



# Anonymized Threat Response Guidance

A Toolkit for K-12 Schools

September 2024

# Acknowledgments

The team at the Cybersecurity and Infrastructure Security Agency (CISA) would like to acknowledge the many partners and organizations across the kindergarten through grade 12 (K-12) school community for supporting the development of this product by participating in interviews and offering insights into their approaches toward anonymized threat response. In particular, CISA would like to acknowledge the support of the Federal Bureau of Investigation (FBI) for their extensive and valuable participation in feedback sessions during the development of this product. We also would like to thank our partners from the Homeland Security Operational Analysis Center (HSOAC) for conducting the research and development efforts for this toolkit. The contributions and insights were invaluable toward the development of this product that we hope supports communities in continuing to provide safe and supportive learning environments for our Nation's schools and districts. This publication is in the public domain. Authorization to copy and distribute this publication in whole or in part is granted. However, the CISA logo and FBI logo may not be otherwise reproduced or used in any other manner without advance written permission from the agencies. While permission to reprint this publication is not necessary, when quoting, paraphrasing or otherwise referring to this report, the citation should be: Cybersecurity and Infrastructure Security Agency (CISA). Anonymized Threat Response Guidance: A Toolkit for K-12 Schools. 2024. Department of Homeland Security.

*This Guidance is not intended to, and does not, create any legal rights. The U.S. Department of Homeland Security (DHS) and the U.S. Department of Justice (DOJ) do not endorse any individual, enterprise, product, or service. DHS and DOJ do not mandate or prescribe practices, models, or other activities described in this communication. DHS and DOJ do not control or guarantee the accuracy, relevance, timeliness, or completeness of any information outside these respective Departments, and the opinions expressed in any of these materials do not necessarily reflect the positions or policies of DHS and DOJ.*

*Editor's Note: A quality control review discovered that an earlier version of this document contained an erroneous statistic from DOJ regarding the number of threats made to schools. This updated version has removed this statistic.*

# Executive Summary

Anonymous threats, including those posted to social media, are taxing school and law enforcement resources, contributing to losses in instruction time and traumatizing school communities. The *CISA Anonymized Threat Response Guidance: A Toolkit for K-12 Schools* is designed to help local education agencies and their law enforcement and community partners create tailored approaches to addressing anonymous threats from assessment to response. This guide is intended to assist the range of kindergarten through grade 12 (K-12) schools across the United States and is applicable to schools across diverse geographical settings, student populations, and levels of maturity in emergency operations planning.

## // Key Strategies to Address Anonymized Threats

### **Build awareness about reporting to detect threats early and deter future threats.**

Bystander reporting is a critical violence prevention tool for K-12 schools (see e.g. CISA and NTAC, 2023; Moore et al., 2023; NTAC, 2021). Like threats or comments made by known individuals (sometimes termed “leakage” in threat assessment protocols), efforts to detect anonymized threats against schools before they can spread should focus heavily on building awareness about reporting. Encourage community members to “Report, Don’t Repost” threats they see online, since stopping the further dissemination of a threat both aids investigation and limits the potential impact of threats that, while alarming, are not intended to be followed through. Efforts to educate parents and others across the school community about youth social media use are also critical to spreading the word about what constitutes a threat and the damage threats can do to a school community. Be clear about what the consequences are for making threats, even if they are meant to be jokes. Finally, threats made by students are often indicators of underlying problems and akin to cries for help. Early intervention by mental health and other professionals is often better than intervention after the fact.

### **Develop a partnership structure that will help address anonymized threats.**

Schools work with several different partners both inside and outside the immediate school community to address anonymized and other threats. In addition to school administrators, intelligence organizations, such as fusion centers or the Federal Bureau of Investigation, and school-based or school-knowledgeable law enforcement personnel, such as school resource officers (SROs), will play a key role in assessing threats and deciding on appropriate response actions. Mental health and other threat assessment professionals will provide key resources to schools addressing threat situations, including in the aftermath of threats, to ensure that the mental health, emotional and other needs of the community are met.

### **Consider the inclusion of a multidisciplinary threat assessment team when addressing anonymous threats, and utilize their expertise if the subject who made the threat becomes known.**

Multidisciplinary threat assessment teams can help identify the level of concern posed by an individual who made a threat or exhibited concerning behavior and can decide on the appropriate supports and interventions for individuals identified as “at risk of doing harm.” At a minimum, these teams should include a school administrator, a school-based law enforcement representative, and a school counselor and/or other mental health professional with the option of adding individuals who can further help assess the situation and contribute to developing the right intervention plan. While the utility of a multidisciplinary threat assessment team may be limited prior to knowing the identity of the threat’s source, awareness of an anonymous threat could identify a link to previous incidents, thereby aiding the response, and expediting the team’s response if an individual is eventually identified.

## **Response coordinators should balance initial steps to ensure the campus is safe.**

Schools that are targets of anonymized threats must treat each one as initially credible. If a school is the target of a threat, determining which assets need to be on-scene to keep the campus and school community safe is a critical first step. Because certain response actions, such as full lockdowns or an increased police presence, can be traumatizing for some students, schools should consider the intensity and overtness of their response. Determine how to balance the initial response and leave open the potential to scale up rapidly as necessary. Be prepared to announce to the community whether the decision is made to lock down, secure campus or close school. Ensure that school personnel coordinate with local law enforcement to deliver uniform messages about a threat situation and provide accurate, up-to-date information to the broader school community.

## **Triage and determine the level of concern a threat poses.**

The first step in triaging anonymous threats is to engage a law enforcement partner whose expertise is critical to managing threat situations and deciding when it is okay or necessary to scale response actions up or down. First, consider key background and contextual information about a threat. Then, move on to identify any discernable patterns that might elevate or decrease the level of concern posed by the threat. Finally, identify any signs of the threat's imminence that might call for a rapid response reaction to keep the community safe.

## **Putting it all together: Enhance school preparedness to address future threats.**

Every school and school district can take steps throughout the school year to better prepare for threat situations. Successful response during an emergency begins with ongoing preparedness and prevention efforts outside of emergencies. Establish a response protocol that addresses threat situations, and conduct developmentally and age-appropriate drills and training exercises to help prepare for responding to threats. Establish protocols for communicating with families, and make sure the resources are in place to address the impacts of a threat.

