procedures to recover from the attack and regain network connectivity in a timely manner. This course integrates hands-on computer lab applications to maximize the student's learning experience.

Slide 17

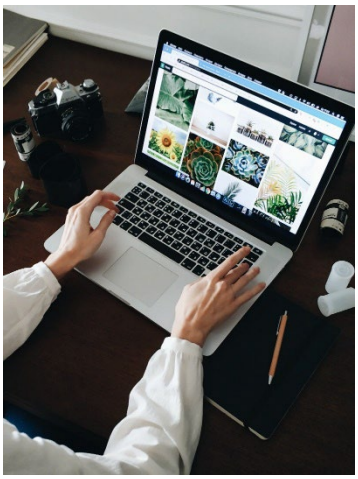
IT Security Personnel- 18 Courses

Technical Training

- PER-377 – Cybersecurity Proactive Defense (Length – 32 hours)
  Cybersecurity Proactive Defense (CPD) is an advanced-level course designed for technical personnel who monitor and protect our nation's critical cyber infrastructure. CPD uses hands-on computer lab applications to simulate advanced attack vectors, sequential and escalating attack steps, and hands-on attack execution. Students learn penetration testing skills, defense analysis techniques, and real-time response and threat mitigation steps.

Slide 18

Target Audiences



End User

- Courses that assist individuals to be in sync with the organization/communities cybersecurity to improve performance/effort/knowledge and change behaviors. Roles can be employees or individuals within an organization or community.

End User - 13 Courses

Slide 19

End User - 13 Courses

Awareness

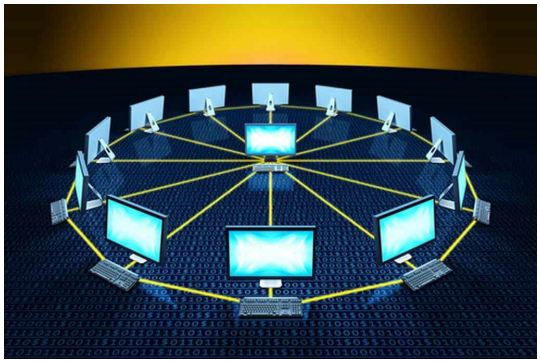
- AWR-367W – Understanding Social Engineering Attacks (Length – 8 hours)
  This course educates members of the public to understand some common defense tactics that can be used to mitigate social engineering attacks, this course provides students with an understanding of how social engineering attacks can be better mitigated by combining comprehensive security measures with an understanding and awareness of how such attacks can exploit human behaviors. Phishing, spear-phishing, water-holing, ransomware and other types of advanced persistent threats.
- AWR-402W – Introduction of Internet of Things (IoT) Devices (Length – 2 hours)
  This course provides an understanding of the history, definitions and components that make up IoT. It addresses the different applications of IoT, as well as applicable laws and policies, technologies, emerging threats, best practices, security and a variety of existing and developing technologies. This course is ideal for participants, from throughout the various levels of government, private industry and community, wanting to understand how they are affected by IoT.

Slide 20

End User - 13 Courses

Awareness

- AWR-397W – Cybersecurity for Everyone (Length – 4 hours)
  Computers, mobile devices and the Internet of Things (IoT) are a part of our daily lives. By using all of this technology, which makes our lives easier, we have opened ourselves up to the risks of cyber-attacks. This course will introduce you to the basics of protecting your computer and the data it stores as well as protecting yourself when you are online, on social media, and while using your mobile or smart devices.



Slide 21

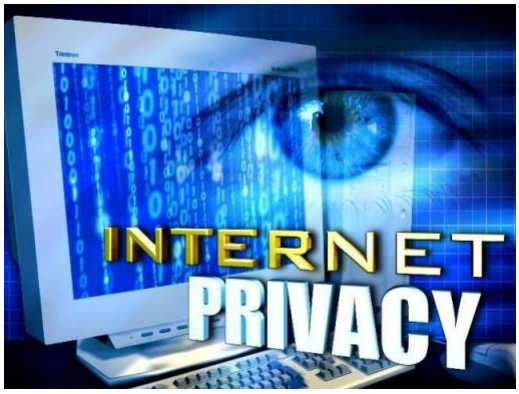
End User - 13 Courses

Awareness

- AWR-395W – Cybersecurity in the Workplace (Length – 2 hours)
  Every employee using a computer connected to the organization's network is a potential point of entry for a cyber-attack. For this reason, cybersecurity and protecting the organization's data/information is every employee's responsibility. This course will help students understand the different types of cyber-attacks their company may face, the type of information that is at risk, how to recognize cyber-attacks and why it is important for everyone in the organization to participate in cybersecurity.

Slide 22

End User – 13 Courses



Technical Training

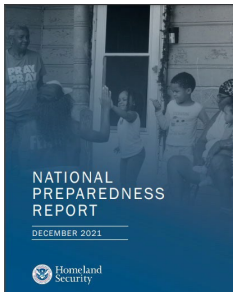
- AWR-TBDW – End-User Security and Privacy (Length – 4 hours)

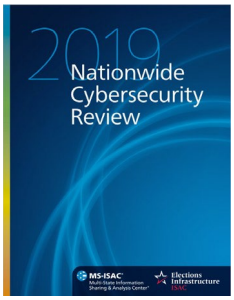
  This course will focus primarily on end-user's perspective. In particular, various security-related challenges faced by end-users and their impact on data privacy. The course will also include content concerning online content providers and local ISPs on access rights, unintentional data sharing, mobile apps and how to be compliant to a NIAP Protection Profile (PP), etc.

Slide 23

NCPC SLTT Experience

- Insights and statistics are taken into consideration for all courses
  - Observations
  - Interviews
  - Reports (Nationwide Cybersecurity Report – MSISC; National Preparedness Report; NASCIO Reports e.g.)
- Addresses
  - People, Capabilities, Resources
- Need a plan
  - Where to start (step by step)
  - No and low cost solutions





Slide 24

NCPC Establishing a National SLTT Program

FEMA SLTT Training

- Awareness
- Coordination and Planning
- Cyber Incident Response and Recovery
- Infrastructure Technical Training
- Cyber Threat Information Sharing

Other Capabilities

- Cybersecurity Exercises
  - Organization, Sector, Municipality & State
- Information Sharing
- Establishing Cybersecurity Programs
- Workforce Development
- Cybersecurity for Small Businesses
- K-16 Education
- Culture of Cybersecurity
- Rural Needs

Slide 25

NCPC SLTT Experience

- Key/Critical Actions
  - Back Up All Data
  - Ensure All Software Patches Are Updated Immediately
  - Ensure Passwords are Changed Frequently
  - Use Multi-Factor Authentication-MFA (VPN Capabilities)
  - Encryption
  - Cybersecurity Policies and Procedures are in Place
- Cybersecurity and Infrastructure Security Administration (CISA)
  - Know Your Vulnerabilities
  - Conduct FREE Vulnerability Assessments

Slide 26

Contacts

- WWW.NATIONALCPC.ORG

- Jimmy Nobles
  Criminal Justice Institute
  Cyber Defense Initiative
  501-570-8058
  jwnobles@cji.edu

National Cybersecurity Preparedness Consortium

Slide 27

Discussion & Questions: Thank You

Slide 28

2022

CYBERSECURITY TRAINING COURSES

Contents

About the NCPC

The mission of the National Cybersecurity Preparedness Consortium (NCPC) is to provide research-based, cybersecurity-related training, exercises, and technical assistance to local jurisdictions, counties, states, tribes, territories and the private sector.

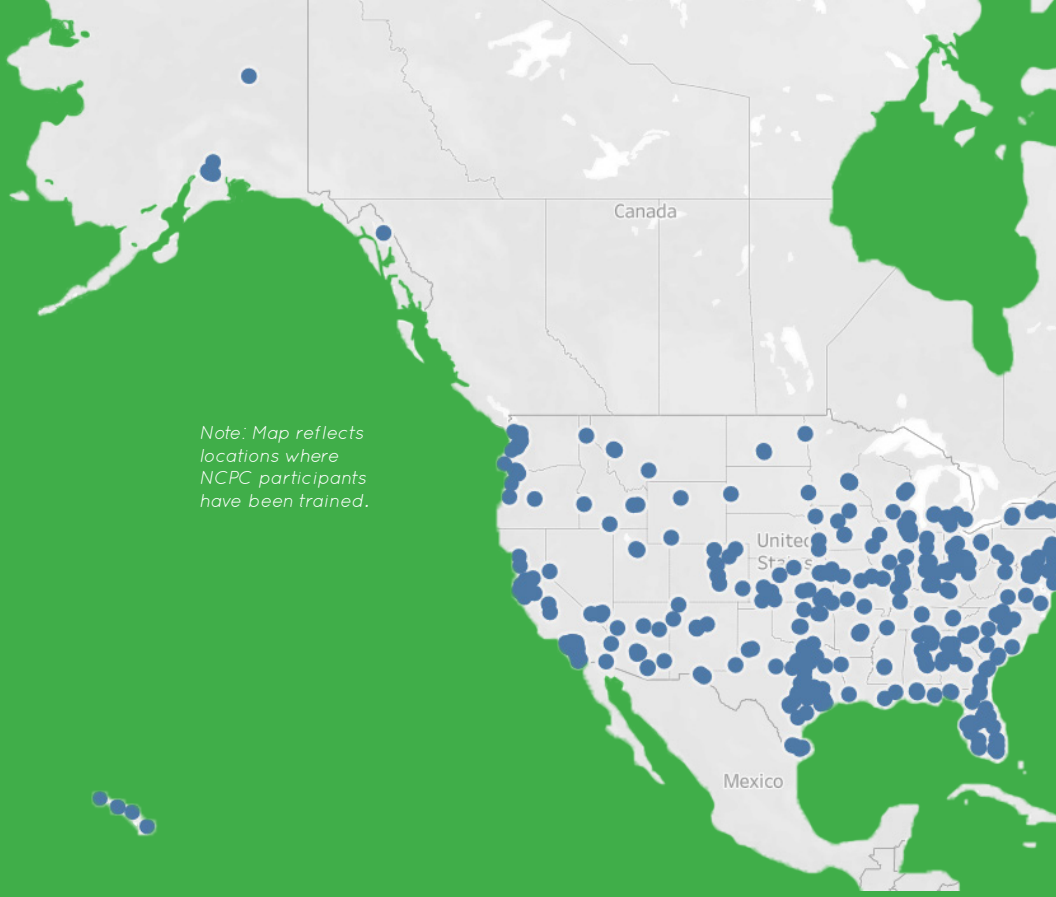
Using the Community Cyber Security Maturity Model (CCSMM) as a basis from which to work, the consortium collectively works with states and communities as they progress through the model.

The CCSMM is based on over a decade of experience with states and communities working to develop viable and sustainable cybersecurity programs for the whole community.

To register for NCPC web-based and instructor-led courses, contact your state's Homeland Security Training Office. More information on how to register for courses is on NationalCPC.org.

FEMA

UA University of Arkansas System Criminal Justice Institute · CIAS Center for Infrastructure Assurance and Security · TEEX Texas A&M Engineering Extension Service, National Emergency Response and Recovery Training Center · The University of Memphis, Center for Information Assurance · Norwich Pro™



Note: Map reflects locations where NCPC participants have been trained.

By the Numbers

As of October 2021, members of the Consortium have trained more than 113,606 participants:

- CIAS – 8,553 trained
- CJI – 5,946 trained
- CfIA – 5,052 trained
- NU – 1,551 trained
- TEEX/NERRTC – 92,504 trained

NCPC Experience

As early as 2004, in partnership with the Department of Homeland Security (DHS) and Federal Emergency Management Agency (FEMA), the individual members of the NCPC have developed and delivered DHS/FEMA certified online and face-to-face **no cost** training courses to an array of states, counties, local jurisdictions, and critical infrastructure components nationwide addressing cybersecurity concerns.

NCPC Partners

Center for Infrastructure Assurance and Security (CIAS) at the University of Texas, San Antonio | cias@utsa.edu

Criminal Justice Institute (CJI), University of Arkansas System | cdi@cji.edu

Norwich University (NU) | norwichpro@norwich.edu

Texas A&M Engineering Extension Service/National Emergency Response and Recovery Training Center (TEEX/NERRTC) | bcs@teex.tamu.edu

University of Memphis, Center for Information Assurance (CfIA) | cfia@memphis.edu

Awareness

Cyber Ethics (AWR-174-W)
WEB-BASED. 13 hours; 1.3 CEUs; 2 hours - ACE; 2 semester hours.
This course shares the proper techniques for approaching the difficult ethical dilemmas arising from use of the modern Internet. Develop the skills to assess future ethical dilemmas by examining some of the more pressing concerns related to Internet usage today.

Cyber Security Awareness for Municipal, Police, Fire & EMS IT Personnel (AWR-388-W)
WEB-BASED. 2 hours; .2 CEUs.
This course provides participants with an increased knowledge of threats specific to their jurisdiction and an understanding of the processes and procedures needed to develop a cyber-awareness program. It focuses on the steps involved in being aware of cyber threats and effectively communicating the processes and procedures to protect users against common cyber threats.

LEGEND

Web-Based Course

Instructor-Led Course

COMING SOON
Courses Under Development

Cybercrime Insight and Introduction to Digital Evidence Identification

COMING SOON

INSTRUCTOR-LED. 8 hours.

A course that introduces state, local, tribal and territorial first responders with limited or no prior knowledge of computer crime and cyber investigations to the importance of identifying evidence related to suspected criminal activity, and incorporating evidence into investigation.

Cybersecurity Risk Awareness for Officials and Senior Management (AWR-383)

INSTRUCTOR-LED. 4 hours; .4 CEUs.

This is a non-technical course designed to develop awareness of cybersecurity risks for elected officials, appointed officials and other senior managers so that they are better informed to properly protect the jurisdiction/organization during a cybersecurity incident. It is designed to help officials and senior management work more effectively with their Information Technology (IT) departments to mitigate cyber threats.

Cybersecurity for Everyone (AWR-397-W)

WEB-BASED. 4 hours; .4 CEUs.

This course introduces participants to the basics of protecting their computer and the data it stores, as well as how to protect themselves when online, on social media and while using a mobile or smart device.

Cybersecurity in the Workplace (AWR-395-W)

WEB-BASED. 2 hours; .2 CEUs.

This course helps participants understand the different types of cyber-attacks their company may face, the type of information that is at risk, how to recognize cyber-attacks and why it is important for everyone in the organization to participate in cybersecurity.

Detecting and Responding to a Cyber Attack (AWR-399-W)

WEB-BASED. 4 hours; .4 CEUs.

This course introduces students to varous types of cyber-attacks and how to detect and respond to them in order to protect their data and information.

Awareness

Essentials of Community Cybersecurity (AWR-136)

INSTRUCTOR-LED. 4 hours; .4 CEUs.

This discussion-based, non-technical course is an introduction to cybersecurity that provides individuals, community leaders and first responders with information on how cyber-attacks can impact, prevent and/or stop operations and emergency responses in a community. The course provides a cursory introduction to cybersecurity vulnerabilities, risks, threats, countermeasures and actions that communities can take to establish a cybersecurity program.

Foundations of Cyber Crimes (AWR-168-W)

WEB-BASED. 10 hours; 1.0 CEUs; 2 hours - ACE; 2 semester hours

This course examines cyber and cyber faciliated non-violent white-collar crimes, fraud and financial crimes, and violent crimes, and the appropriate response by first responders and other local, state and federal agencies that may encounter them. Participants will identify legislative, organizational and suggested personal efforts to control or prevent cyber crimes.

Introduction to Internet of Things (IoT) Devices (AWR-402-W)

WEB-BASED. 2 hours; .2 CEUs.

This course provides an understanding of the history, definitions and components that make up IoT. It addresses the different applications of IoT, as well as applicable laws and policies, technologies, emerging threats, best practices, security and a variety of existing and developing technologies. This course is ideal for participants, from throughout the various levels of government, private industry and community, wanting to understand how they are affected by IoT.

Mobile Device Security & Privacy (AWR-385-W)

WEB-BASED. 6.5 hours; .7 CEUs.

This course is designed to provide a better understanding of security and privacy issues associated with mobile devices and infrastructure; including benefits and challenges of designing, implementing and maintaining Bring Your Own Device (BYOD) Programs. Using scenarios, thought challenges and exercises as a framework, students will learn about the purpose of Enterprise Mobile Management platforms; elements that make mobile networks and operating systems different Mobile malware classifications and detection strategies; and mobile architecture data leakage detection and prevention strategies.

Network Security for Homes and Small Businesses (AWR-396-W)

WEB-BASED. 2 hours; .2 CEUs.

This course introduces students to the basics of networks for homes and small businesses, and provides them with best practices to secure their networks in order to protect their personal information as well as other information (e.g., friends, family, customerrs, vendors) that may flow through their network.

Demystifying Cyber Attacks (AWR-421)

INSTRUCTOR-LED. 6 hours.

This course demonstrates tools used by bad actors and cyber defenders to provide a complete picture of a cyber-attack. This course is ideal for any individual responsible for responding to cyber incidents or organizational strategy.

Practical Internet of Things (IoT) Security

INSTRUCTOR-LED. 16 hours.

This course will introduce students to components of an IoT system and associated security concerns. It will cover the elements of an IoT system, including programmable logic controllers, sensors and network interfaces. Students will explore IoT vulnerabilities using common vulnerability assessment tools such as Kali Linux. Lecture and exercises will culminate in a laboratory experience where teams of students will build an IoT system and examine security considerations, vulnerabilities, and threats.

Remote/Home-Office Cybersecurity Preparedness (RHC)

WEB-BASED. 4-6 hours.

COMING SOON

This course addresses the changing workforce as a result from the COVID-19 Pandemic situation, opening the door for remote work environments that are changing the landscape of cyber-security and Work From Home (WFH) strategies. The need for home office and normal work strategy/infrastructures is becoming tightly coupled, requiring using different cyber-enabled systems, devices, and services.

Understanding Social Engineering Attacks (AWR-367-W)

WEB-BASED. 8 hours; .8 CEUs.

This course educates members of the public in the general understanding and some common defense tactics that can be used to mitigate social engineering attacks. It provides students with an understanding of how social engineering attacks can be better mitigated by combining comprehensive security measures with an understanding and awareness of how such attacks can exploit human behaviors. The course will introduce phishing, spear-phishing, water-holing, ransomware and other types of advanced persistent threats.

Understanding Targeted Cyber Attacks (AWR-376)

INSTRUCTOR-LED. 8 hours; .8 CEUs.

This course provides specific information regarding targeted cyber attacks, including advanced persistent threats. This information will place participants in a better position to plan and prepare for, respond to and recover from targeted cyber attacks. This course will fill the gap in threat-specific training for cybersecurity as a community-driven course that focuses on the phases of targeted cyber attacks and the attacker methods used during each phase. Participants will also receive valuable information on cyber attack prevention, mitigation and response.

Coordination & Planning

Community Preparedness for Cyber Incidents (MGT-384)

INSTRUCTOR-LED.
12 hours; 1.2 CEUs.

This non-technical course is designed to provide organizations and communities with strategies and processes to increase cyber resilience. Participants will analyze cyber threats and initial and cascading impacts of cyber incidents, evaluate the process for developing a cyber preparedness program, examine the importance and challenges of cyber related information sharing and discover low to no-cost resources to help build cyber resilience.

Community Cyber Defense (an Interactive Exercise)

INSTRUCTOR-LED. 8 hours.

COMING SOON

This course will train students to establish community cybersecurity strategies to prevent, respond and recover from cyber-attacks. Participants will learn fundamental concepts of what's included in a cybersecurity program for organizations and the community.

Coordination & Planning

Cybersecurity Vulnerability Assessment and Remediation

INSTRUCTOR-LED. 16 hours.

Through learning to conduct cybersecurity vulnerability assessments and developing a vulnerability remediation program, organizations will be able to prepare and plan for cyber incidents.

Physical and Cybersecurity for Critical Infrastructure (MGT-452)

INSTRUCTOR-LED. 8 hours; .8 CEUs.

This course encourages collaboration efforts among individuals and organizations responsible for both physical and cybersecurity toward development of integrated risk management strategies that lead to enhanced capabilities necessary for the protection of our nation's critical infrastructure. Participants will identify physical and cybersecurity concerns impacting overall infrastructure security posture, examine integrated physical and cybersecurity incidents and the evolving risks and impacts they pose to critical infrastructure.

Using the Community Cyber Security Maturity Model to Develop a Cyber Security Program (AWR-353-W)

WEB-BASED. 2 hours; .2 CEUs.

This course will enable community leaders, network/security personnel and those individuals involved in developing or maintaining plans used for and throughout the community. It will help participants understand what is required to develop a coordinated, sustained and viable community cybersecurity program. Participants will also be introduced to various resources, including the DHS-supported Community Cyber Security Maturity Model (CCSMM), to guide communities and states in developing their own cybersecurity programs.

Cyber Incident Response & Recovery

Cyber Incident Analysis and Response (AWR-169-W)

WEB-BASED. 10 hours; 1.0 CEUs;
2 hours - ACE; 1 semester hour.

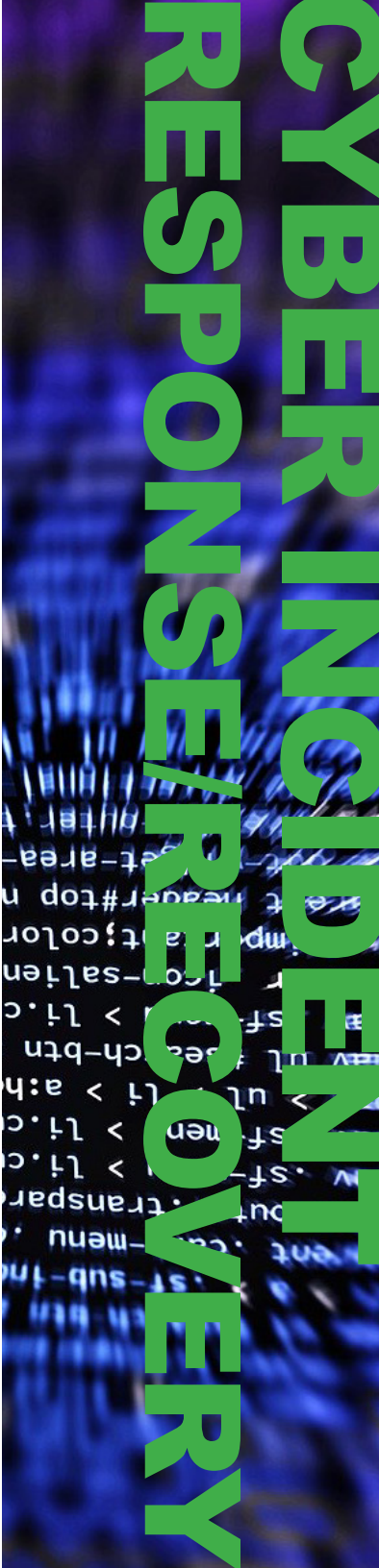
This course provides practical guidelines on responding to incidents effectively and efficiently as part of an incident response program. Primary topics include detecting, analyzing, priortizing and handling cyber incidents. Real-world examples and scenarios to help provide knowledge, understanding and capacity for effective cyber incident analysis and response.

Cybersecurity Incident Response for IT Personnel (PER-371)

INSTRUCTOR-LED.
24 hours; 2.4 CEUs.

This course is designed to address the gap in specific technical skills needed for an effective cyber response. This course will also help improve the limited availability of targeted hands-on IT and security training focused on cyber-attacks. This training focuses on government and private sector technical personnel who have intermediate and advanced knowledge of network operations and/or the responsibility for network security.

CYBER INCIDENT RESPONSE & RECOVERY Courses >>



Cyber Incident Response & Recovery

Developing a Cyber Security Annex for Incident Response (AWR-366-W)

WEB-BASED. 6 hours; .6 CEUs.

This course addresses the need for a strategic-level "how to" of responding to and sharing information about cybersecurity incidents through the cyber annex vehicle. At the end of this course, participants should possess the fundamentals needed to design and develop a cyber annex for states, locals, tribes and/or territories (SLTTs). It addresses what the annex is, how it is used, and who should participate in the design, implementation and execution.

Disaster Recovery for Information Systems (AWR-176-W)

WEB-BASED. 10 hours; 1.0 CEUs; 2 hours - ACE; 1 semester hour.

This course trains business managers to respond to varying threats that might impact their organization's access to information. The course provides requisite background theory and recommended best practices needed by managers to keep their offices running during incidents of different types. Topics include disaster recovery planning; guides for implementing and managing disaster recovery plans; a discussion of technical vulnerabilities; and an examination of legal issues.

Incident Response for Municipal, Police, Fire & EMS IT Personnel (AWR-389-W)

WEB-BASED. 2 hours; .2 CEUs.

The course introduces the basics of the incident response process to the Information Technology personnel in Police, Fire or EMS departments. The content of the course will include: cyber incidents in Police, Fire, EMS and IT departments, and developing a response plan to cyber incidents.

Integration of Cybersecurity Personnel into the Emergency Operations Center (EOC) for Cyber Incidents (MGT-456)

INSTRUCTOR-LED. 24 hours; 2.4 CEUs.

The course is designed to assist jurisdictions with coordinating and managing response efforts between emergency response organizations and critical infrastructure cybersecurity personnel. The course will help to ensure that traditional emergency management personnel and cybersecurity personnel recognize the importance of working together to mitigate the effects of a cyber incident. This course utilizes the Emergency Management Exercise System (EM*ES) incident simulation software.

Recovering from Cybersecurity Incidents (MGT-465)

INSTRUCTOR-LED. 16 hours; 1.6 CEUs.

This course provides guidance to a jurisdiction on the actions necessary to effectively recover from a cybersecurity attack. It discusses the pre- and post-incident programmatic activities needed for short-term and long-term recovery, and bridges the different worlds of information technology and emergency management. This training is particularly pertinent to IT management, emergency management personnel, as well as any other government, critical infrastructure, or private sector personnel who has the responsibility for recovering after a cyber incident.

Network Traffic Analysis

INSTRUCTOR-LED. 24 hours.

COMING SOON

This course will train students to conduct traffic analysis on their internal networks by doing a “deep-dive” into network traffic analysis using Wireshark and other tools to identify regular and anomalous network traffic. It will teach techniques necessary to identify network attacks by context and type.

Infrastructure Technical Training

Comprehensive Cybersecurity Defense (PER-256)

INSTRUCTOR-LED. 32 hours.

A basic-level course designed for technical personnel who monitor and protect our nation's critical cyber infrastructure. The course introduces students to cyber-defense tools that will assist in monitoring their computer networks and implementing cybersecurity measures to prevent or greatly reduce the risk of a cyber-based attack. This course integrates hands-on computer lab applications to maximize the student's learning experience.

Cyber Identity and Authentication (AWR-384-W)

WEB-BASED. 6 hours; .6 CEUs.

This course addresses different forms of authentication, such as two-factor, multi-factor and other protections addressing identity compromise. Designed for public and private personnel at all levels of government, law enforcement, the private sector and other stakeholders, CIAA provides a broad-base of knowledge connecting the underlying concepts of digital identity to how people, devices and systems are authorized to access digital resources and services.

Cybersecurity First Responder (PER-257)

INSTRUCTOR-LED. 32 hours.

An intermediate-level course designed for technical personnel who are first responders to any type of cyber-based attack. Blended learning methods are used to include a balance of classroom lecture, hands-on laboratory exercises and the use of response tools against real world simulated cyber-attacks. Students learn the steps of an incident response to include incident assessment, detection and analysis, and containing, eradicating, and recovering processes from a system or network-based attack.

Cybersecurity Fundamentals (AWR-418-W)

WEB-BASED. 4 hours.

An introductory level course for new and transitioning Information Technology professionals. Learn preferred network topologies and the uses of Intrusion Detection/Prevention systems; the use and maintenance of firewalls and anti-virus software; to recognize various types of network-based attacks; to recognize social engineering attacks; and the importance of establishing policies, and disaster planning.

Cybersecurity Proactive Defense (PER-377)

INSTRUCTOR-LED. 32 hours.

An advanced-level course for technical personel who monitor and protect critical cyber infrastructure. It uses hands-on computer lab applications to simulate advanced attack vectors, sequential and escalating attack steps, and attack execution. Learn penetration testing skills, defense analysis techniques, and real-time response and threat mitigation steps.

Cybersecurity Resiliency in Industrial Control Systems (PER-398)

INSTRUCTOR-LED. 8 hours.

This course will review the Internet of Things vulnerabilities within Operational Technology and Supervisory Control and Data Acquisition systems, methods of detecting and responding to cyber attacks in the systems, and actions that can be taken by non-technical personnel to mitigate or minimize the effects of cyber attacks.

Infrastructure Technical Training

Digital Forensics Basics (AWR-139-W)

WEB-BASED. 7 hours; .7 CEUs; 2 hours - ACE; 1 semester hour.

This course explains investigative methods and standards for the acquisition, extraction, preservation, analysis, and deposition of digital evidence from storage devices. Using realistic forensics situations, learn how to find traces of illegal or illicit activities using computer forensics tools and manual techniques. Also, learn how to recover data intentionally hidden or encrypted by perpetrators.

End-User Security and Privacy

WEB-BASED. 4-5 hours.

This course will focus primarily on end-user's perspective. In particular, various security-related challenges faced by end-users and their impact on data privacy. The course will also include content concerning online content providers and local ISPs on access rights, unintentional data sharing, mobile apps and how to be compliant to a NIAP Protection Profile (PP), etc.

Examining Advanced Persistent Threats (AWR-403-W)

WEB-BASED. 4 hours; .4 CEUs.

This course will address best practices that can assist in protecting against advanced persistent threats. Designed for public and private personnel at all levels of government, law enforcement, the private sector and other stakeholders, it provides a broad base of knowledge focused on how to prepare for, respond to and recover from the impacts of advanced cyber-attacks that exploit targeted victims.

Information Risk Management (AWR-177-W)

WEB-BASED. 13 hours; 1.3 CEUs; 2 hours - ACE; 1 semester hour.

This course addresses topics related to information assets, identifying risks, and management processes. Receive training on information risk-related tools and technologies for better understanding of potential threats and vulnerabilities in online business. Learn best practices and how to apply levels of security measures.