# Table of Contents

Acknowledgments	ii
Executive Summary	iii
Introduction and Overview	1
Toolkit Goals and Intended Audience	2
Methods Used to Develop This Toolkit	2
Navigating and Using This Toolkit	3
<b>SECTION ONE   Getting Started: Trends in Threats Against K-12 Schools</b>	<b>4</b>
1.1 Social Media, Youth and Threats Against Schools	5
1.2 What Impact Are Anonymized Threats Having on K-12 Schools?	7
<b>SECTION TWO   Containing the Problem: Early Awareness and Detering Future Threats</b>	<b>8</b>
2.1 Build Awareness About Reporting Threats	8
2.2 Prepare Staff Who Might Receive Anonymous Threats By Phone to Capture Key Information	8
2.3 Educate the Community About Youth Social Media Use, Especially Families	9
2.4 Provide Mental Health Resources to Help Mitigate Threats	9
2.5 Take Actions to Deter Future Threats	10
<b>SECTION THREE   Key Partners in Addressing Anonymized Threats to K-12 Schools</b>	<b>12</b>
3.1 Reporting Party	12
3.2 School Administrators	13
3.3 School-Knowledgeable Law Enforcement	13
3.4 School-Knowledgeable Mental Health and Threat Assessment Professionals	14
<b>SECTION FOUR   First Response: Immediate Actions When a Threat is Received</b>	<b>15</b>
4.1 Initial Response to Threats to Ensure Campus Safety	15
4.2 Initiating Threat Evaluation to Inform Response	16
4.3 Crisis Communication with the School Community	21
<b>SECTION FIVE   Deliberate Response: Balancing Response Actions for Complex and Uncertain Threats</b>	<b>23</b>
5.1 Options Available to Schools to Heighten Response to Anonymized Threats	23
5.2 Ongoing Threat Evaluation to Inform Response Changes	28
5.3 Communication as the Threat is Resolved and Beyond	29
<b>SECTION SIX   Preparedness to Enhance Schools' Capabilities to Manage Anonymized Threats</b>	<b>30</b>
6.1 Establish a Threat Response Protocol for Addressing Anonymized Threats	31
6.2 Engage in Training and Drills Covering Different Options for Threat Response	32
6.3 Inform Families of Basic Threat Response Plans and Prepare to Communicate with the School Community When Threats Occur	33
6.4 Prepare to Provide Support Resources to Address the Impacts of Threats	33
6.5 Conclusion	34
<b>Additional Resources</b>	<b>vii</b>
<b>Worksheets</b>	<b>ix</b>
Worksheet 1. Taking Stock of Anonymized Threats at Your School	ix
Worksheet 2. Gathering Information When You Receive a Threat: Where to Start?	xi
<b>Abbreviations</b>	<b>xiv</b>
<b>References</b>	<b>xv</b>

# Figures

Figure 1.1 Timing of Press Reports About Social Media Threats Against Schools, 2012-2022	4
Figure 3.1 Potential Partners for Addressing Anonymized Threats Against Schools	12
Figure 4.1 Action Streams in the Initial Response to an Anonymized Threat	15
Figure 4.2 Weighing the Level of Concern Posed by an Anonymized Threat	19
Figure 5.1 The Evolution of Action Streams Throughout Response to Anonymized Threats	23
Figure 5.2 Law Enforcement or Security Personnel Response Options for Threatened Schools	25
Figure 5.3 Campus Movement Restriction and Closure Options for Threatened Schools	26
Figure 5.4 Options for Preventing Weapons on Campus in Threatened Schools	27

# Introduction and Overview

School violence shapes the educational experience of many students and school staff across the United States. In a fall 2022 survey of over 950 kindergarten through grade 12 (K-12) teachers across the United States, about one third (35%) reported that their school had been disrupted by threats posted to social media during the 2021-2022 school year (Jackson et al., 2023).

## What is an Anonymized Threat?



Anonymous threats can be delivered via a multitude of different ways, whether by phone, using technology that masks phone numbers and distorts a caller's voice, over anonymous platforms like email or social media, or written on the wall of a school building. Across these various modes of delivery, the identity of the individual making the threat is not immediately discernable.



Anonymized threats are different from threats made by known individuals, which may be made publicly (e.g. a threat made in writing at school or online connected to the threatener's identity) or may be termed "leakage" in threat assessment protocols (when the threat to engage in violence against a target becomes known through communication to a third party).



Anonymous reports of threats by other individuals (i.e. a student calling an anonymous tip line or other reporting mechanism to report a threat they heard from a peer or saw posted by a peer online) are also not anonymous threats because the identity of the individual who made the threat is known.

Social media-based and other types of anonymized threats of violence against K-12 institutions are common. The age of the internet and of social media grant a perception of anonymity that can make individuals more comfortable saying or doing things online that they would not do in person. With this newfound comfort has come a rise in anonymous threats to schools and other public spaces (Ward, 2023).

These threats vary in their delivery and intent. Many threaten attacks against students, but some target additional members of the school community, such as teachers and other school staff. A threat might mention a bomb at a specific school or that a student is bringing a gun to school the next day to target a specific person or group of persons. Other threats might be more general, such as an image of someone with a firearm urging people not to come to school the next day. Some anonymous threats posted to social media and elsewhere can be so vague as to just mention the initials of a supposedly targeted school or no specific location at all (Ward, 2023). Indeed, a common characteristic among threats targeting K-12 schools is their anonymous nature—schools are often unable to immediately discern who posted the threat.

Most of the anonymous threats schools receive are intended to be jokes—hoax threats by students trying to get out of school for a day or trying to sow disorder. Others can be cries for help. Their timing also varies. Sometimes, threats come at random times during the school year or follow disturbing patterns in the wake of actual tragedies. Highly publicized mass shootings, for example, often prompt an

onslaught of so-called copycat threats of more violence (Santucci, 2022). Threats can also come in response to trends spreading across various social media platforms, such as the "National Shoot Up Your School" or "School Shooting" TikTok challenge that tasked students to prank call their schools and local police claiming that there would be a mass shooting on a specific date. This particular challenge plagued school districts across the United States in December 2021 (Mak, 2021; Klein, 2022).

When a school is the target of a threat, district and school-level administrators, school-based law enforcement personnel, other school staff, and local law enforcement partners have no choice but to immediately devote extensive resources to tracking down its origins, determining the level of concern that it poses and implementing response actions to keep their communities safe. Often, these school-led responses—evacuations, lockouts, lockdowns or school cancellations among others—have a significant emotional impact on students, teachers and other members of the school community, making it difficult for schools to foster a positive educational experience and maintain an accepting and trusting environment.

Given the complexity of the problem, there is no one-size-fits-all approach to addressing anonymized threats against schools. Through the development of this toolkit, the Cybersecurity and Infrastructure Security Agency (CISA) hopes to alleviate some of the challenges that local education agencies face in this area.

## // Toolkit Goals and Intended Audience

The purpose of this toolkit is to provide guidance to local education agencies that have been targeted by anonymous threats, including those originating on social media, and other similar threats, such as swatting ([see Box 1.1](#)). This toolkit outlines steps that school leaders can take to respond to threats in a balanced way that will not induce further stress on or unfairly impact their communities, assess the level of concern posed by a threat, and better prepare themselves for and prevent future threats. It also highlights key partners that local education agencies can work with to address such threats and how schools can best work with these partners. The information in this toolkit is meant to speak to diverse K-12 school settings and populations and is based on current practices highlighted by local education agencies, law enforcement agencies and other partners situated across the country.

This toolkit is intended for K-12 schools and districts serving all grade levels across different geographical contexts, whether or not they have been the target of anonymous threats in the past. Local law enforcement agencies working with K-12 schools to address threats may also find the content in this toolkit useful.

## // Methods Used to Develop This Toolkit

The guidance included in this toolkit draws on findings presented in [Developing Practical Responses to Social Media Threats Against K-12 Schools: An Overview of Trends, Challenges, and Current Approaches](#) (Moore et al., 2024). This study is based on four key research activities: a literature review of over 115 sources focused on assessing written threatening communications in the educational and other contexts, including anonymous social media-based and swatting threats; an analysis of over 1,000 news reports about social media threat incidents against K-12 schools between 2012-2022; over 40 interviews with more than 60 individuals involved in school safety at the federal, state, county, local community, school district and individual school levels; and a panel discussion with eight experts from the K-12, law enforcement and threat assessment communities.