Information Security Basics (AWR-173-W)

WEB-BASED. 13 hrs; 1.3 CEUs; 2 hrs - ACE; 1 semester hour.

This course provides entry/mid-level IT staff a technical overview of information security, focusing on the knowledge to identify and stop various cyber threats. General concepts and topics covered include TCP/IP protocol, introductory network security, introductory operating system security, and basic cryptography.

Introduction to Basic Vulnerability Assessment Skills (AWR-368-W)

WEB-BASED. 7.5 hours; .8 CEUs.

This course helps prepare learners for the technical challenges associated with conducting vulnerability assessments and/or penetration testing. It introduces the basic skills needed to begin mastering in order to conduct or manage vulnerability assessments. It also introduces, Metasploit, which red teams use to test networks.

Malware Prevention, Discovery and Recovery (PER-382)

INSTRUCTOR-LED. 32 hours.

An intermediate-level course designed for technical personnel who monitor and protect critical cyber infrastructure. Learn how to recognize, identify, and analyze malware; the remediation process to eliminate the malware; and proper procedures to recover from the attack and regain network connectivity.

Network Assurance (AWR-138-W)

WEB-BASED. 5 hours; .5 CEUs; 2 hours - ACE; 1 semester hour.

This course covers secure network practices to protect networked systems against attacks and exploits. Topics include authentication, authorization, and accounting (AAA), as well as firewalls, intrusion detection/prevention, common cryptographic ciphers, server and client security, and secure policy generation.

Secure Software (AWR-178-W)

WEB-BASED. 9 hours; 0.9 CEUs; 1 semester hour.

This course teaches programming practices used to secure applications against attacks and exploits. Fundamental concepts and topics covered include secure software development, defensive programming techniques, secure design and testing, and secure development methodologies.

Cyber Threat Information Sharing

Community Cybersecurity Information Sharing Integration (MGT-478)

INSTRUCTOR-LED. 16 hours.

This course will show SLTTs how to integrate cybersecurity information sharing into their community programs. Learn to strategically design and implement a cybersecurity information sharing program for the state, territory, tribe, jurisdiction, or region. This includes governance; creating public/private partnerships; and coordinating efforts to prevent, mitigate and counter attacks for a community.

Cyber Threat Intelligence

INSTRUCTOR-LED. 16 hours.

COMING SOON

This course introduces the information analysis process and how an organization can use it to identify, define and mitigate cybersecurity threats. Participants will gain a general understanding of the tools and processes needed for an analysis team to create cybersecurity information and intelligence within their organization. It establishes a framework for an analytical process; how shared analysis can provide actionable information, reduce uncertainty and reduce risk to enable decision makers.

Establishing an Information Sharing and Analysis Organization (AWR-381-W)

WEB-BASED. 8 hours; .8 CEUs.

This course will assist communities to establish an Information Sharing and Analysis Organization (ISAO). The course will introduce the value proposition of creating an ISAO and provide considerations to joining an existing ISAO. It will closely follow the guidance provided by the ISAO Standards Organization (ISAO SO), whose mission is to "improve the nation's cybersecurity posture by identifying standards and guidelines for robust and effective information sharing and analysis related to cybersecurity risks, incidents, and best practices".

Introduction to ISAOs (AWR-398-W)

WEB-BASED. 2 hours; .2 CEUs.

This course is designed to introduce the basics of the cybersecurity information sharing processes. Participants will have an increased knowledge of cyber security information sharing and an understanding of the steps taken to join or establish an ISAO/ISAC.

Organizational Cybersecurity Information Sharing (MGT-473)

INSTRUCTOR-LED. 16 hours.

This course introduces fundamental cyber information sharing concepts that can be incorporated into a cybersecurity program for both inside and outside an agency or organization. It introduces the purpose and value of information sharing and how sharing can assist with cyber incident preparedness and response before, during and after a cyber incident occurs.

"Our cyber infrastructure is every bit as important as our roads and bridges It's important to our economy. It's important to protecting human life, and we need to make sure we have a modern and resilient cyber infrastructure."

~ Rep. Jim Langevin,
Co-Chair of the Congressional
Cybersecurity Caucus

Thank you for your interest in the National Cybersecurity Preparedness Consortium (NCPC) courses. These courses are developed by the NCPC partners with funding from the Department of Homeland Security/FEMA and are offered at no cost to States, Locals, Territories and Tribes.

To register for NCPC web-based and instructor-led courses, contact your state's Homeland Security Training Office. More information on how to register for courses is available on NationalCPC.org.

DHS/CISA Protective Security Programs

https://www.cisa.gov/infrastructure-security

Critical Infrastructure Vulnerability Assessments:
https://www.cisa.gov/critical-infrastructure-vulnerability-assessments
These voluntary, nonregulatory and no cost assessments are a foundational element of the National Infrastructure Protection Plan's risk-based implementation of protective programs designed to prevent, deter, and mitigate the risk of a terrorist attack while enabling timely, efficient response and restoration in an all-hazards, post-event situation. Types of Assessments Offered are below:

- Security Assessment at First Entry: A more consolidated assessment that provide a shorter executive level report that can be provided a few days after the on-site assessment. Duration is around 1-2 hours.
- Infrastructure Survey Tool: A comprehensive physical security, continuity and emergency management focused assessment that provide a more detailed assessment report with a planning dashboard. Duration is around 4-6 hours.
- Multi-Asset and System Assessment: A comprehensive assessment process that provides risk and criticality analysis on a individual infrastructure system and provides interactive risk reduction solutions. Duration is 3-6 months.
- Infrastructure Visualization Platform: We create a virtualized platform of a facility (like a virtual tour) that can be used for a more interactive Table-top exercises or discussion-based drills focused on physical security threats.
    - https://share.dhs.gov/pwqobrcia96j/
    - **Passcode: 04302021**

Infrastructure Dependency and Interdependency All-Hazard Planning:
https://www.cisa.gov/idp
This tool is a supplement to the Infrastructure Resilience Planning Framework and is intended to help state, local and private sector planners better understand how infrastructure dependencies can impact risk and resilience in their community and incorporate that knowledge into all-hazard planning activities. CISA field staff will also provide on-site assessments to help support dependency and interdependency planning as requested at no-cost.

Emergency Services Sector Continuity Planning Support:
https://www.cisa.gov/emergency-services-sector-continuity-planning-suite
State/Local Government and First responders can leverage these resources through the CISA field staff to help evaluate and improve their continuity capability and enhance their preparedness for emergencies. Services are at no cost.

Securing Public Gathering Programs:
https://www.cisa.gov/securing-public-gatherings
To help organizations mitigate potential risks in today's dynamic and rapidly evolving threat environment, CISA provides a compendium of resources for securing public gatherings. These resources cover the numerous threat vectors in CISA's portfolio, including unauthorized access to facilities, cybersecurity, election security, active shooters, bombings, and small unmanned aircraft systems (sUAS).

- Businesses and Critical Infrastructure: CISA provides businesses and critical infrastructure partners with resources to identify, develop, and implement scalable security measures to build or improve capabilities across the private and public sectors.
- SLTT Authorities, Government and First Responders: These resources provide information to help first responders, and state, local, tribal, and territorial (SLTT) governments protect themselves from a variety of CISA-identified threats.
- Schools: CISA, along with other organizations throughout government, law enforcement, and communities nationwide, is postured to continually enhance school safety and security.
- Houses of Worship: This resource page is designed to guide houses of worship through building improved security and safety protocols for their specific organization's congregants and facilities.

Active Shooter Preparedness:
https://www.cisa.gov/active-shooter-preparedness
DHS aims to enhance preparedness through a "whole community" approach by providing products, tools, and resources to help you prepare for and respond to an active shooter incident. We do a 1-2 hour on-site active shooter preparedness training workshop and conduct a active shooter security specific walk-through as a part of the workshop. On-site outreach resources are available to critical infrastructure stakeholders at no cost.

Insider Threat Mitigation:
https://www.cisa.gov/insider-threat-mitigation
The information and resources available from the Cybersecurity and Infrastructure Security Agency (CISA) will help individuals, organizations, and communities create or improve an existing insider threat mitigation program. The key steps to mitigate insider threat are Define, Detect and Identify, Assess, and Manage. On-site outreach resources are available to critical infrastructure stakeholders at no cost.

Improvised Explosive Device Awareness Training:
https://www.cisa.gov/office-bombing-prevention-obp
The Office for Bombing Prevention (OBP) leads the Department of Homeland Security's (DHS) efforts to implement the National Policy for Countering Improvised Explosive Devices (National Counter-IED policy) and enhance the nation's ability to prevent, protect against, respond to, and mitigate the use of explosives against critical infrastructure; the private sector; and federal, state, local, tribal, and territorial entities. There are monthly virtual IED training opportunities that I will start sharing with you as well. On-site outreach resources are available to critical infrastructure stakeholders at no cost.

Critical Infrastructure Security Exercises:
https://www.cisa.gov/critical-infrastructure-exercises
CISA has several types of exercise packages from discussion-based to table-top exercises. The CISA Table-Top Exercise Packages (CTEPs) serve as an off-the-shelf solution for a variety of exercise needs. We can be resources for supporting any of these exercises as needed.

Cybersecurity and Physical Security Convergence
https://www.cisa.gov/cybersecurity-and-physical-security-convergence
The adoption and integration of Internet of Things (IoT) and Industrial Internet of Things (IoT) devices has led to an increasingly interconnected mesh of cyber-physical systems (CPS), which expands the attack surface and blurs the once clear functions of cybersecurity and physical security.

Simple Steps for Real Threats

Ray Girdler
DESE Director of Data Use & Privacy
ray.girdler@ade.arkansas.gov

Why are we here?

IT

Who is responsible for cybersecurity?

technology

people

vendors

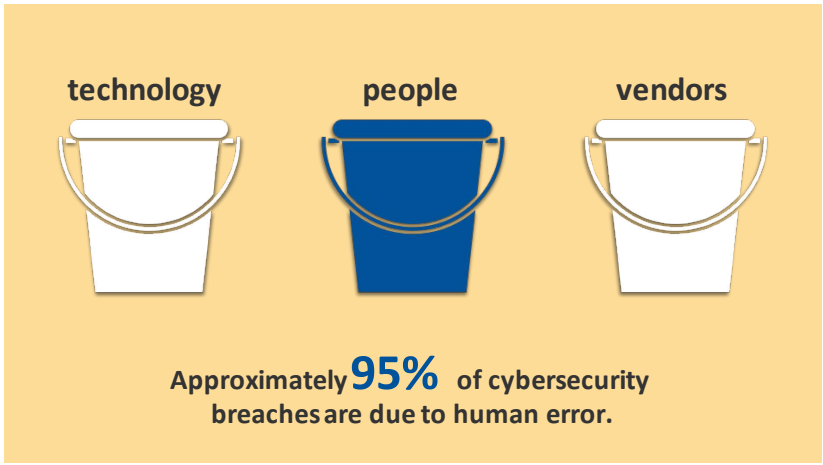
Cybersecurity is not just an IT issue.

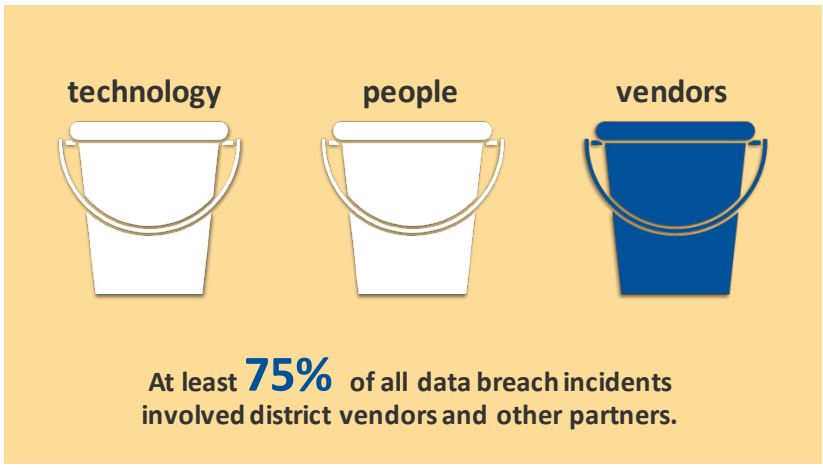
technology

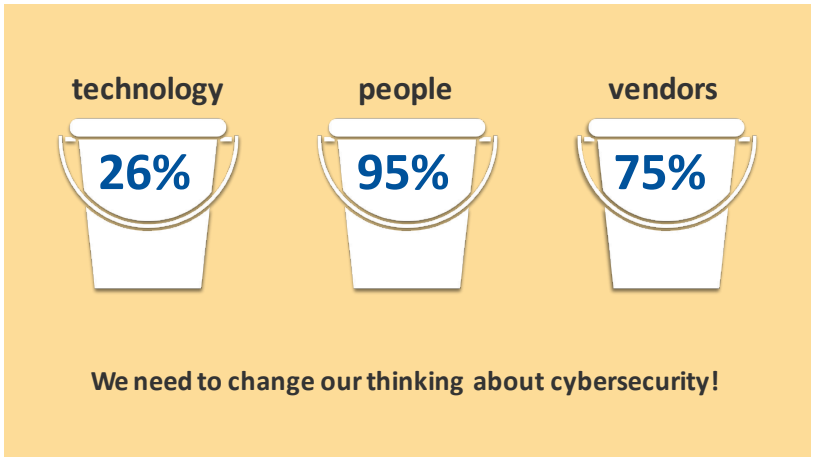
people

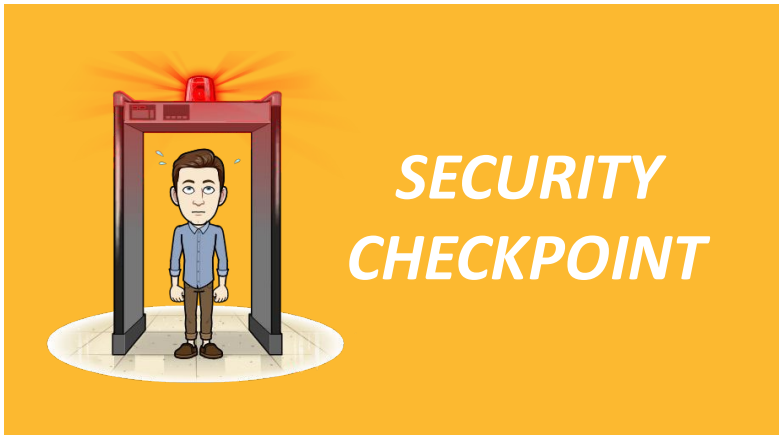
vendors

Technology alone would only address **26%** of the security vulnerabilities.


technology
people
vendors
Approximately 95% of cybersecurity breaches are due to human error.


technology
people
vendors
At least 75% of all data breach incidents involved district vendors and other partners.


technology
26%
people
95%
vendors
75%
We need to change our thinking about cybersecurity!


SECURITY CHECKPOINT

How frequently does your district provide **data privacy** or **security** training?

Students choose an option

To your knowledge, has your district ever completed a **risk assessment** or **data inventory**?

Students choose an option

To your knowledge, has your district ever conducted a **phishing test**?

Students choose an option

Employees in my district know how to identify and report **data incidents** .

Students choose an option

There are people in my district who have their **usernames** and **passwords** in plain sight.

Students choose an option

There are people in my district who share their **usernames** and **passwords** with others.

Students choose an option

Have you ever received notification that your **personal information** was **compromised** ?

Students choose an option

Has your district ever been part of a **data incident** that compromised student or staff records?

Students choose an option

How many **data incidents** do you think went <u>unreported</u> in your district last year?

Students choose an option

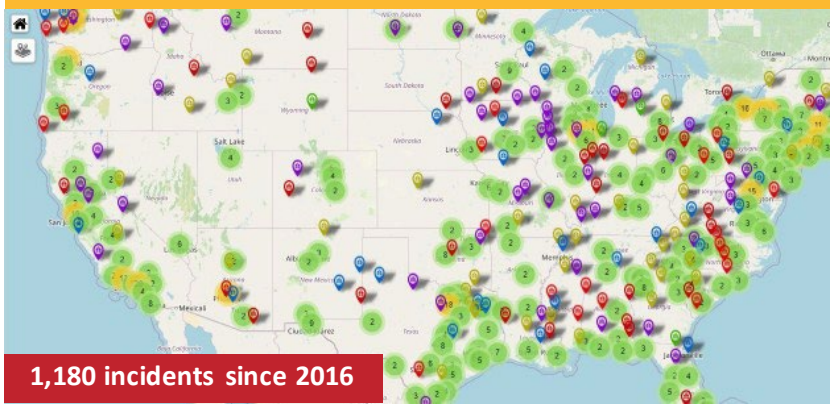
Pear Deck Interactive Slide
Do not remove this bar

I'M HERE TO HELP!

Security Awareness

Security is not just an IT issue

https://k12cybersecure.com/map



1,180 incidents since 2016

2 in 5

have indicated

lost or **stolen** data.

21

that is

110 of 276

AR school districts.

22

that is possibly

190,000

AR student records.

23

which is

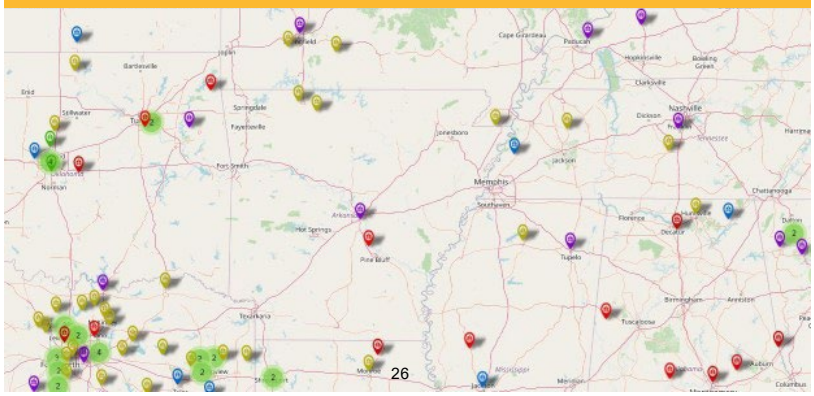
22 times

the incidents being **publicly** reported.

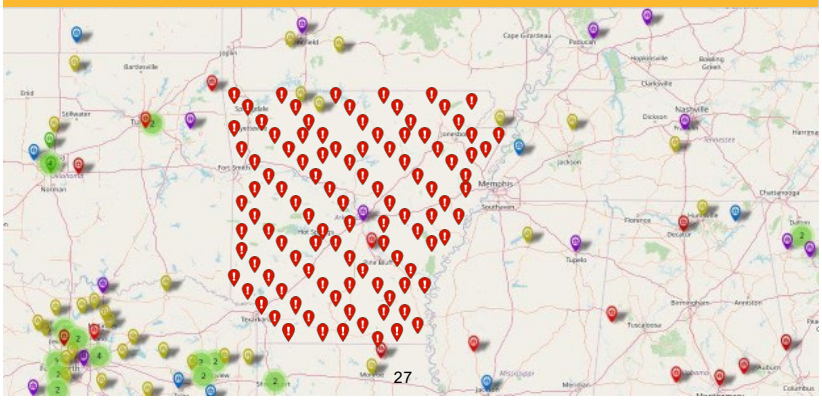
24

How would this map look with x 22 incidents?

How would AR look with x 22 incidents?



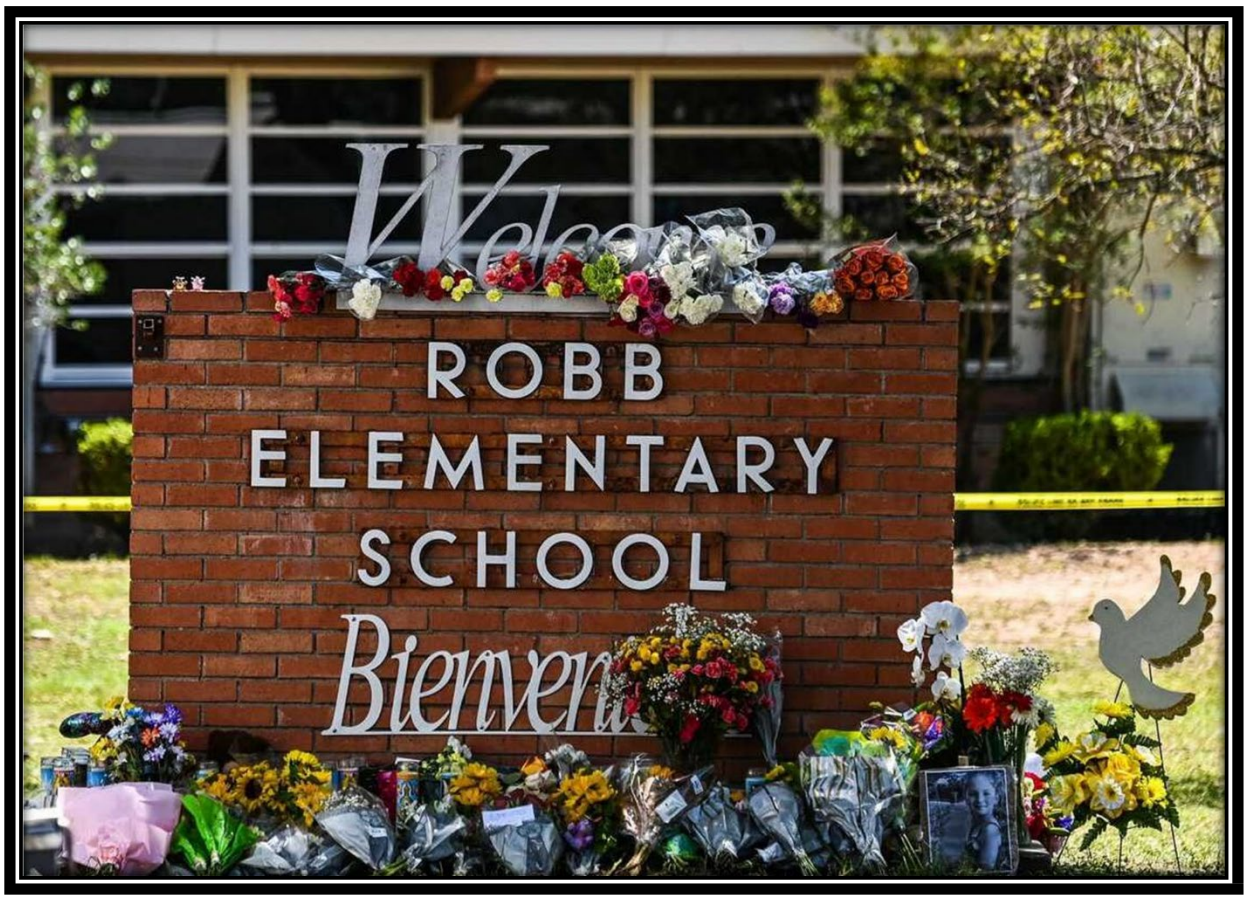
At 22 times AR would have 110 incidents



post-**pandemic**

+ attempts have increased 6 fold +
+ num. of devices increased exponentially +
+ connectivity increased exponentially +
+ data transfers increased exponentially +
+ num. of vendors increased exponentially +

Robb Elementary School Attack Response Assessment and Recommendations



ADVANCED LAW ENFORCEMENT RAPID RESPONSE TRAINING

ALERRT

TEXAS STATE UNIVERSITY

Table of Contents

The following abbreviations are used throughout the report.

ISS – Internal School Surveillance
FH – Funeral Home video footage
OS – Officer Statement
IOI – Investigating Officer Interview
BWC – Body Worn Camera
UPD CS – Uvalde Police Department Call Sheet
RL – Radio Logs
UCISD PD – Uvalde Consolidated Independent School District Police Department
UPD – Uvalde Police Department
DPS – Texas Department of Public Safety
BP – Border Patrol
BORTAC – Border Patrol Tactical Teams

This report was created using school video, third party video exterior of school, body cameras, radio logs, verbal testimony of officers on scene, and verbal statements from investigators. This report should not be considered a definitive or final report as all investigatory options have not been exhausted at this point. This report should be considered a living document. It is subject to changes as new or further evidence becomes available. This report is being compiled for the explicit purpose of identifying training gaps to be addressed by police officers across the state of Texas. The authors of this report are subject matter experts in their field of active attack incidents, patrol, and tactical operations with over 150 years of combined experience. These are the expert opinions based on experience, research, and studies of other incidents and not a formal accusation of the responders on this incident.

Introduction

Robb Elementary School in Uvalde, Texas was attacked on May 24, 2022. The attack resulted in 21 fatalities (19 students and 2 teachers) and 17 injuries. The Texas Department of Public Safety contacted the Advanced Law Enforcement Rapid Response Training (ALERRT) Center soon after the attack to assess the law enforcement response. The ALERRT Center was selected for this task for a variety of reasons. First and foremost, ALERRT is nationally recognized as the preeminent active shooter / attack response training provider in the nation. ALERRT was recognized as the national standard in active shooter response training by the FBI in 2013. ALERRT's excellence in training was recognized in 2016 with a Congressional Achievement Award.

More than 200,000 state, local, and tribal first responders (over 140,000 law enforcement) from all 50 states, the District of Columbia, and U.S. territories have received ALERRT training over the last 20 years. The ALERRT course catalog includes several courses designed to prepare first responders to 1) isolate, distract, and neutralize an active shooter, 2) approach and breach a crisis site using traditional and non-traditional methods, 3) incorporate effective command to manage a rapidly evolving active situation, and 4) manage traumatically injured patients to improve survivability. ALERRT's curriculum is developed and maintained by a team of subject matter experts with over 150 years combined law enforcement, fire, and tactical experience.

ALERRT training is research based. The ALERRT research team not only evaluates the efficacy of specific response tactics (Blair & Martaindale, 2014; Blair & Martaindale, 2017; Blair, Martaindale, & Nichols, 2014; Blair, Martaindale, & Sandel, 2019; Blair, Nichols, Burns, & Curnutt, 2013;) but also has a long, established history of evaluating the outcomes of active shooter events to inform training (Martaindale, 2015; Martaindale & Blair, 2017; Martaindale, Sandel, & Blair, 2017). Specifically, ALERRT has utilized case studies of active shooter events to develop improved curriculum to better prepare first responders to respond to similar situations (Martaindale & Blair, 2019).

For these reasons, ALERRT staff will draw on 20 years of experience training first responders and researching best practices to fulfill the Texas DPS request and objectively evaluate the law enforcement response to the May 24, 2022, attack at Robb Elementary School. This initial report will be focused on the portion of the response up until the suspect was neutralized.

The information presented in this report is based on a incident briefing held for select ALERRT staff on June 1, 2022. The briefing, which was held for approximately 1 hour, was led by an investigating officer with knowledge of the event and investigative details. Briefing materials included surveillance footage from the school, Google Maps, a brief cell phone video, and verbal questions and answers between ALERRT staff and the investigator. We were first oriented to the location of this incident by the investigator via Google Maps. We were then given a chronological timeline of events and actions by the investigator as we reviewed the cell phone and school surveillance video. All times presented in this report are based on timelines provided by investigators. Additionally, we have received additional information as the investigation is still ongoing. The timeline presented here is based on the most current information as of 6/30/2022.

The report will begin by presenting a thorough timeline of events as evidenced through video footage and details garnered from the ongoing investigation. Each entry cites the data source (refer to abbreviations presented on the Table of Contents). Following the timeline, we will comment on tactics utilized by responding officers. Information related to breaching options will be presented as a supplemental attachment at the end of the report. The tactical discussion is the opinion of ALERRT, and it is based on years of extensive training, research, and an ever-evolving understanding of active shooter response. The concepts discussed are foundational to ALERRT's nationwide training curriculum. While the discussion will be frank and objective, it is not meant to demean the actions taken by law enforcement during this incident. Rather, the discussion is intended to improve future response. For this reason, attention will be drawn to actions that worked well and actions that did not.

Detailed Timeline

Figure 1. Overhead View

At 11:27:14, a female teacher (Female 1) exits the exterior door in the west hall propping the door open with a rock to prevent it from closing behind her (see Figure 2 for suspect entry point). (ISS)

At 11:28:25, the suspect becomes involved in a motor vehicle crash in a dry canal near the elementary school. Two people from a nearby business approached the crash scene at 11:29:02. The suspect engaged them both with a rifle. The two people were able to flee back to the business unharmed and called 9-1-1. (FH)

At 11:29:40, Female 1 returns through the west entry deliberately kicking the rock from the door jamb. Female 1 pulls the door shut and continues to look out of the exterior door as she is frantically speaking on her cell phone. Female 1 attempts to enter a door on the south side of the west hallway only to find it locked. Female 1 knocked on the door, and it was eventually answered by another female (Female 2). Female 1 appears to advise Female 2 of the emergency whereupon Female 2 re-enters her room and secures the door. Female 1 moves into a room closest to the exit on the north side of the west hallway. Female 1 re-enters the hallway numerous times yelling down the hall for students to get into their classrooms. (ISS)

At 11:30:14, the suspect, wearing dark clothing and carrying a bag, left the crash scene and climbed a chain-link fence onto the elementary school property. The suspect walked deliberately across the open grounds between the fence and the teachers' parking lot. The suspect moved towards the school buildings on the westmost side of the campus. Although a defect that might have been caused by a bullet was located on a building south of the affected structure, it could not be

substantiated at this time that any rounds were fired at a teacher and children on the playground at the time of the crash. (FH)

At 11:31:36, the suspect is captured on video between the cars shooting, and a Uvalde Patrol unit is captured arriving at the crash site. (FH)

At 11:31:43, a Uvalde Consolidated Independent School District Police officer drives through the west gate near the crash site and across the field to the south side of the affect building, at a high rate of speed. (FH)

At 11:32:08, the suspect reached the west teachers' parking lot adjacent to the affected building and fired through windows into the westmost rooms prior to entering the building. (FH and audio file from ISS)