- The literature review identified indicators that have been used to assess the credibility and level of concern posed by written threats in the K-12 educational context. It also includes contexts that hold appropriately relevant and translatable lessons for schools, such as anonymous threats made to public officials, threats from fixated individuals (stalkers), bomb threats, and, to a lesser extent, cyberbullying.
- The analysis of news reports helped identify discernable trends around social media threats against K-12 schools such as information about their timing, geographical scope, type of schools targeted, and how schools and districts have been responding to these threats.
- The direct interviews, which represented 17 school districts across 12 states as well as school safety offices, tip lines and state law enforcement agencies from 15 different states, collected information on current practices that local education agencies and their law enforcement partners are using to address anonymized threats as well as the challenges they face in this area.
  - To highlight the contributions of this diverse group of stakeholders and emphasize key points, this toolkit includes selected “Voices from the Field” throughout each section.
  - There are several “Example Threat Scenarios” provided throughout the document that recount real-world situations involving K-12 schools and districts. These entries have been collected during the research process and include quotes that have been edited or paraphrased to avoid any identifiable information about the institutions subject to these threats.
- Finally, the research team held an expert panel in July 2023 to collect feedback on the draft report and gather recommendations for the development of this toolkit. Experts consisted of K-12 administrators, federal law enforcement personnel, and threat assessment professionals from academia and law enforcement.

# // Navigating and Using This Toolkit

This toolkit acknowledges the myriad diverse contexts that characterize K-12 schools across the United States and the ensuing need for flexible solutions that can help them meet the needs of their unique populations as they address anonymized threats. Its purpose is to provide simple, actionable guidance around assessing and responding to such threats and enhancing preparedness in this area.

## **SECTION ONE**

Provides background about trends in social media-based and other types of anonymous threats targeting K-12 schools, including how schools are becoming aware of threats. This section also describes the impact that these threats are having on local education agencies across the country such as loss of instruction time, the high demand they place on school and law enforcement resources, and the trauma and emotional stress that they induce.

## **SECTION TWO**

Outlines initiatives that schools can consider putting in place to help prevent and deter threat-making. The discussion focuses on strategies to increase awareness and reporting of threats, adding mental health resources to schools and efforts to educate the community about the potential consequences of threat-making even when threats are meant to be jokes.

## **SECTION THREE**

Describes key partners in the process of addressing anonymous threats made against K-12 schools. Schools should think about what additional capabilities and expertise they will need to effectively respond to threats and to help them investigate the origins of a threat and the risk that it poses.

## **SECTION FOUR**

Discusses the first set of response actions that schools can take to ensure safety immediately upon receiving notification of a threat. This section also provides in-depth guidance about the parallel process of threat evaluation that will guide decisions about whether to escalate or downgrade response actions and recommendations about communicating with families and the broader community during threat emergencies.

## **SECTION FIVE**

Builds on the previous section to describe the broad menu of response actions available to schools and their partners when it comes to heightening response actions based on information gathered about a threat during the assessment process.

## **SECTION SIX**

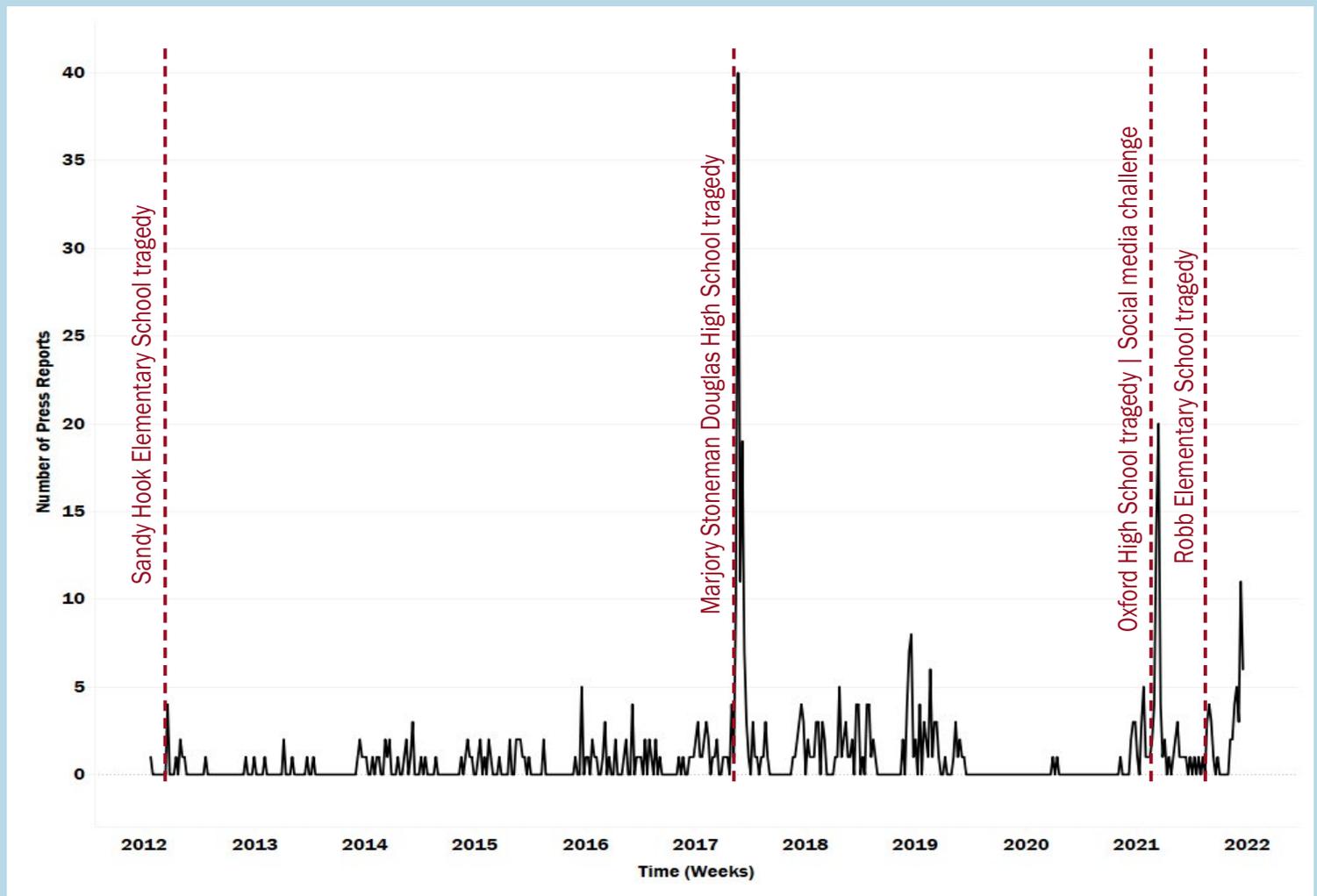
Summarizes key takeaways for local education agencies and considerations for future steps to enhance preparedness. The end of this toolkit also provides diverse resources for K-12 stakeholders to access as they enhance their preparedness to address anonymized threats, as well as worksheets to spur more in-depth and context-specific thinking about the topic.

# Getting Started: Trends in Threats Against K-12 Schools

Anonymous threats are a growing concern for schools and pose significant challenges when it comes to deciding on appropriate responses. This section covers recent trends in such threats and discusses the impacts they have had on K-12 schools across the country.