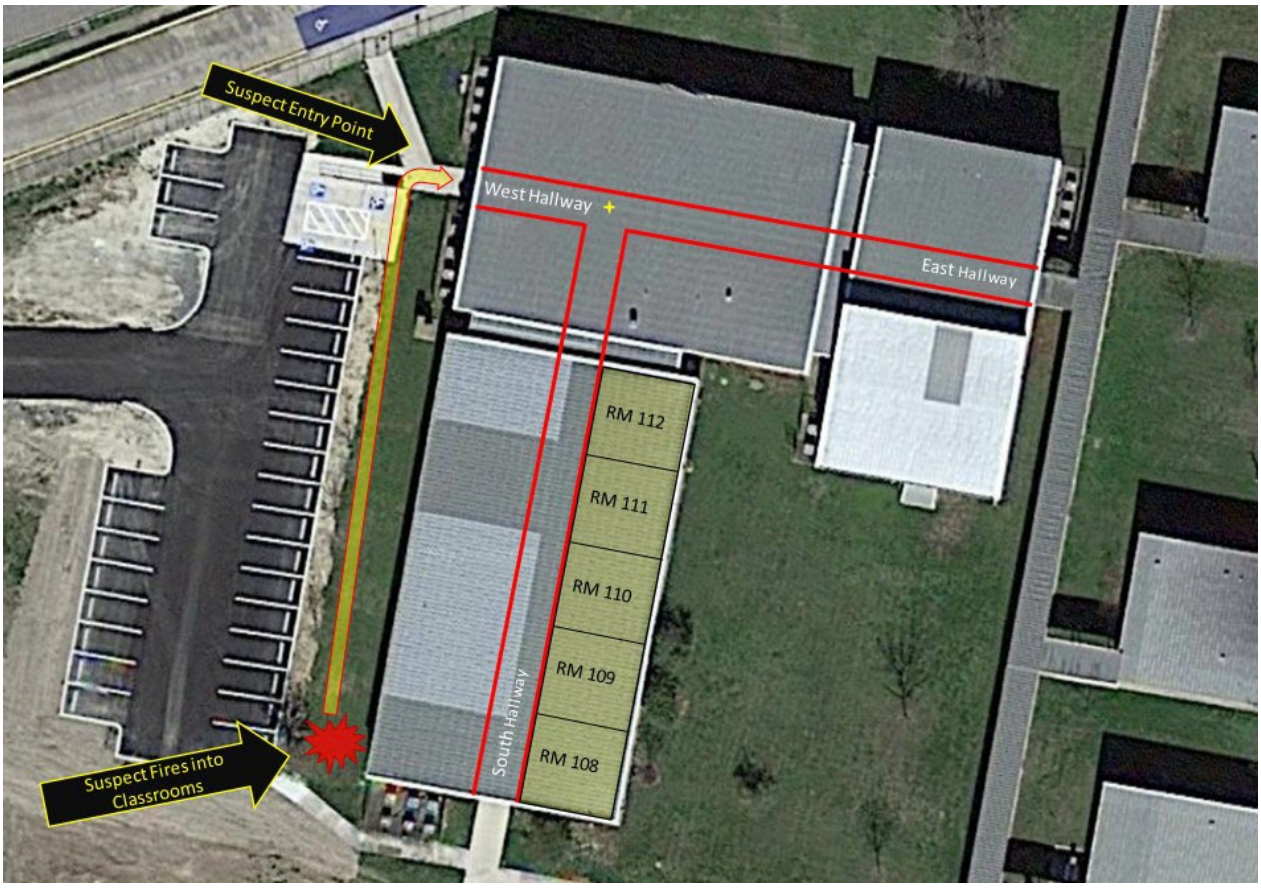


Figure 2. Suspect Entry Point

Prior to the suspect's entry into the building at 11:33:00, according to statements, a Uvalde Police Officer on scene at the crash site observed the suspect carrying a rifle outside the west hall entry. The officer, armed with a rifle, asked his supervisor for permission to shoot the suspect. However, the supervisor either did not hear or responded too late. The officer turned to get confirmation from his supervisor and when he turned back to address the suspect, he had entered the west hallway unabated. (OS per investigating officer interview).

Note: *The internal school surveillance (ISS) video consisted of a ceiling-mounted camera that was situated at the intersection of three intersecting hallways (as indicated by the yellow star in Figure 3) This camera captured 1) the suspect's entry point, which was the short (West) hallway leading to an exterior door; 2) a second long hallway (South) with multiple classrooms on either side of the hall and an exterior door at the southmost end of the hall; and 3) a third hallway (East) that leads to other classrooms, restrooms, a teachers' lounge, a library, and an exterior door at the eastmost end of the hallway.*

Figure 3. West Building Layout

At 11:33:00, the suspect enters the school from the exterior door in the west hall while holding a rifle. The suspect looked around the hallway and then continued to walk down the west hallway before turning right (down the south hallway). The suspect walked past a series of rooms with closed doors and a firewall "break." before making his way to room 111 and 112. (ISS)

At 11:33:24, upon reaching rooms 111 and 112, the suspect fired a series of rounds from the hallway in the direction of classrooms 111 and 112. (ISS)

At 11:33:32, the suspect made entry into what appears to be classroom 111. Immediately, children's screams could be heard along with numerous gunshots in the classrooms. The rate of fire was initially very rapid then slowed, lasting only a few seconds. (ISS)

At 11:33:37, the suspect backed out of what appears to be classroom 111 into the south hallway. The suspect made a slight turn to what appears to be his left and fires a series of rounds from the hallway into classroom 112. The suspect then re-enters what appears to be classroom 111 and continues to fire what is estimated to be over 100 rounds by 11:36:04 (according to audio analysis). During the shooting the sounds of children screaming, and crying, could be heard (according to audio analysis). (ISS)

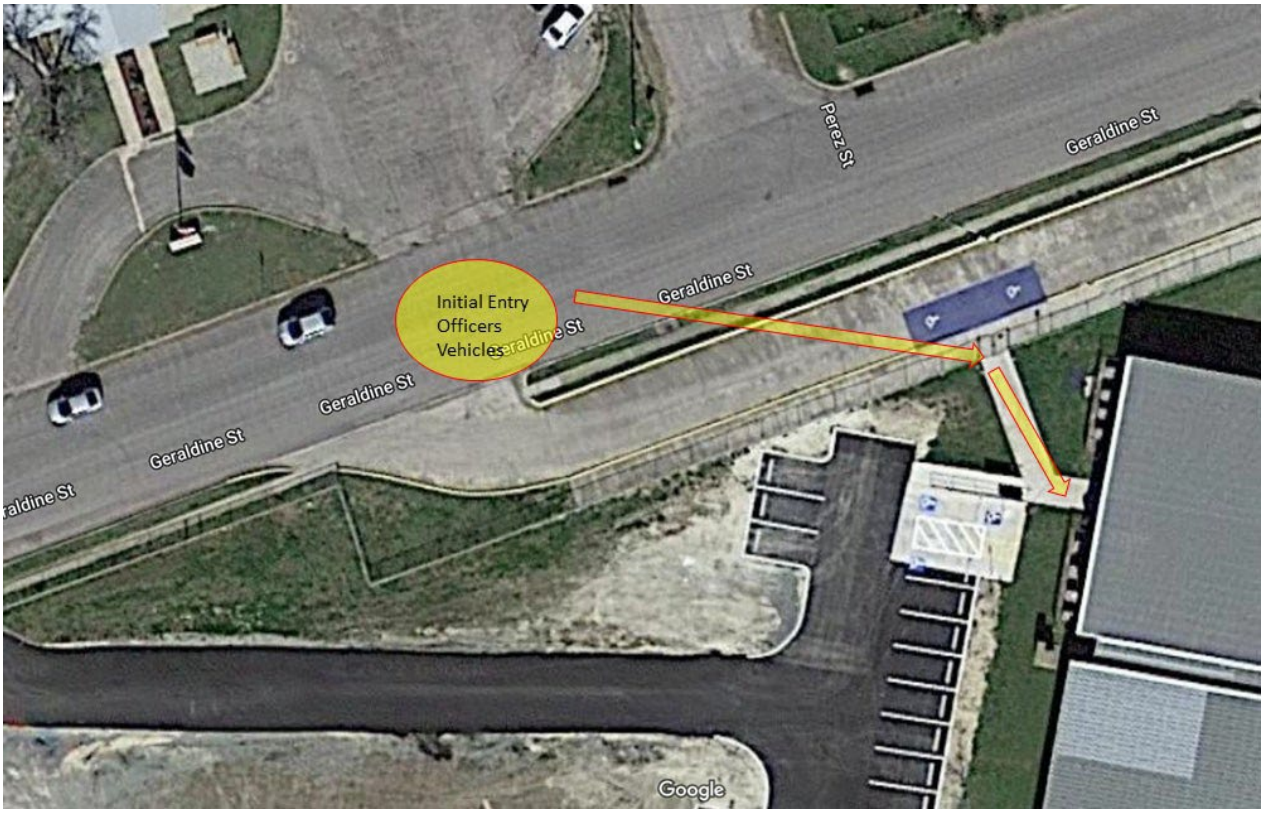


Figure 4. Officers Initial Entry into West Building

After the suspect made entry into the west building, three Uvalde Police Department (UPD) officers gathered on Geraldine Street (behind police vehicles) in front of the school drop-off / pick-up area. Then the officers, using a bounding overwatch tactic, move quickly (one at a time) to the west door.

At 11:35:55, all three Uvalde Police Department (UPD) officers entered the structure through the west door into the west hallway. These officers were equipped with the following: one with external armor and two with concealable body armor, two rifles, and three pistols. At 11:36:00, four officers entered the south hallway through the south door closest to the suspect. It is not clear what equipment these officers had with them. Four more officers entered the west hallway through the west door at 11:36:03. Three of these officers were from the UPD and one was from the Uvalde Consolidated Independent School District Police Department (UCISD PD). They were equipped with three external body armor carriers and one with concealable body armor and pistols. (ISS)

It did not appear that any of the officers were in possession of breaching tools, medical equipment, ballistic shields, or "go-bags." (ISS)

NOTE: *A "go-bag" is typically a bag or backpack that is widely used in the law enforcement community to respond to critical incidents. The "go-bag" commonly consists of spare ammunition, medical equipment, and breaching tools. The purpose of the "go-bag" is to carry equipment needed for a specialized response, when carrying that equipment on a regular basis is not feasible. Taking a "go-bag" into a crisis site facilitates the availability and implementation of these tools in a patrol response where tactical assets and teams are not readily available.*

At 11:36:04, the last shots from the initial barrage from the suspect were fired. There were seven officers in the west hallway and four officers in the south hallway. (ISS)

At 11:36:10, officers from the west and south hallway advanced to rooms 111 and 112. As the officers entered the threshold of rooms 111 and 112, they were fired upon by the suspect, who was in room 111. The gunfire at 11:37:00 and 11:37:10 drove the officers away from the threshold of room 111 and 112 and back to the west and south hallways prior to either team making contact with either room 111 or 112 classroom doors. (ISS)

At 11:38:38, the suspect concludes firing, according to audio estimates 11 rounds are fired. (ISS)

Investigators advised that two officers were injured by building material fragments caused by the suspect's rounds passing through the walls. (IOI and ISS)

Officers generally remained at the intersection of the west and south hallway and in the south hallway near the south entrance until the final assault. (IOI and ISS)

At 11:38:11, officers on scene, but outside of the hallway, call for additional assistance to include a tactical team with specialized capabilities. (BWC and UPD CS)

At 11:38:37, an officer outside of the hallway advises the suspect "is contained." (BWC)

At 11:40:58, the suspect fires 1 round according to audio estimates. (ISS)

At 11:41:30, dispatch asked via radio if the door was locked, a UPD officer responds, "I am not sure, but we have a hooligan to break it." (BWC)

At 11:44:00, the suspect fires one more round according to audio estimates. (ISS)

At 11:48:18, a UCISD PD officer enters through the west hallway door and states, “She says she is shot,” referring to his wife. He is escorted outside of the building. (BWC)

By 11:51:20, law enforcement from various agencies (including UPD, UCISD PD, Uvalde Sheriff's Office (USO), Fire Marshals, Constable Deputies, Southwest Texas Junior College Police Department (SWTJC PD), and the United States Border Patrol (BP) had arrived at the scene and were moving inside and out to evaluate the situation. (ISS, UPD CS, RL)

At 11:52:08, the first ballistic shield entered the west hallway. (ISS)

At 11:53:10, a Texas Department of Public Safety (DPS) special agent arrived at the perimeter and was advised to man the perimeter. Another officer makes a comment about there being kids still in the building, the DPS special agent advised, “if there is then they just need to go in.”

At 11:56:49, the DPS special agent states “there's still kids over here. So, I'm getting the kids out!” (BWC)

At 12:03:51, a second ballistic shield arrives, and at 12:04:16 a third shield arrives on scene in the west hallway. (ISS)

At 12:06:16, UPD RL notes that no Command Post is set up, advised bodies needed to keep parents out. (RL)

At 12:10:17, officers in the west hallway begin passing out and donning gas masks. (ISS)

At 12:14:10, CS gas cannisters and launcher deliverable varieties are brought in. (ISS)

By 12:13:00, dispatchers had received numerous 9-1-1 calls from a child explaining that there were several children and one of her teachers deceased and another teacher hurt in room 112. (UPD 9-1-1)

At 12:15:27, it appears tactical team members of United States Border Patrol Tactical Teams (BORTAC) arrive and assist with fortifying the law enforcement position at the intersection with ballistic shields. (ISS)

At 12:20:46, a fourth ballistic shield arrives in the west hallway. (ISS)

At 12:21:08, four shots are fired by the suspect from within one of the two classrooms. (ISS)

At 12:21:22, BORTAC members move to a set of double doors within 36’ of rooms 111 and 112 bringing two ballistic shields. However, no assault on the rooms was conducted. (ISS)

At 12:23:35, BP medical team members began setting up medical triage in the east hallway in front of the restrooms. They had numerous backboards, medical kits, a defibrillator as well as bleeding control supplies. (ISS)

From 12:21:16 until 12:34:38, a continuous conversation takes place in the south hallway, involving UCISD PD Chief Arredondo and a UPD officer discussing tactical options and considerations including snipers, windows, and how to get into the classroom. They also discussed who has the keys, testing keys, the probability of the door being locked, and if kids and teachers are dying or dead. (BWC)

At 12:35:39, BP agents arrive in the west hallway with the first observed breaching tool, a Halligan tool. (ISS)

From 12:37:45 until 12:47:25, UCISD PD Chief Arredondo attempts to negotiate with the suspect, speaking in English and Spanish. The Chief also calls someone to try to look into the windows from outside, he then begins asking for more keys. At 12:46:18, he exclaims, “If y’all are ready to do it, you do it. But you should distract him out that window.” At 12:47:25, Chief Arredondo states, “He’s going in! He’s going in! Tell those guys on the west that they’re going in! Let ’em know!” (BWC)

At 12:47:57, a USO deputy arrives in the west hallway with a sledgehammer. (ISS)

At 12:50:03, an ad Hoc team assaults room 111, neutralizing the suspect. The suspect had concealed himself in a book closet, he then emerged when the team made entry. Footage showed officers frantically carrying the dead and injured to the casualty collection point (CCP) in the east hallway. Some law enforcement officers rushed casualties directly through the exterior door at the end of the west hallway. It is unknown if medical personnel (EMS) were staged nearby for direct patient handoff. (ISS)

The result of this incident was 19 children and two adults killed with an additional 17 reported injuries. Additionally, the suspect was neutralized through gunfire in the assault.

Physical Site Assessment

The investigator escorted ALERRT staff to the crime scene for a site walkthrough. As expected, there was a large quantity of dry blood on the floors in all three hallways. There were noticeable penetrating ballistic defects throughout various walls in the south hall.

The classroom doors were inset just over 36” into a 90-degree inset from the hallway to accommodate the swing of the outward opening classroom doors towards the hall. Each inset had two separate doors, side-by-side, leading into a separate classroom. The door on the left-hand side of the inset opened outward from right to left, and the door on the right-hand side of the inset opened outward from left to right as seen in Figure 5.

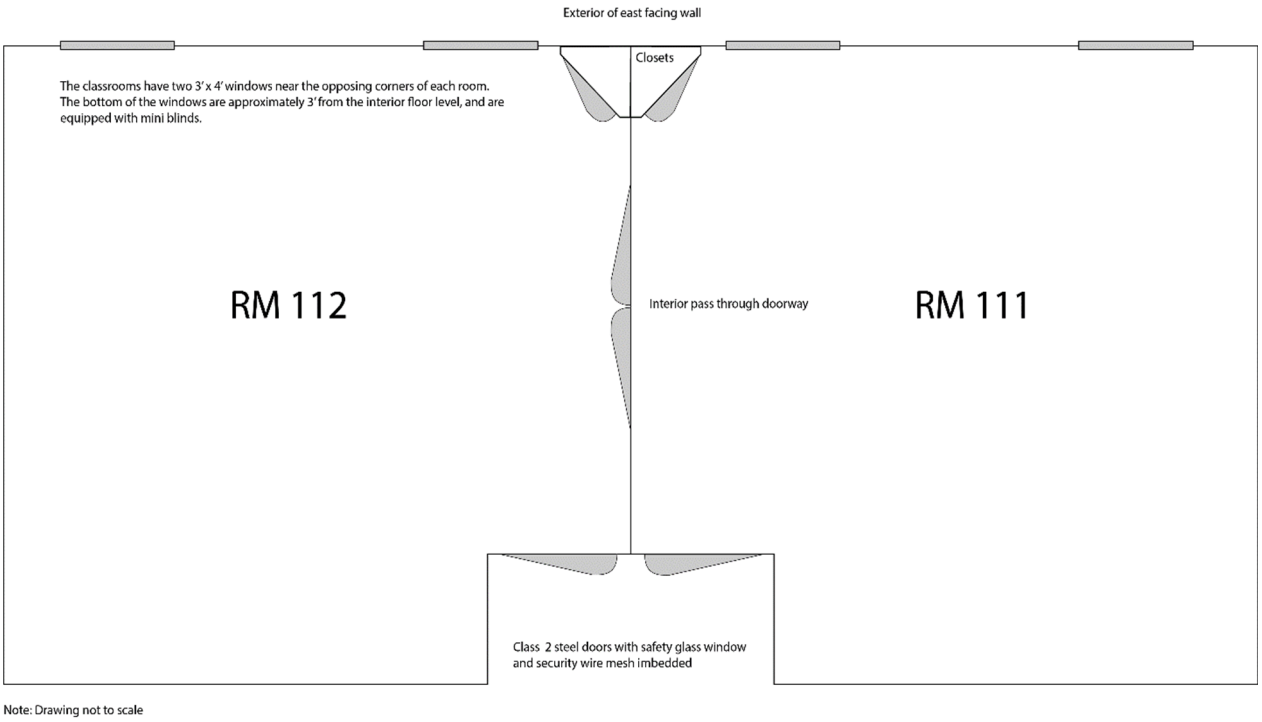


Figure 5. Classroom Layout

The classroom doors were class 2 steel doors. The classroom doors had safety glass with security wire mesh imbedded (see Figure 6). The hardware consisted of a single metal door handle locking latch, three exterior metal hinges, and a door closure device mounted to the top inside portion of the door. The door jambs were composed of steel and set in a metal stud and sheetrock wall.

Figure 6. Class 2 Steel Door

The door to room 111 had been removed for evidentiary purposes and collection. Once the evidence had been removed the door was left on the floor of the room. The door for room 112 was intact and in place. There was a noticeable concentration of exiting bullet defects in the area of the inset. There were noticeable bullet defects on the door jamb of classroom 111, approximately 5’ from floor level. Both rooms 111 and 112 possessed an extraordinary amount of dry blood concentrated on the floor.

The exterior walls of each classroom had two 3’ x 4’ windows near the opposing corners of each classroom (see Figure 3). The bottom of each window was approximately 3’ from interior floor level, and they were equipped with mini blinds. From the exterior, the windows were approximately 4’ from ground level. The windows were composed of a heavy aluminum frame with three lateral cross beams that held four (4) 1’x3’ panes of tempered glass, as seen in Figure 7.

Figure 7. Exterior Classroom Window

An exterior window on the right-hand side as you enter room 111 had a clear bullet defect. Based on the fragmented spiderweb pattern it was evident that the window was composed of safety glass, which fragments into small pieces when it is struck with enough force to break.

It appears the investigative teams cut out sections of sheetrock in the south hall to collect evidence. The interior walls were constructed with vertical metal studs every 16”. Pink fiberglass insulation was installed between each vertical metal stud and was encapsulated between sheetrock material to form walls that separated each “paired” set of classrooms.

An assessment of the classroom closet, on the exterior wall, which is directly opposite of the classroom door, revealed that the exterior wall was cinder block on the inner portions and decorative brick on the exterior (as seen in Figure 7).

Tactical Assessment

While the previous section detailed the timeline, the following discussion will assess different tactical issues present in the response. We will use the most recent version of our Level I manual (v.7.2) as our primary reference (ALERRT & FBI, 2020). We are breaking this discussion into three parts: 1) circumstances outside the building prior to suspect entering building, 2) initial officer response, and 3) changing environment leading to the eventual assault on room 111.

Circumstances Before the Suspect Entered the Building

We identified three key issues that occurred prior to the suspect gaining entry to the building. First, a teacher propped open the exterior door at 11:27:14. ALERRT staff noted rocks (some of which were painted) were placed at most external doors of the building. Based on this observation, it appears that propping doors open is common practice at this school. While the teacher did kick the rock and close the door prior to the suspect making entry, and the propping open of the door did not affect what happened in this situation, circumventing access control procedures can create a situation that results in danger to students. After the teacher closed the door, she did not check to see if the door was locked. Perhaps this was because the door is usually locked. However, on this day the door was not locked, and because it was not locked, the attacker was able to immediately access the building. This again highlights the importance of not circumventing access control procedures. Even if the teacher had checked to see if the door was locked, it appears that she did not have the proper key or tool to engage the locking mechanism on the door. Finally, we note that the door was a steel frame with a large glass inlay. This glass was not ballistic glass, nor was there film on the glass to maintain the integrity of the door if the suspect shot the glass. This suggests that the suspect would have been able to gain access to the building even if the door was locked.

Second, one of the first responding officers (UCISD PD) drove through the parking lot on the west side of the building at a high rate of speed. The suspect was in the parking lot at this time, but the officer did not see him. If the officer had driven more slowly or had parked his car at the edge of the school property and approached on foot, he might have seen the suspect and been able to engage him before the suspect entered the building (ALERRT & FBI, 2020, p. 3-4.)

Third, a Uvalde PD officer reported that he was at the crash site and observed the suspect carrying a rifle prior to the suspect entering the west hall exterior door. The UPD officer was armed with a rifle and sighted in to shoot the attacker; however, he asked his supervisor for permission to shoot. The UPD officer did not hear a response and turned to get confirmation from his supervisor. When he turned back to address the suspect, the suspect had already entered the west hall exterior door at 11:33:00. The officer was justified in using deadly force to stop the attacker. Texas Penal Code § 9.32, DEADLY FORCE IN DEFENSE OF PERSON states, an individual is justified in using deadly force when the individual reasonably believes the deadly force is immediately necessary to prevent the commission of murder (amongst other crimes). In this instance, the UPD officer would have heard gunshots and/or reports of gunshots and observed an individual approaching the school building armed with a rifle. A reasonable officer would conclude in this case, based upon the totality of the circumstances, that use of deadly force was warranted. Furthermore, the UPD officer was approximately 148 yards from the west hall exterior door. One-hundred and forty-eight yards

is well within the effective range of an AR-15 platform. The officer did comment that he was concerned that if he missed his shot, the rounds could have penetrated the school and injured students. We also note that current State of Texas standards for patrol rifle qualifications do not require officers to fire their rifles from more than 100 yards away from the target. It is, therefore, possible that the officer had never fired his rifle at a target that was that far away. Ultimately, the decision to use deadly force always lies with the officer who will use the force. If the officer was not confident that he could both hit his target and of his backdrop if he missed, he should not have fired.

If any of these three key issues had worked out differently, they could have stopped the tragedy that followed. First, had the exterior door been secured, the suspect may have never gained access to the building. At the very least, the suspect would have been delayed and responding officers would have had more time to find and stop the shooter before he entered the building. The UCISD PD officer might have seen the suspect had the officer not been driving as fast or if he had approached on foot. Lastly, had the UPD officer engaged the suspect with his rifle, he may have been able to neutralize, or at least distract, the suspect preventing him from entering the building.

Initial Response Within Building

We identified three key issues that occurred before the suspect entered rooms 111 and 112 for the last time. First, Uvalde ISD had protocols in place requiring doors to remain locked at all times, and the school was currently on an active lockdown prior to the suspect gaining entry to the school. The suspect was still able to gain access to room 111. We received information from the investigating officer that the lock on room 111 had been reported as damaged multiple times; however, this has not been confirmed through work orders at this time. Regardless, the suspect is seen entering the room, exiting the room, and then reentering the room again prior to officers entering the building at 11:35:55. The only way to engage the lock is to insert a key from the hallway side of the door. At no point is the suspect observed entering the hallway and engaging the locking mechanism. Based upon this, we believe that the lock to room 111 was never engaged.

The second issue involves having teams of officers at both ends of the south hallway. ALERRT teaches that a single team should be in a single area of building at a time (ALERRT & FBI, 2020, pp. 2-20 to 2-26 & 7-4). Having multiple teams or splitting an existing team can create a crossfire situation. If the suspect had emerged from the classrooms, officers from both teams presumably would have opened fire resulting in a high likelihood of officers at either end of the hallway shooting officers at the other end. The teams should have quickly communicated, and officers at one end of the hallway should have backed out and redeployed to another position. Additionally, ALERRT teaches that teams consist of up to 4 members (ALERRT and FBI, 2020, pp. 4-1 to 4-27). Teams larger than 4 tend to create congestion and interfere with the ability of the team to operate quickly and effectively. Therefore, once 4 officers were in the south hallway area of the building, no additional officers were needed in that area. Additional officers should have been assigned other tasks.

The third issue revolves around losing momentum. The first three responding UPD officers enter the west hall exterior door at 11:35:55 and an additional four officers entered the south hall at

11:36:00. Audio recordings indicate the suspect was actively firing his weapon until 11:36:04. The first responding officers correctly moved toward the active gunfire, which was acting as their driving force (ALERRT & FBI, 2020, pp. 2-15 to 2-16, 2-26, 2-33). The seven officers converged on rooms 111 and 112 at 11:37:00. As the officers approached the doors, the suspect began firing. This gunfire caused both teams of officers to retreat from the doors. We note that the officers **did not** make contact with the doors (i.e., they never touched any part of the doors). The team approaching from the north fell back to the T-intersection of the west and south hallways. This position is approximately 67 feet from the doors of rooms 111 and 112. The team approaching from the south fell back to the south end of the south hallway. The team in the south hallway were not visible on camera, so their distance from the affected classrooms is unknown.

ALERRT teaches that first responders' main priority in an active shooter situation is to first **Stop the Killing** and then **Stop the Dying** (ALERRT & FBI, 2020, pp. 2-9, 2-15 to 2-16). Inherent in both stopping the killing and dying is the priority of life scale (ALERRT & FBI, 2020, pp. 2-6 & 2-34). At the top of this scale, the first priority is to preserve the lives of victims/potential victims. Second, is the safety of the officers, and last is the suspect. This ordering means that we expect officers to assume risk to save innocent lives. Responding to an active shooter is a dangerous task (Blair & Duron, 2022). There is a chance that officers will be shot, injured, or even killed while responding. This is something that every officer should be acutely aware of when they become a law enforcement officer.

To adhere to the priority of life, the first responding officers' actions should be determined based on the current driving force. In this instance, there is a suspect actively shooting inside an occupied elementary school. The active gunfire is the driving force, and the officers correctly responded to this driving force by moving toward the rooms that were being attacked.

Ideally, the officers would have placed accurate return fire on the attacker when the attacker began shooting at them. ALERRT trains the widely-used ABCs of cover – **A**ccurate return fire, **B**ody armor, and **C**over (ALERRT & FBI, 2020. p. 2-21; Blair et al., 2013). The ABCs give the first responder a tiered approach to achieving cover while maintaining control of the situation. Further, the ABCs are presented in order of preference (A first, B second, C third). As noted in Figure 6, there was a window in the center of each classroom door. Officers could have utilized the window to send accurate return fire back at the suspect. Even though the room was darker than the hallway, the suspect would have been backlit by the exterior windows and muzzle flashes would have been present. Obviously, this return fire must be consistent with the fundamental firearms safety rules (e.g., the officers must ensure that students will not be hit by the officers' return fire). Any officer with body armor should have squared their body armor to the threat to improve protection. In this situation, we don't believe the last course of action (moving to cover) was a viable option because the interior construction of the school would not stop bullets, and therefore, was not cover. Maintaining position or even pushing forward to a better spot to deliver accurate return fire would have undoubtedly been dangerous, and there would have been a high probability that some of the officers would have been shot or even killed. However, the officers also would likely have been able to stop the attacker and then focus on getting immediate medical care to the wounded.

It is not surprising that officers who had never been shot at before would be overwhelmed by the directed gunfire. This is especially the case if they had not been consistently training to deal with this type of threat. However, even after retreating, the officers were still presented with a clear driving force. The suspect was actively firing his weapon when the officers entered the building, and a reasonable officer would assume that there were injured people in the classrooms. The officers also knew the suspect was still alive and preventing them from accessing the wounded in the classrooms. These injured people are a driving force (ALERRT & FBI, 2020, p. 2-17) Once the officers retreated, they should have quickly made a plan to stop the attacker and gain access to the wounded. There were several possible plans that could have been implemented. We list a few here:

A. Perhaps the simplest plan would have been to push the team back down the hallway and attempt to control the classrooms from the windows in the doors. Any officer wearing rifle-rated body armor (e.g., plates) would have assumed the lead as they had an additional level of protection. A team of 4 officers could have utilized the windows in the doors to control a large portion of the classroom from the hallway. Two officers would have taken angular positions on each window. This would have allowed them to cover a large portion of each classroom and the officers would have been likely to see and engage the attacker. Again, this would have been dangerous, but the priority of life scale dictates that the officers assume risk to save innocent lives. It is also worth noting, the officers had weapons (including rifles), body armor (which may or may not have been rated to stop rifle rounds), training, and backup. The victims in the classrooms had none of these things. If the classroom doors were locked, some of the officers on the door windows would have been able to provide cover while the other officers breached the doors.
B. If the officers believed that they could not establish control through the doors, they should have found another way to stop the killing and dying. One option would have been to breach the exterior windows of the classrooms. Ideally, this would have involved breaking more than one window simultaneously and then raking the blinds out of the window. It is likely that the suspect would have fired at the officers, but the exterior construction of the building would have provided them with good cover. After the windows were broken (i.e., ported), the officers could have planned to simultaneously stand up in the windows to confront the attacker (i.e., cover). The room would have been substantially darker than the bright exterior conditions at the time. However, breaking the windows and raking the blinds would have increased lighting in the room. Hand-held or weapon-mounted lights could also have been used to increase visibility (see Supplementary information regarding an assessment of breaching options).
C. Both options a and b could have been done simultaneously. The window breaks could have been used to signal the start of the assault and draw the suspect's attention from the doors. The window officers would stay behind the cover of the exterior wall while the door officers had priority of fire. Then the window officers could stand and cover the rest of the room.
D. Other options (such as breaching the sheetrock walls or having an officer run past the rooms to draw fire while other officers moved up to cover the interior windows) could also have

been utilized. Each of these alternatives would have had various strengths and weaknesses but would have regained momentum for the officers.