Anonymized threats—such as bomb threats, threats originating on social media, and instances of swatting ([see Box 1.1](#))—are a growing problem for K-12 schools across the country (Ward, 2023). They are most common in the aftermath of high-profile mass shootings at schools or during trending social media challenges, but threats have also come at random times during the school year (Moore et al., 2024; Natanson and Meckler, 2021). Social media threats often come in clusters, meaning that several schools across a district, state or even nationally are targeted by the same or similar threats at the same time. School testing season (e.g. in the late fall/early winter and again in the spring) is also associated with an increase in such threats. Most of the schools that receive threats are high schools located in suburban locales followed by high schools in large urban areas (Moore et al., 2024).<sup>1</sup>

Figure 1.1 **Timing of Press Reports About Social Media Threats Against Schools, 2012-2022**



SOURCE: Moore et al., 2024.

<sup>1</sup> This trend may be due to the propensity of news outlets to cover incidents impacting schools and districts in high-population areas as opposed to smaller, more remote and sparsely populated locations.

## Box 1.1 What is “Swatting?”

Swatting calls are prank calls made to emergency dispatch centers or nonemergency police phone numbers about a false, ongoing, active assailant attack. They are meant to prompt a significant law enforcement response to the targeted area. According to news reports, hundreds of swatting calls occur annually, with some hoaxers using computer-generated calls to harass schools and other targets (Yousef, 2022; Jojola and Staeger, 2023). In November 2022, the Federal Bureau of Investigation (FBI) issued a statement saying that many of the calls appeared to be originating from overseas (Balsamo, 2022). Swatting threats to K-12 schools are comparable to social media-based threats due to their anonymity and the significant challenges that they introduce when it comes to assessing their viability and deciding on an appropriate response. Incidents of swatting that occurred during the 2022-2023 school year also suggest that they tend to come in clusters, impacting several schools across one state or the entire country at the same time (see e.g. Case, 2023).

### Reporting an Incident

If K-12 community members believe they have been victim of an anonymous threat or swatting incident, they should first report this potential crime to local law enforcement. To report threats directly to the FBI, see the [Internet Crime Complaint Center](#), contact [your local FBI field office](#) or report online at [tips.fbi.gov](#). Further, as part of their efforts to combat swatting in 2023 the FBI launched the National Common Operating Picture Virtual Command Center (NCOP-VCC) information-sharing application as a resource for partner organizations to collaborate on swatting incidents across all levels of government. For more information about this FBI initiative, contact the [FBI Law Enforcement Enterprise Portal](#) help desk at 888-334-4536.

## // 1.1 Social Media, Youth and Threats Against Schools

Social media use is ubiquitous among today’s youth, with over 95% of youth between the ages of 13 and 17 using at least one platform and a third reporting that they use social media “almost constantly” (U.S. Surgeon General’s Office, 2023). Technology has revolutionized the American school system, making education more accessible than ever before. Despite positive advances, social media is playing a growing role in fueling school threats. This shift parallels other related trends, such as the shift of gang violence, self-harm, bullying and other harmful behavior to online spaces (Patton et al., 2014; Reynolds et al., 2017).

The popularity of social media platforms is constantly shifting. When one falls out of fashion among youth, another quickly rises to take its place. Many widely known and used platforms advertise features that help connect individuals with broader audiences whose identities are largely unknown to the individual user (Reynolds et al., 2017). Other, lesser-known platforms have also helped fuel threats. Many grant users a heightened level of anonymity (Trump, 2016). This anonymity as well as the accessibility and ease of use that characterizes social media has reduced barriers to threatening communications and introduced myriad challenges for local education agencies across the country (Monagas and Monagas, 2015).

## VOICES FROM THE FIELD

“Social media is the new bathroom wall [in schools].”

- School district-level representative, March 2023

While many social media-based and other threats against schools initially appear anonymous, trends suggest that most are made by students at the targeted school as opposed to outsiders. That said, social media and the internet has made it especially easy for individuals unrelated to a school or district to make specific threats. Students' personal information, including their names and the name and location of the school that they attend, is often readily available on social media profiles that are not set to private.

These factors combined make specific threats from outsiders commonplace. Regardless of their origin, individuals who make threats against their own or another school are often identified. Reports about social media threat incidents between 2012-2022 suggest that law enforcement agencies were able to identify the individual making the threat in more than 65% of cases (Moore et al., 2024). In many of these instances, individuals are arrested and charged with a crime.

## Box 1.2 Pros and Cons of Early Detection Software

K-12 schools become aware of threats through a variety of mediums. Schools might find out about a threat through direct communication with a student, staff, or family member or through an established tip line. In some cases, they also receive alerts about potential threats from third-party monitoring programs and software that scans student activity on school-issued devices or devices connected to school Wi-Fi networks. Other tools are becoming increasingly available that scan public social media data more broadly for mentions of threats, locations or specific schools.

### Pros

These programs identify potential threats in student writing preemptively by scanning documents, internet searches, social media, and other activity occurring on school district-owned devices or Wi-Fi networks. Their goal is to flag key words or phrases that have been previously identified as potentially threatening within a specific school community. Because they use artificial intelligence to detect potentially threatening language, they are intended to alleviate burdens placed on school staff who might otherwise be responsible for reviewing material on school-issued devices or passing through school Wi-Fi networks on their own. Such scanning may detect threats or concerning situations that would otherwise not be detected.

### Cons

Despite their potential utility when it comes to detecting threats early, these technologies have raised concerns across the K-12 school community. Alone, they are often insufficient to identify threats, and many stakeholders emphasize that the human element is still critical to determining the urgency of a threat. Monitoring software is often expensive and requires significant staff oversight to function effectively. The staff time required to review alerts produced by such systems, a significant percentage of which will be false alarms, can be a burden to smaller schools already facing staffing constraints. If staff are not available to review alerts rapidly, the potential detection advantage such technologies are intended to provide will be lost. Perhaps most importantly, use of third-party tools may introduce concerns around bias and student privacy and civil rights. The notion of "constant surveillance" can also blur the line around when local education agencies should be held responsible for not having prevented an incident.

## // 1.2 What Impact Are Anonymized Threats Having on K-12 Schools?

Anonymous threats, on social media and more generally, are a significant burden to schools. They erode trust that schools are safe places, contribute to losses in instruction time, overwhelm school and local partner resources, and traumatize entire communities. In most cases, the explicit goal of anonymous or hoax threats is to induce exactly this level of disruption and chaos.

### VOICES FROM THE FIELD

**“People do not understand the amount of time school administrators are spending on [behavioral] threat assessments. They are doing this on a regular basis. What district offices are doing and what they are training [administrators] to do is a very different conversation.”**

*- K-12 school district and state-level representative, February 2023*

**“Kids are expected to go back to class and go back to learning like [a lockdown] didn’t happen. Students have to go through these mental mind shifts all the time—lockdown back to learning. [In] communities that have had a [gun violence] incident in the past, you are retraumatizing them.”**

*- K-12 school district-level representative, February 2023*

The actions that local education agencies and their law enforcement partners take after becoming aware of a threat often promote stress and fear across a school community with the emotional toll lasting well beyond the immediate aftermath of a threat. Lockdowns and school cancellations resulting from a threat often induce long-term trauma and instill a fear of returning to school (Rich and Cox, 2018; Perez, 2022). An increase in law enforcement presence at a targeted school—a common response to threats—can also further heighten stress among certain populations (Rich and Cox, 2018). These impacts are especially pronounced among students who have already experienced some form of trauma. Parents and other caregivers are also deeply affected by threats of shootings and commonly make their own decisions to keep kids at home after hearing about or seeing a threat (Chabria, 2023; Rich and Cox, 2018). When threats spread like wildfire, which they often do when posted online and to social media, they become the subject of rumors and misinformation that only intensify fear across a community (Regehr et al., 2017; Wong, 2021).

Anonymized threats also have a significant impact on community-level resources, most notably law enforcement and first responder partners. According to the FBI, hoax threats can place police officers and others in unnecessary danger and divert critical resources away from other community responsibilities (FBI, 2018). The sheer number of threats that some schools and districts have faced, many on a weekly basis, places a cumbersome tax on already constrained resources and workforces.

# Containing the Problem: Early Awareness and Detering Future Threats

Schools can work to detect threats early and deter threat-making by emphasizing the importance of reporting and educating their school community about the consequences of making threats, even if they are intended to be jokes. This section details strategies schools can implement to prevent, detect and deter threats.

Responding to threats effectively depends on information that is provided to a school and public safety decisionmakers about the threat and information shared with the school community to reduce the number of threats made by students in particular. Students, staff, parents and others with direct interaction with students are the best source of information about what is happening in a school community. As a result, their awareness about how to report threats and vigilance about what is going on across online and offline communities connected to school is critical to ensuring that school leaders find out about threats in a timely way. The information and resources that a school and local education agency provide to their community, particularly students, can also reduce the number of threats made against a school by providing a path to addressing the underlying problems that can lead students to making threats and educating them about the potential consequences of doing so.

## // 2.1 Build Awareness About Reporting Threats

Bystander reporting is a critical violence prevention tool for K-12 schools (see e.g. CISA and NTAC, 2023; Moore et al., 2023; NTAC, 2021). Efforts to detect threats against schools before they can spread should therefore focus heavily on building awareness about reporting. This is especially important for students. Students at a school are often most aware of the behavior of their peers and can often provide some of the most valuable information about threatening posts that may include some level of anonymity.

Surveys of K-12 teachers suggest they feel confident that students and school staff report threats when they hear of one. They believe most students will report directly to teachers, followed by other school staff members, and then school security staff such as school resource officers (SROs) (Jackson et al. 2023). Schools often become aware of threats either through direct communication with school staff, students, and parents, or through anonymous tip lines. Spreading the word about the importance of reporting and how to report is critical

to preventing the spread of threats posted online. A key message issued by schools when it comes to online threats such as those posted to social media can be to “Report, Don’t Repost” threats. Capturing a screenshot of a threat to provide to school or law enforcement (e.g. directly through a tip line if it allows submission of image or video data) can help an investigation while reposting that screenshot broadly hinders efforts to resolve the situation. When threats are reposted, sometimes across different social media platforms, users may further spread misinformation, cause confusion, strain additional resources and make identifying the origin of the threatening post even more difficult for investigators. Schools can help build awareness about reporting at various points throughout the school year through all-school assemblies, messages to families, posters and other methods. The [CISA-United States Secret Service K-12 Bystander Reporting Toolkit](#) provides in-depth guidance about how to support and encourage a trusting reporting culture at K-12 schools across the country.

## // 2.2 Prepare Staff Who Might Receive Anonymous Threats By Phone to Capture Key Information

The goal of investigators responding to an anonymous threat is to break that anonymity and to identify who is making the threat as quickly as possible. In contrast to anonymous threats made via social media or communicated in writing, telephoned threats provide an opportunity to collect information that can aid an investigation. Because telephoned bomb threats have been a security problem for schools and other sectors for decades, protocols exist that lay out a list of questions that individuals fielding a phoned-in threat (e.g. administrative

assistants and attendance clerks) can attempt to ask when the threat comes in. For example, CISA’s [Bomb Threat Checklist](#) includes questions the receiver should ask the caller about the supposed bomb (e.g. what it looks like, where it is placed). The more information collected, the better an individual fielding the threatening communication can aid response operations and actions. Discrepancies or contradictions in the caller’s answers can also suggest that the call is a hoax.

Similarly, CISA's guidance includes questions for those receiving the called-in threat focused on what they heard: details about background noises in the call, the characteristics of the caller, and whether the voice sounded familiar. Such details can help identify a caller, but caution is also warranted. Manipulating details like background noises (e.g. adding gun fire sounds) is one way swatting calls have been made to seem more credible.

## // 2.3 Educate the Community About Youth Social Media Use, Especially Families

The more education that schools can provide to students, school staff, parents and others about youth behavior on social media, the better. Social media can often be a black box for school staff and parents, in part given the proliferation of platforms. Many adults are left in the dark when it comes to even their own children's activity in these spaces. Considering the near ubiquity of social media use by today's youth and what appears to be a growing number of threats posted to social media, many schools have implemented communications campaigns to educate students, parents, and school staff about what constitutes a threat online, what is considered inappropriate or threatening behavior on social media platforms, and the damage that threats can do to a community even if they are meant as a joke (Moore et al., 2024).

Outreach and training directed specifically at parents may be especially important to prevent threats or help detect them

early. Schools have hosted meetings on internet safety designed for parents and published guides on identifying threats and what to do when a threat is discovered. These meetings and other short training materials can serve as an introduction to various social media or gaming platforms, language or imagery commonly used online by youth, and other trends. A number of states have also published resources in this area (see e.g. Texas School Personnel's [Guide to Social Media](#)). Some schools and school districts have also taken to social media to disseminate their own posts about internet safety, dispel rumors about a threat or respond to social media-based challenges that often prompt an onslaught of threats. Such messaging can confirm to their communities that they are aware of ongoing trends and reinforce the message of not contributing to their spread.

### VOICES FROM THE FIELD

**"It is super important that parents know what their kids are doing in social media."**

*- State school safety agency representative, January 2023*

## // 2.4 Provide Mental Health Resources to Help Mitigate Threats

The lessons already gleaned from experience with behavioral threat assessment in K-12 schools suggest efforts focused exclusively on penalizing threatening behavior are not the answer. Instead, experts suggest that directing resources towards treating whatever underlying problem may have caused an individual to initially post a threat is likely a more effective strategy. Threats made by students are often indicators of other problems or student needs, including suicidal intent, and more akin to cries for help than intent to do harm. Studies have shown that expressions of suicidal intent often precede acts of targeted violence both inside and outside of school environments (Stephenson, 2023; Williams, Bogel-Burroughs, and Arango, 2023). By fostering a positive school climate, students may feel more supported and encouraged to report problems or threats by themselves or with classmates.

Unfortunately, K-12 schools and school districts across the country are experiencing a dire shortage of school counselors, psychologists, social workers and therapists. As of this writing, the shortfall could be upward of 100,000 professionals (St. George, 2023). A key way to help prevent future threats will likely be to ensure that school counselors, teachers and parents understand that earlier intervention is better than intervention after the fact (i.e. after a student has made a threat). Schools should consider adding mental health professionals and other affiliated services or programs, such as multi-tiered support systems and frameworks like Positive Behavioral Interventions & Supports that emphasize social, emotional and behavioral health. By incorporating these practices, school districts can identify students' needs sooner, putting them on a path towards addressing any underlying issues and potentially preventing threats and the disruption that they cause.