None of these actions were taken. While it would have taken a few minutes to coordinate and execute any of these actions once the officers retreated from the rooms, taking 2, 3, 5 or even 10 minutes to do so would have been preferrable to the more than an hour it took to ultimately assault the room.

We commend the officers for quickly entering the building and moving toward the sounds of gunfire. However, when the officers were fired at, momentum was lost. The officers fell back, and it took more than an hour to regain momentum and gain access to critically injured people.

Changing Circumstances Prior to Assault

As discussed, the situation became static at 11:38:37. Prior to this, at 11:38:11, the UCISD PD Chief called for additional assistance (tactical teams and equipment). The responding officers began treating the situation as a hostage/barricade rather than an active shooter event. The timeline shows that the shooter was killed at 12:50:03. This section will describe the escalating circumstances that unraveled over the one hour, eleven minutes, and twenty-six seconds between officers taking static positions and the moment the suspect was killed. We will detail key moments where officers' capabilities increased due to arriving equipment and personnel as well as moments where the exigency of the situation increased due to either suspect actions (e.g., firing his weapon) or additional information (e.g., injured people) being communicated to the officers inside the building.

A reasonable officer would have considered this an active situation and devised a plan to address the suspect. Even if the suspect was no longer firing his weapon, his presence and prior actions were preventing officers from accessing victims in the classroom to render medical aid (ALERRT & FBI, 2020, p. 2-17).

For the sake of argument, we will assume that officers believed the active shooter situation had transformed into a hostage barricade starting at 11:38:37. We'll also assume that officers needed additional equipment and/or trained tacticians to perform the room assault. In a hostage/barricade, officers are taught to utilize the 5 Cs (Contain, Control, Communicate, Call SWAT, Create a Plan; ALERRT & FBI, 2020, pp. 2-17 to 2-19). In this instance, the suspect was contained in rooms 111 and 112. The officers established control in that they slowed down the assault. However, the officers did not establish communication with the suspect. The UCISD PD Chief did request SWAT/tactical teams. SWAT was called, but it takes time for the operators to arrive on scene. In the meantime, it is imperative that an immediate action plan is created. This plan is used if active violence occurs. It appears that the officers did not create an immediate action plan.

Factors Increasing Exigency

We identified two factors that we believe increased the exigency of the situation and should have prompted officers to execute an immediate action plan. These factors were ongoing gunfire and the presence of injured people.

Gunfire. At 11:40:58, the suspect fired one shot. At 11:44:00, the suspect fired another shot, and finally, at 12:21:08, the suspect fired 4 more shots. During each of these instances, the situation had gone active, and the immediate action plan should have been triggered because it was reasonable to believe that people were being killed.

Injured People. While it is unclear whether the information from 9-1-1 about injured people in the classrooms was being communicated to officers on the inside of the school, at 11:48:18, a UCISD PD officer enters through the west hallway door and states, "She says she is shot," referring to his wife. The officer was looking at his phone when he relayed the information to the other officers in the hallway. Based on statements, he had received a call from his wife in the room. This statement illustrates officers on scene were aware of at least one injured person in need of assistance.

Factors Increasing Capability

In addition to information that should have increased the exigency of the situation, a variety of factors increased the capabilities of the officers while dealing with these threats. These included breaching tools, shields, tactical operators, and CS gas. Please refer to Figure 8 on page 20 for a detailed timeline of the factors that increased both exigency and officer capability.

Breaching Tools. A UPD officer stated that they had a Halligan at 11:41:30 when asked by dispatch if the doors were locked. This tool was not seen on camera, and if he was referring to the tool being on scene or at the UPD is unclear. A Halligan tool was captured on camera at 12:35:39. A USO deputy arrives on scene with a sledgehammer at 12:47:57. This completed the toolset needed to breach an outward opening door.

Ballistic Shields. The first ballistic shield arrives on scene at 11:52:08. A second ballistic shield arrived at 12:03:51, a third ballistic shield arrived at 12:04:16, and a fourth ballistic shield arrived at 12:20:46. Each ballistic shield afforded first responders additional protection from potential gunfire. We do not have information about the ballistic rating of each shield at this point.

Tactical Operators. While many officers flowed through the scene, the first known tactical operators (i.e., BORTAC) arrived at 12:15:27. BORTAC operators receive extensive training and equipment to respond to barricaded suspects. Additionally, it is common for tactical operations to be turned over to tactical operators upon their arrival; however, it appears that control of tactical operations was not given to the tactical operators on scene.

CS Gas. Between 12:10:17 and 12:14:10, gas masks were passed out and CS gas cannisters and launchers were on scene.

The assault team entered the room at 12:50:03, 1 hour, 11 minutes, and 26 seconds after the first responding officers took static positions. The assault team had keys that could unlock the door. It

does not appear that any officer ever tested the doors to see if they were locked. As we described earlier, we do not believe the door to room 111 was locked.

As this section illustrates, there were multiple points in time where the driving force increased through additional gunfire; however, officers did not act on these increases in driving force. Additionally, officers on scene continually received additional equipment and tactical components that increased their capabilities to address the suspect. Ultimately it is unclear why the officers decided to assault the room at 12:50:03. There was no apparent change in driving force or response capability at this point.

While we do not have definitive information at this point, it is possible that some of the people who died during this event could have been saved if they had received more rapid medical care. In the next part of this AAR, we intend to address that Stop the Dying portion of the response that occurred following the killing of the suspect.

Additionally, we have noted in this report that it does not appear that effective incident command was established during this event. The lack of effective command likely impaired both the Stop the Killing and Stop the Dying parts of the response. The final part of this AAR will address incident command issues.

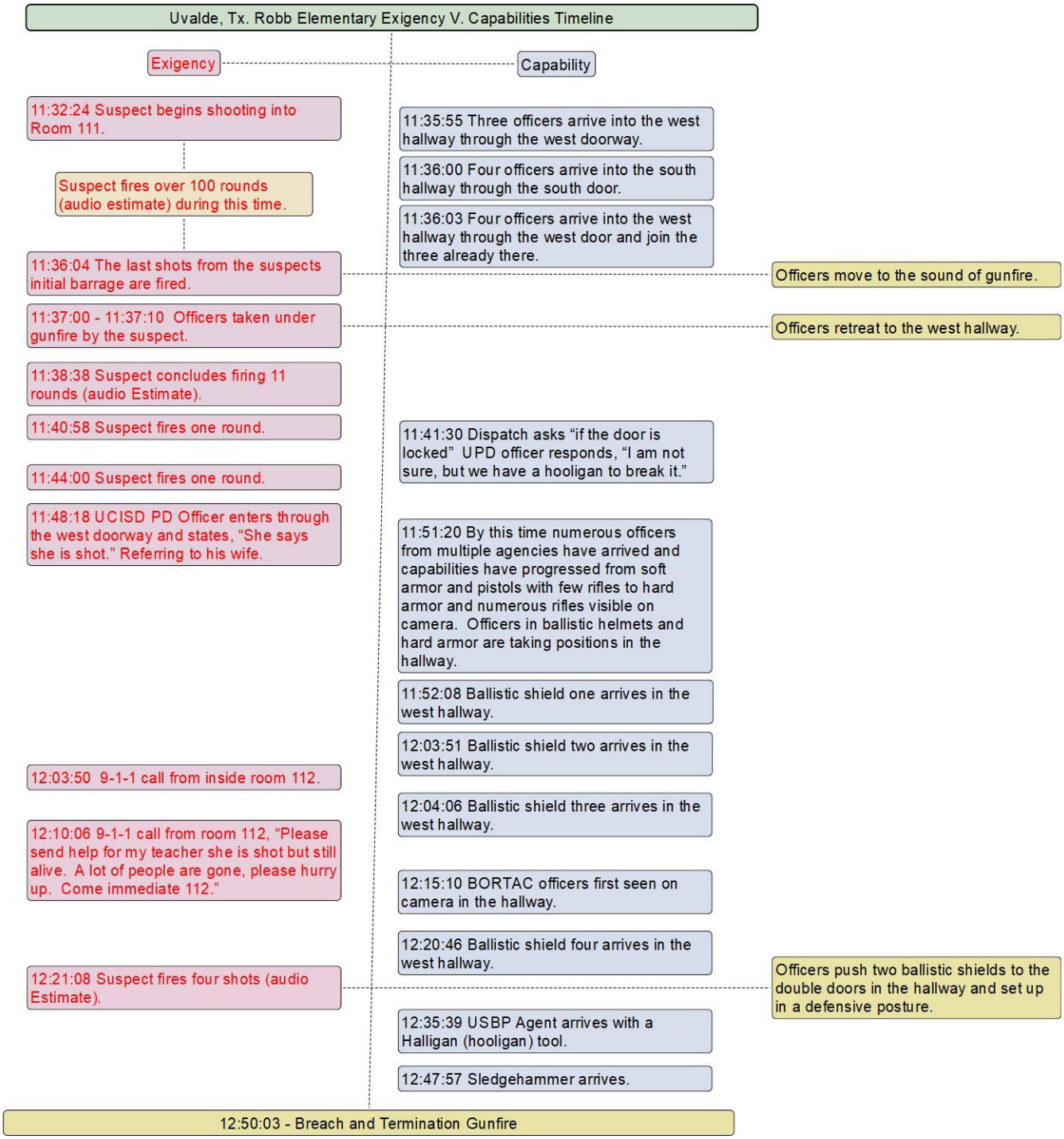


Figure 8. Exigency vs Capability Timeline

Supplemental Materials

Breaching Assessment and Opportunities

The initial wave of officers in this incident worked to locate and identify the location of the suspect. However, in doing so, they were met with a difficult challenge posed by the suspect; they were being fired at while attempting to enter the classroom where the suspect, victims, and casualties were located. Furthermore, the officers did not have any breaching tools. For the purposes of this report, breaching tools refer to common tools that are expected to be carried and utilized during active shooter / active attack events. The responding officers making the initial approach did not have immediate access to ballistic shields. The officer's overall level of training is unknown at this point.

ALERRT staff conducted a series of tests at Robb Elementary School incorporating critical thinking and breaching techniques to determine possibilities that may have changed the incident outcome. ALERRT staff used non-traditional tools that can be purchased at most any hardware store or obtained from a firetruck. The tools used were a 10LB sledgehammer, a Stanley Fat Maxx, and a Halligan tool (see Figure 9).

Figure 9. Breaching Tools

Keyed Entry

After much discussion and observation, it was clear that an unshielded officer faced imminent serious bodily injury or death if they were to attempt to unlock the door. This was proven during the initial responding officers first attempt to open the door. The breach point and inset locations in the south hall received heavy gunfire, and this breach method, alone, was untenable.

Pry

ALERRT staff performed a “pry” on the door using a Stanley Fat Maxx and a sledgehammer. The breaching technique was recorded and performed relatively quickly (the door was opened in 3-4

seconds). Although the breach was conducted quickly, and a positive breach was established, there was still a substantial risk of serious bodily injury or death to officers if this breach were to be performed without a ballistic shield.

Pry with a Distraction

The purpose of implementing a distraction during the breach is to redirect the suspect's focus away from the breach point while the breach is performed. In this case, banging on a wall in the south hallway was used as a distraction. The distraction was initiated, and a positive breach was established relatively quickly (i.e., 3-4 seconds). When the door was opened the ALERRT staff member that was placed in the room as a suspect was focused on the wall where the distraction was performed. The distraction afforded the breachers time to perform the breach while lowering the risk of serious bodily injury or death.

Breaching an outward opening door with a sledgehammer

Typically, outward opening doors are breached using a pry technique. There are techniques that can be used to breach outward opening doors using a sledgehammer or ramming technique. This technique was attempted and proven to not be a viable option due to the construction of the metal door. A positive breach was not established, and performing this technique took a long time. Unshielded, the probability of serious bodily injury or death would be high.

Wall Breaching

Utilizing the walls in an adjoining classroom, a series of wall breaches were conducted. The purpose for a wall breach is to create a distraction prior to conducting a pry breach. Additionally, a wall breach can create a port hole allowing officers to engage the suspect through the opening.

Using a sledgehammer with the strike face toward the wall, a distraction was created by striking the wall multiple times. The strikes resulted in limited penetration to the interior wall in the adjacent classroom.

Using a sledgehammer with the strike face turned sideways, a port was created with 2-3 strikes to the wall. Any remaining insulation materials were removed by hand to clear out the opening.

Using the Stanley Fat Maxx, a distraction was performed by penetrating the sheetrock into the adjacent room with a single puncture through the wall.

It was evident that the suspect in this attack fired numerous rounds from a rifle that penetrated the sheetrock walls. These distractions/ports offer a breaching option but still come with a risk for unshielded officers.

Pry with a window distraction

This breaching method incorporated an exterior window breach as a distraction while simultaneously prying the classroom door. The windows were breached with a Halligan tool while the interior door was breached with a Stanley Fat Maxx and sledgehammer. The window breach added to the tactical advantage by causing the subject in the room to direct attention to the windows while the interior breach team was able to breach, enter, and address the subject.

It was found that "port and cover" on the window was challenging due to miniblinds obstructing view and unequal lighting conditions.

- Port and cover refers to breaching a window and addressing threats from that opening.
- Miniblinds or obstructions would need to be cleared with a breaching tool for a view into the room,
- The classroom was significantly darkened without artificial lighting while the exterior was relatively sunny and bright. When the exterior window was breached, the unequal lighting conditions resulted in the exterior members having diminished capabilities to see into the dark classroom to acquire a target. Raking the blinds out would increase the lighting in the room, and hand-held or weapon mounted lights could further improve lighting conditions.

Additional Breaching Options

Vehicle Breaching. The use of a motor vehicle to breach fortified locations should always be considered as a breaching option in matters of exigent circumstances and loss of life. However, in this incident, vehicle breaching was not a viable option due to the construction and layout of the school. Vehicle breaching was also not feasible because the officers were unsure where innocent children and teachers were located in the room.

Ballistic Breaching. The use of a 12-gauge shotgun and 00 buck is another viable breaching method that could have or may have been used with the proper equipment and training.

References

ALERRT & FBI (2020). *Active Shooter Response – Level 1*. Version 7.2.