## // 2.5 Take Actions to Deter Future Threats

Multidisciplinary threat assessment teams can be an effective violence prevention tool, especially when the threat is known. However, what can schools do beyond prevention to deter future threats? Here, too, the answer lies largely in efforts to educate the broader community. If threats are often the indicators of other problems experienced by a student or someone else, imposing penalties on threat-making should be the exception rather than the rule. Schools can learn from existing practices in the field of behavioral threat assessment that respond in a way that changes behavior without imposing lifelong consequences for poor decisions made as a youth. Schools should communicate the potential consequences of making threats, even as a joke, as part of regular outreach and education efforts to prevent violence. Deterrence through education, in other words, is likely to be a better solution than focusing exclusively on deterrence through visible consequences.

That said, law enforcement and criminal justice organizations will make their own decisions if a law has been

broken. Moreover, different solutions and approaches may be required when the disruption caused by a threat is significant. The swatting incidents that have plagued districts across numerous U.S. states, for instance, likely require law enforcement and legal consequences. If the individuals responsible for such threats are indeed located overseas, as some sources suggest (Keierleber, 2022; Glass, 2023), proposals to impose severe consequences for threat-making are not problematic. When students are the ones making threats that cause significant disruption to their school or even an entire district, individual cases can also be brought to prosecutors and judges who understand the global costs of such incidents. For this solution to provide tangible benefits as far as deterring threats is concerned, efforts should also focus on educating prosecutors, judges and others involved in the juvenile justice system about trends around and the impacts of anonymized threats.

### Box 2.1 Setting Up Practices to Prevent and Deter Anonymized Threats

#### What's happening with anonymized threats in your school district?

Worksheet 1 of this toolkit, [Taking Stock of Anonymized Threats at Your School](#), includes a set of questions for schools and districts to consider as they assess trends on social media-based and other types of anonymous threats and their current detection and deterrence practices.

#### How do your school's current practices support bystander reporting?

See CISA and United States Secret Service's [K-12 Bystander Reporting Toolkit](#) to assess your current reporting practices.

#### Informing parents and others about youth social media behavior

Safer Schools Together offers a parent guide, [Raising Digitally Responsible Youth: A Guide for Parents and Caregivers](#), that includes an overview of multiple social media platforms, common internet and social media slang used by youth, as well as descriptions of common internet safety issues and tips for setting digital boundaries with youth (Safer Schools Together, 2023).

Safer Schools Together also developed the [Social Media Parents Checklist](#) with suggested practices and habits to establish around social media use (Safer Schools Together, n.d.).

### Informing parents and others about youth social media behavior

Schools across the country are providing various resources focused on improving digital citizenship across their communities. New York City Public Schools (NYCPS), for instance, provide information on [digital citizenship](#) to their community through the district website. Fairfax County Public Schools in Virginia provides [a similar resource](#). These resources include details on parent, teacher and student responsibilities around using the internet in ways that are “safe, responsible, and appropriate” (NYCPS, n.d.).

### Resources to address school crises

The National Association of School Psychologists (NASP) provides a tip sheet called [Social Media and School Crises](#). The resource describes the potential risks associated with social media use including its potential to contribute to psychological trauma and other challenges. It also discusses its benefits to schools in the areas of crisis prevention, intervention and postvention.

### Building awareness on the consequences of threat-making

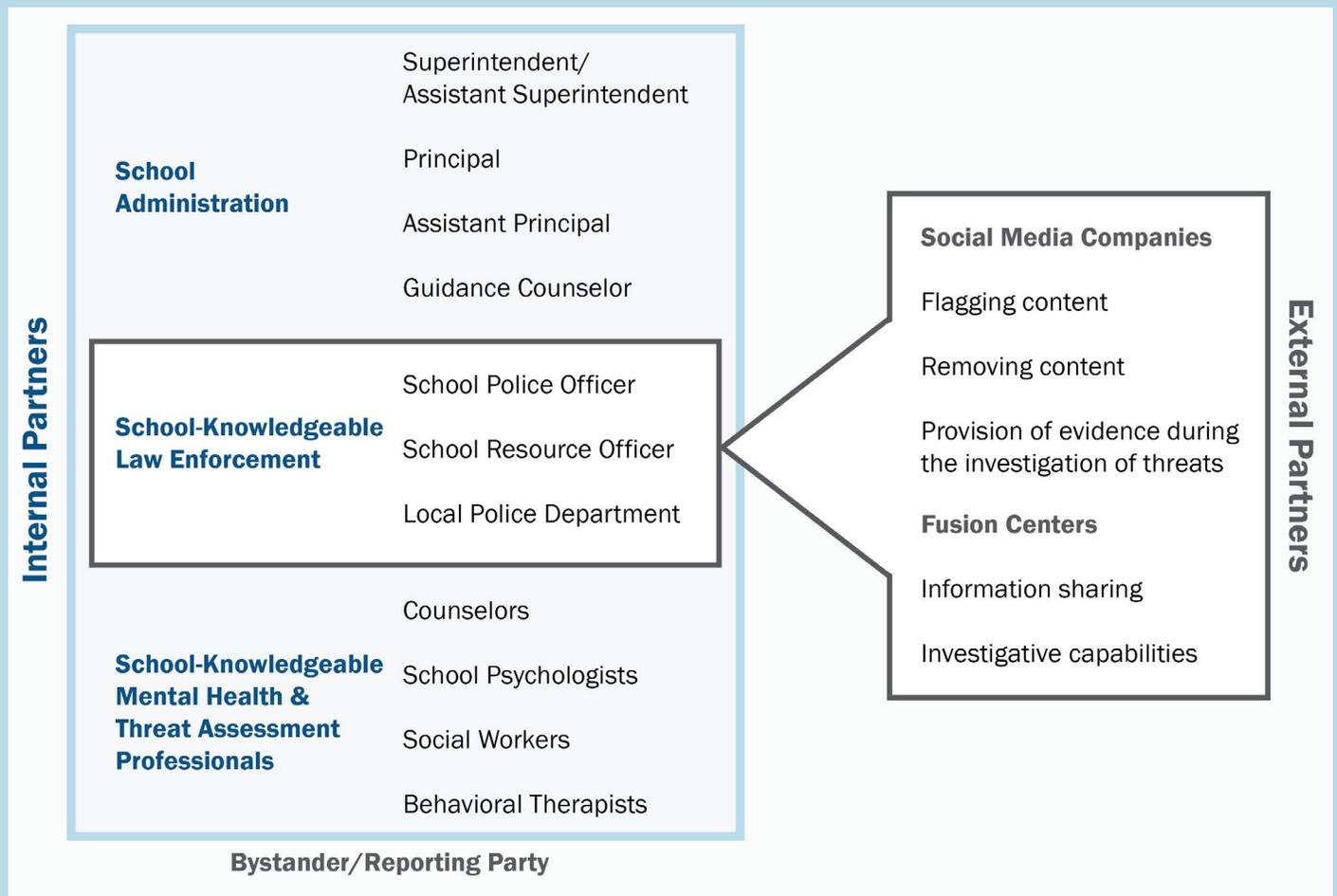
According to the FBI, hoax threats can be serious federal crimes. The FBI’s 2018 [#THINKBEFOREYOUPOST](#) public awareness campaign aims to build awareness about the potential consequences of engaging in inappropriate and dangerous behavior on social media (FBI, 2018).

# Key Partners in Addressing Anonymized Threats to K-12 Schools

Addressing anonymous threats requires strong partnerships within the school community and with outside community partners, such as law enforcement agencies and mental health professionals. This section provides an overview of key partners involved in the response to anonymous threats.

Schools work with several different partners both inside and outside the school community to address anonymized threats. Each one plays a key role in the immediate response to threats, investigation and assessment of threats, and aftermath of threats. Often, partners can play numerous important roles across these different phases. Figure 3.1 provides an illustrative model of a partnership structure for addressing threats. Because every school context is unique, schools and school districts should strategize to decide what type of partners work best to meet their unique needs.

Figure 3.1 **Potential Partners for Addressing Anonymized Threats Against Schools**



SOURCE: Homeland Security Operational Analysis Center (HSOAC) analysis.

## // 3.1 Reporting Party

As noted in the previous section, bystanders are key to making schools and school districts aware of threats via reporting. Students, school staff, parents and other members of a school community are, therefore, critical partners in the process of addressing threats against schools. Whether a threat is reported directly to a teacher, other school staff member, law enforcement officer or via a tip line, bringing a threat to someone’s attention is the first step towards addressing it quickly and effectively.

## // 3.2 School Administrators

Administrators—superintendents, principals, assistant principals, etc.—are often the first to become aware of a threat against their school or district. They are also often responsible for making immediate decisions about how to keep their communities safe. Will they lock the school’s exterior doors? Will they go into full lockdown inside the school? Will they evacuate the school or cancel school the following day when a threat comes in overnight? School administrators are also the central link to other partners, discussed below.

## // 3.3 School-Knowledgeable Law Enforcement

Law enforcement personnel with knowledge of the local school community are key partners for schools and school districts targeted by anonymized threats. Law enforcement is critical when it comes to responding to threats, investigating threats and assessing the level of concern posed by threats. For example, they may provide additional security personnel to ensure the safety of the community. Law enforcement can often provide immediate assistance in areas where school administrators and other school personnel may lack expertise, for instance through access to intelligence and other information that can help schools address threats more expediently. Some law enforcement agencies may have the capability to carry out social media searches and analysis to gather more information about a threat at a much more sophisticated level than schools. Local police’s ability to liaise with other law enforcement and intelligence agencies, including fusion centers, can help ascertain the origin of a threat, assess whether other schools in the area have received

identical or similar threats, and specify what others are doing to respond (REMS TA Center, n.d.). Law enforcement agencies can also connect with social media companies to gather additional intelligence about user accounts and other details about a threat that may not otherwise be publicly available.

Many times, the critical link between a local education agency and a local police department is the school or district SRO or a school police officer. Other times, school district staff such as an assistant principal, principal or superintendent may have built up strong rapport with local law enforcement in their community, making communication during and outside emergencies seamless. In general, these types of longstanding relationships between school and law enforcement personnel within the same community help to build trust and create working relationships that greatly benefit schools when they are the target of a threat.

### VOICES FROM THE FIELD

**“I have a group of kids [I can rely on]. A lot of times they come to me with things. Or I can ask them questions. These relationships with a network of students are key to the SRO role - they really help us out.”**

*- K-12 school safety professional, February 2023*

Of course, the reality that every school context is unique means that relationships with school-based law enforcement agencies vary across the country. Districts in remote rural areas, for instance, may have inconsistent access to smaller and less well-resourced police departments relative to local education agencies situated in suburban or urban locales. Because there is no real national standard for school-based law enforcement personnel (including SROs), there is also considerable variation among the officers working directly with schools. Some have close relationships with the student body that they’ve developed over time, whereas others may have

limited opportunity to engage with schools due to competing responsibilities. Community attitudes towards police in schools are also uneven across different parts of the country. Ultimately, this means that there is no one way for local education agencies to partner with law enforcement when addressing threats, and relationship-building will look different from one school or district to another. Nevertheless, sharing responsibilities between local education agency and law enforcement personnel in the context of anonymized threats is critical to making difficult and potentially high-stakes decisions and avoiding tragedy.

## VOICES FROM THE FIELD

“Some areas have amazing SRO programs. These officers have great relationships with the students, they know how to ask questions that let them sort out whether a threat is real or not. But there is no SRO standard across the country. Some are just there, and other schools are served by patrol officers who know nothing about a school.”

- Federal law enforcement agency representative, February 2023

### // 3.4 School-Knowledgeable Mental Health and Threat Assessment Professionals

Several other partners may help schools address anonymized threat situations. Determining the response to anonymous threats can be informed by expertise not just from the school and public safety perspectives, but from school-based psychology, counseling, social work and other fields that participate in a multidisciplinary threat assessment team. The heart of a traditional multidisciplinary threat assessment team involves bringing together knowledge, perspectives and approaches from different fields to better understand the level of concern posed by a threat from a known actor. Therefore, the individuals on a school’s multidisciplinary threat assessment team may be able to play a key role in providing insight and context to anonymized threats, particularly if similarities are identified among current threats with past incidents.

It is important to note that the utility of a multidisciplinary threat assessment team to support response efforts may be limited prior to knowing the identity of the individual making the threat. However, given the range of experience among team members and their insight of past incidents, they should be considered for inclusion when determining a response to an anonymous threat. Additionally, should the individual who submitted the threat or engaged in the concerning

behavior eventually be identified, including the multidisciplinary threat assessment team early on may position them better to conduct their traditional processes and expedite necessary support or intervention services.

Beyond response, school-based psychology, counseling and social work professionals can be critical to minimizing some of the negative impacts that threats can have on the school community at large. Having mental health professionals such as school counselors, psychologists, behavioral therapists, social workers and others from the wider community ready to work with students, teachers and other staff in the aftermath of a threat is key to minimizing emotional trauma and recovering from such incidents. These individuals can also work with parents to help manage the stress and trauma that they too can experience in such situations. In short, although K-12 schools are currently experiencing a national shortage of such professionals (St. George, 2023), they are likely critical to helping schools address social media threat situations in addition to myriad other challenges.

#### Example Threat Scenario

Students at an elementary school saw and circulated a threatening message written on the bathroom wall. School administrators were eventually notified and removed the writing, and a multidisciplinary threat assessment team was able to identify the student responsible. The following day, the district superintendent sent the following message to the school community: “We are taking this incident very seriously and following the necessary protocols and safety precautions, including working with our school resource officers, local law enforcement and our district safety team. A longstanding practice in the district... involves us also doing a threat assessment for our students experiencing distress. This is underway as we send this communication. ...the safety and wellbeing of our students is our top priority.”

# First Response: Immediate Actions When a Threat is Received

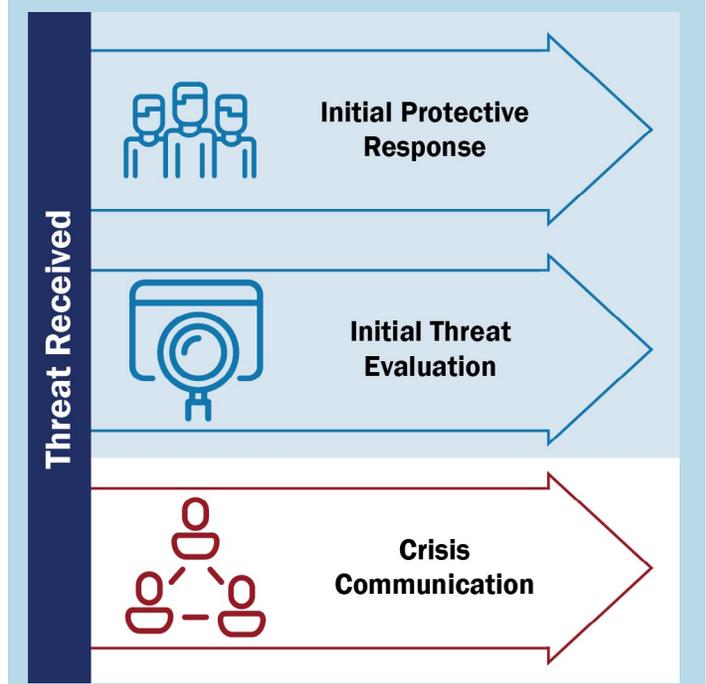
Every threat received by a school should initially be deemed credible, and schools should work with their law enforcement partners to decide on immediate needs to keep their community safe. This section provides information on the initial responses schools should take to anonymized threats, including assessing the level of concern posed by a threat and communicating with parents and the broader community in a timely and accurate manner.