Blair, J. P. & Duron, A. (2022). How police officers are shot and killed during active shooter events: Implications for response and training. *The Police Journal*. DOI: 10.1177/0032258X221087827

Blair, J. P., & Martaindale, M. H. (2014). *Evaluating police tactics: An empirical assessment of room entry techniques*. Routledge.

Blair, J. P., & Martaindale, M. H. (2017). Throwing a chair could save officers' lives during room entries. *International Journal of Police Science and Management. 19*(2). DOI: 10.1177/1461355717711452

Blair, J. P., Martaindale, M. H., & Nichols, T. (2014). Active shooter events from 2000 to 2012. *Law Enforcement Bulletin*, Retrieved from http://leb.fbi.gov/2014/january/active-shooter-events-from-2000-to-2012

Blair, J. P., Martaindale, M. H., & Sandel, W. L. (2019). Peek or push: An examination of two types of room clearing tactics for active shooter event response. *Journal of Police Emergency Response. 9*(3). DOI: 10.1177/2158244019871052

Blair, J. P., Nichols, T., Burns, D., & Curnutt, J. R. (2013). *Active shooter events and response*. CRC Press.

Martaindale, M. H. (2015). Police considerations in active shooter events. *Royal Canadian Mounted Police Gazette. (77)*1.

Martaindale, M. H., & Blair, J. P. (Spring, 2017). Active Shooter Events in Schools. *The Journal of School Safety*. Hoover, AL: National Association of School Resource Officers.

Martaindale, M. H., & Blair, J. P. (2019). The evolution of active shooter response training protocols since Columbine: Lessons from the Advanced Law Enforcement Rapid Response Training Center. *Journal of Contemporary Criminal Justice*. *35*(3), 342-356.

Martaindale, M. H., Sandel, W. L., & Blair, J. P. (2017). Active shooter events in the workplace: Findings and policy implications. *Journal of Business Continuity and Emergency Planning*. *11*(1).

Appendix H

2019 and 2021 Legislation Related to School Safety

Act	Code Section	2019 Overview	School Safety Commission Recommendation
190	Ark. Code Ann. § 6-18-2003 Comprehensive School Counseling Program and Plan Framework	School Counseling Improvement Act -Requires each district to develop a comprehensive school counseling plan that focuses on the needs of the individual district; and -Ensures that counselors are afforded the time needed to work with students during student contact days by minimizing the assignment of administrative duties during time when direct and indirect support to students is appropriate. Increased from 75% to 90%.	MHP: #5
245	Ark. Code Ann. § 6-10-133 Bleeding Control Training	Requires that each public school shall provide bleeding control training as a component of a health course to be taught to students in grades nine through twelve (9-12).	AEOPD: #6
629	Ark. Code Ann. § 6-13-1701 et seq.	Established the requirements for having institutional law enforcement officers.	LES: #6
640	Ark. Code Ann. § 6-18-502 Rules for Development of School District Student Discipline Policies	District student discipline policies must: -Address: -Assaults/Threats -Possession of Firearm -Be reviewed annually along with State and District discipline data. -Include: -Prevention, intervention, and conflict resolution provisions -Programs, measures, or alternative means and methods to continue student engagement and access to education when suspended or expelled. Requires teachers, administrators, classified employees, and volunteers to be provided "appropriate student discipline, behavioral intervention, and classroom management training and support.	MHP: #3

1029	Ark. Code Ann. § 6-17-711 Bullying Prevention - PD	Requires DESE to require two (2) hours of PD for licensed personnel: -Bullying prevention; and -Recognition of the relationship between bullying and suicide Requires DESE to develop guidance to assist in resolving complaints concerning student bullying behaviors – which will be provided to licensed personnel during PD. Clarifies that "cyberbullying" is bullying. Requires that the superintendent, one (1) time each school year, report discipline data to the school board of the district at a public hearing.	MHP: #2
1029	Ark. Code Ann. § 6-18-514 Antibullying Policies	Requires: -Responding to reports of bullying "as soon as reasonably practicable" by: -Notifying parents of victim, and -Preparing a written report of alleged incident; -Promptly investigating a credible report and completing within five (5) school days; -Notifying parents of perpetrator; -A written record of investigation and result; -Discussion of available counseling and intervention services with involved students. Additional requirements for district policies, including annual reevaluation, reassessment, and review of policies.	MHP: #2

Act	Code Section	2021 Overview	School Safety Commission Recommendation
182	Ark. Code Ann. § 6-13-629 Training and Instruction for School Boards	Changed the requirement created by Act 1029 of 2019 that school boards receive training "regarding school safety and student discipline" from one time to annually.	MHP: #2
551 & 622	Ark. Code Ann. § 6-10-128 School Resource Officers	Requires that "sworn, nonsupervisory law enforcement personnel" on campus during the day or employed by the school obtain certification in Youth Mental Health First Aid within 18 months. -YMHFA certification must be renewed every 4 years Requires that school boards that accept an SRO enter into an MOU with the local law enforcement agency, or adopt policies and procedures if the school district has an institutional law enforcement officer (§ 6-13-1701), that governs the SRO and includes without limitation: - The financial responsibility of each party - The chain of command - The process for the selection of SROs - The process for the evaluation of SROs - The training requirements for SROs; and - The roles and responsibilities of SROs, which shall include without limitation: - clarification of SROs role in student discipline - the use of physical restraints or chemical sprays; - the use of firearms; and - making arrests on the public school campus	MHP: #3 LES: #3 & 4 IC: #4
620 & 648	Ark. Code Ann. § 6-15-1303 Safe Schools	Requires a school district to conduct a comprehensive school safety audit every 3 years (initial due no later than Aug. 1,	MHP: #1 & 2 AEOPD: #5

	Initiative Act	2024) to assess the safety, security, accessibility, and emergency preparedness of district buildings and grounds in collaboration with local law enforcement, fire, and emergency management officials, including: - Safety and security of site and exterior of buildings; - Access control; - Safety and security of interior of buildings; - Monitoring and surveillance; - Communication and information security; - Emergency operation plans; and - School climate and culture.	

Other Relevant Laws and Rules:

Act	**Code Section**	**Overview**	**School Safety Commission Recommendation**
541 of 2017	Ark. Code Ann. § 6-15-1304	Records or other information related to a public school district that operates a Pre-K or services any K-12 students, are confidential and exempt from FOIA in the following instances: - records or other information that could reasonably be expected to be detrimental to public safety, including without limitation emergency or security plans, school safety plans, procedures, risk assessments, studies, measures, or systems; and - records or other information relating to the number of licensed security officers, school resource officers, or other security personnel, as well as any personal information about those individuals.	LES: #1-5 AEOPD:#1, 2, 5 IC: #1

Act 1084 of 2021. An act concerning the use of student restraints in public schools or educational settings.

Ark. Code Ann. § 6-15-1005. Safe, equitable, and accountable public schools.
General overall safety requirements.

Ark. Code Ann. § 6-17-113. Duty to report and investigate student criminal acts – Definitions.
Reporting requirements when a reasonable belief exists that any person has committed or threatened to commit an act of violence or any crime involving a deadly weapon on school property or while under school supervision.

Standards for Accreditation of Arkansas Public Schools and School Districts:

Standard 2-E.2: Each public school and public school district shall maintain appropriate materials and expertise to reasonably ensure the safety of students, employees, and visitors. (D/C)

Standard 6-A.2: Each public school district shall adopt and implement school safety policies and procedures in accordance with the laws of the State of Arkansas and the rules of the Division. (D/P)

A.C.A. § 6-15-1005

Current through all acts of the 2021 Regular Session, First Extraordinary Session, Extended Session, Second Extraordinary Session, and the 2022 Fiscal Session including corrections and edits by the Arkansas Code Revision Commission.

AR - Arkansas Code Annotated > Title 6 Education > Subtitle 2. Elementary and Secondary Education Generally > Chapter 15 Educational Standards and Quality Generally > Subchapter 10 — Arkansas Public Education Act of 1997

6-15-1005. Safe, equitable, and accountable public schools.

(a)

(1) Arkansas schools will have safe and functional facilities.

(2) All school buildings will meet existing state and federal requirements.

(3) Instructional facilities will be designed and structured to support learning.

(b)

(1) The school climate will promote student achievement.

(2)

(A) Every school and school district will enforce school district policies to ensure the safety of every student during school hours at school-sponsored activities.

(B) These policies will include, at a minimum, policies on weapons, violence, tobacco, alcohol, other drugs, gangs, and sexual harassment.

(3) Every school and school district will enforce a code of behavior for students that respects the rights of others and maintains a safe and orderly environment.

(4) Every school and school district will have in place a policy on addressing disruptive students.

(5)

(A) Every school and school district will offer appropriate alternative education programs organized to serve those students whose educational progress deviates from the standard expected for a successful transition to a productive life and those students whose behavior interferes with their own learning or the educational process of others.

(B) School districts may serve the needs of these students through regional or cooperative efforts with other school districts.

(c) Local schools will work with parents, families, and business and community members to incorporate responsibility, character, self-discipline, civic responsibility, and positive work habits into adult contacts with students and to promote student demonstration of these behaviors.

(d) Every school will offer opportunities for students to be able to study and participate in the visual and performing arts, health and physical education, and languages.

(e) All public schools will participate in the state school improvement process:

(1)

(A) Every school will engage in the collection and analysis of perceptual, archival, and achievement data in order to establish school and school district goals to improve student academic achievement.

(B) Students shall not be surveyed on values and beliefs;

(2) Every school will develop and implement a data-driven school-level improvement plan based on these analyses that leads to increased student achievement and continuous school improvement; and

(3) Every school will monitor and adjust the plan of action as necessary to promote increased student achievement and continuous school improvement.

(f)

(1) All public schools will have a plan of parental involvement.

(2)

(A) Every school will have a plan for allowing parents to be involved in the education of their children.

(B) These plans will address communication with parents, volunteering, learning activities that support classroom instruction, participation in school decisions, and collaboration with the community.

(3) Every school will involve parents in developing school goals and priorities and evaluating the effectiveness of the school-level improvement plan.

(g)

(1) All public schools will be accountable to the public they serve.

(2) All schools will participate in the Arkansas Educational Support and Accountability Act, *§ 6-15-2901* et seq.

(3) All schools will report to the parents the results of all assessments conducted to measure the achievement progress of their children.

(4)

(A) The highest performing schools will be recognized and rewarded.

(B) Schools reaching predetermined high levels of achievement will be granted charter status with approval of the charter petition by the Division of Elementary and Secondary Education.

(5) Each school will issue a school achievement report to the community on all statewide student assessments.

(h)

(1) All public schools will be led by qualified administrators.

(2) All administrators will demonstrate content knowledge in leadership, finance, organization, school climate, curriculum, and evaluation.

(3) In order for administrators to be able to renew a license, they must have participated in a continuing education and professional development program based on their school-level improvement plans, performance evaluation results, and student achievement scores.

History

Acts 1991, No. 236, § 1; *1995, No. 1296, § 17*; *1997, No. 1108, § 5*; *2017, No. 936, §§ 15*-19; *2019, No. 757, § 12*; *2019, No. 910, § 1214*.

Annotations

Notes

Amendments.

The 2017 amendment substituted “school-level” for “school” in (e)(2), (f)(3), and (h)(3); substituted “Arkansas Educational Support and Accountability Act, *§ 6-15-2901* et seq.” for “Arkansas Comprehensive Testing, Assessment, and Accountability Program” in (g)(2); and substituted “statewide student” for “state-required” in (g)(5).

The 2019 amendment by No. 757 substituted “plan” for “program” in (f)(1).

The 2019 amendment by No. 910 substituted “Division of Elementary and Secondary Education” for “Department of Education” in (g)(4)(B).

Case Notes

Private Right of Action.

Arkansas Public Education Act, *§§ 6-15-1001* — *6-15-1007*, does not expressly provide for a private right of action or for any kind of remedy; therefore, a school district and a bus driver could not have been sued over a student's rape based on alleged failures under *§ 6-15-1002* or this section. *Young v. Blytheville Sch. Dist., 2013 Ark. App. 50, 425 S.W.3d 865 (2013)* .

A.C.A. § 6-17-113

Current through all acts of the 2021 Regular Session, First Extraordinary Session, Extended Session, Second Extraordinary Session, and the 2022 Fiscal Session including corrections and edits by the Arkansas Code Revision Commission.

AR - Arkansas Code Annotated > Title 6 Education > Subtitle 2. Elementary and Secondary Education Generally > Chapter 17 Personnel > Subchapter 1 — General Provisions

6-17-113. Duty to report and investigate student criminal acts — Definitions.

(a) As used in this section:

(1) "Act of violence" means any violation of Arkansas law where a person purposely or knowingly causes or threatens to cause death or serious physical injury to another person;

(2) "Deadly weapon" means:

(A) A firearm or anything manifestly designed, made, or adapted for the purpose of inflicting death or serious physical injury; or

(B) Anything that in the manner of its use or intended use is capable of causing death or serious physical injury; and

(3) "Firearm" means any device designed, made, or adapted to expel a projectile by the action of an explosive or any device readily convertible to that use, including such a device that is not loaded or lacks a clip or other component to render it immediately operable, and components that can readily be assembled into such a device.

(b)

(1) Whenever the principal or other person in charge of a public school has personal knowledge or has received information leading to a reasonable belief that any person has committed or has threatened to commit an act of violence or any crime involving a deadly weapon on school property or while under school supervision, the principal or the person in charge shall immediately report the incident or threat to the superintendent of the school district and the appropriate local law enforcement agency.

(2) The report shall be by telephone or in person immediately after the incident or threat and shall be followed by a written report within three (3) business days.

(3) The principal shall notify any school employee or other person who initially reported the incident that a report has been made to the appropriate law enforcement agency.

(4) The superintendent or his or her designee shall notify the local school district board of directors of any report made to law enforcement under this section.

(c)

(1) Whenever a law enforcement officer receives a report of an incident pursuant to subsection (b) of this section, that officer shall immediately report the incident to the office of the prosecuting attorney and shall immediately initiate an investigation of the incident.

(2) The investigation shall be conducted with all reasonable haste and, upon completion, shall be referred to the prosecuting attorney.

(3)

(A) The prosecuting attorney shall implement the appropriate course of action and, within thirty (30) calendar days after receipt of the file, the prosecuting attorney shall provide a written report to the principal.

(B) The report shall state:

(i) Whether the investigation into the reported incident is ongoing;

(ii) Whether any charges have been filed in either circuit court or the juvenile division of circuit court as a result of the reported incident; and

(iii) The disposition of the case.

(4) Upon receipt of the report from the prosecuting attorney, the principal shall notify any school employee or any other person who initially reported the incident that a report has been received from the prosecuting attorney.

(d) Excluding the reporting requirement set out in subdivision (c)(3) of this section, any person who purposely fails to report as required by this section shall be guilty of a Class C misdemeanor.

(e) The State Board of Education shall promulgate rules to ensure uniform compliance with the requirements of this section and shall consult with the office of the Attorney General concerning the development of these rules.

History

Acts 1995, No. 888, § 1; *1997, No. 1243, § 1*; *1999, No. 1520, § 1*; *2019, No. 315, § 223*.

Annotations

Notes

Amendments.

The 2019 amendment deleted “and regulations” following “rules” twice in (e).