Anonymized threats of violence against a school or district require local education agencies to make quick decisions about how best to keep their community safe, often before knowing much about the origins of the threat. Local education agencies must treat every threat as initially credible. As soon as they are aware of a threat, they are forced into making real-time decisions about whether to increase police presence at the targeted school, restrict movement into and out of the school, go into a full lockdown, cancel school altogether, or implement a combination of options.

These actions, however, can cause trauma for students, teachers, others at the targeted school and the surrounding community. Moreover, some of these actions lead to losses of instructional time or call for even more resources, such as busses to transport children to reunification areas or additional lunches to feed students restricted to campus for the remainder of the school day.

Deciding on how best to keep a school safe immediately after receiving a threat is difficult. In this section, the toolkit discusses those first response actions that can be taken to ensure safety, creating the opportunity for schools to respond deliberately based on an assessment of the seriousness and credibility of a threat. These actions fall into three parallel streams. The first two closely linked streams include initial protective responses and initial steps in the threat evaluation process that will guide decisions about whether to escalate or end response actions over time. The third stream involves crisis communication with the school community to help keep everyone informed and minimize further trauma that threat and response efforts might induce (Figure 4.1).

Figure 4.1 Action Streams in the Initial Response to an Anonymized Threat



SOURCE: HSOAC analysis.

## // 4.1 Initial Response to Threats to Ensure Campus Safety

Responses to anonymized threats against K-12 schools should be specific to the information available at the time. Fortunately, most threats to schools, in the words of one interviewee for this study, “turn out to be nothing.” However, when a school receives a threat and little to no additional information is available, decision makers cannot know for sure if that threat is truly baseless. As a result, the goal of a school’s or district’s initial response should be to act prudently to protect the school but still allow instruction and other everyday school operations to continue uninterrupted. School officials and their community partners should remain prepared to rapidly scale up response should new information add weight to a threat. Such approaches help to minimize the “drama and trauma” associated with many anonymized threats and keep students, teachers and others safe.

Being prepared to take a set of preplanned steps to ensure safety is critical before more detailed information about a threat is available. Starting with actions that are minimally disruptive to the school community, for instance adding low-visibility law enforcement personnel to the targeted school, allows schools to rapidly increase security with minimal concern about how response actions might affect students or staff. Implementing these initial response actions quickly after notification of a threat can provide the time and opportunity for school and law enforcement decision makers to respond deliberately to individual threats and scale up response to threats of greater concern (which this toolkit discusses in depth in [Section 5](#)).

## VOICES FROM THE FIELD

“You don’t want to be overly reactionary, because so many [threats] turn out to be nothing. But even if they are nothing, we still get trauma, absenteeism, anxiety.”

- Local law enforcement agency representative, February 2023

### // 4.2 Initiating Threat Evaluation to Inform Response

A local education agency has no choice but to treat all threats that it receives as initially credible. Given the frequency and volume of threats, assessing the viability of a threat and the risk that it poses is a resource-intensive and daunting task. The anonymity of the internet generally, and of certain social media platforms specifically, also adds unique challenges. Additionally, the proliferation of free internet calling devices often makes it difficult to link threats to a specific individual. In general, the task of discerning between threats that are just seeking attention or a reaction (hoax threats) and those that truly pose danger to school communities is an extremely difficult one. Threats appearing on social media in particular are often reposted and circulated widely, which makes tracing them back to their original source difficult (Moreschi, 2022; Regehr et al., 2017). The use of fake social media accounts, so-called vanity names—unique usernames tied to a social media account that do not reflect the name of the account owner—and internet calling services that allow anyone with an email address to make phone calls appearing to come from a U.S. number also make tracing these kinds of anonymized threats to a specific individual uniquely difficult (Slater, 2023; Amman et al., 2017; Trump, 2016).

Receiving a threat prompts a school to begin a process of gathering more information. This process ultimately allows school officials to adjust response efforts meant to ensure

campus safety. Ideally, such information gathering, which takes place in partnership with law enforcement, breaks the anonymity of a threat and enables a school to use standard behavioral threat assessment processes and their broader knowledge of a specific student and their circumstances to inform judgment about the level of concern that a threat poses. However, when schools and their partners are unable to immediately determine the identity of the person behind a threat, a variety of factors can help provide insight into the level of concern posed by a threat and help a school and its partners decide whether the initial response is sufficient to keep a community safe or if additional measures should be activated.

School and law enforcement personnel across the country have highlighted different types of information to look out for that can add context to an anonymized threat and provide clues about the level of concern that it poses (Moore et al., 2024). For example, factors such as hints of physical proximity to the targeted school(s) as well as specific or personalized language, like references to students or gang symbols, typically add weight to a threat. Posts that include live media streams or that are delivered via close-range wireless communication services such as AirDrop suggest that a threatening individual is physically close to their target.

#### Box 4.1 Assessing Threatening Written Communications

Assessing the risk posed by threatening written communications is different depending on whether the identity of the threatener is known. When a threat is not anonymous, there are several factors that can add weight to a threat. Those factors include evidence of preparation or feasibility of an attack (e.g. access to weapons); details about the specific motivation(s) for an attack; risk behaviors like a history of substance use or abuse; and various other warning behaviors (such as fixation, identification with specific mentalities or personalities, novel aggression, or “last resort” behavior) (Meloy et al., 2021; Mitchell and Palk, 2016). The inclusion of personal information about a targeted individual or hints that the threatening individual may be in close physical proximity to their target as well as repeated threats and the use of escalatory language also suggest higher-risk threats (Amman et al, 2017; Van Brunt, 2016; Safer Schools Together, 2019).

By contrast, the use of recycled photos, stock internet images or reposts of previous school threats might reduce the urgency of a threat. Likewise, threats that come in clusters—targeting multiple schools in the same geographical area, across the same state or even nationwide—might suggest that a threat does not pose a significant level of concern and is more likely part of a series of hoaxes. It is also worth considering that school and even student-specific information is often publicly available online. In other words, individuals making hoax threats can easily make their threats appear eerily specific based on simple internet or social media searches.

When first becoming aware of an anonymized threat, school and law enforcement personnel involved in the threat assessment process can use key questions to gather information that will help to add context to a threat and ultimately help assess the level of concern it poses as well as its imminence. The goal of the questions included in this section is not to present a checklist of items that will help schools and law enforcement personnel assign a risk “score” to a threat but rather to assess concern based on the specific circumstances of the threat.

## Consider Background and Contextual Information

This initial set of questions represents the minimal amount of information a team should possess before moving on to a more comprehensive assessment. They focus on critical background and contextual information related to the threat situation (Simons and Tunkel, 2021):

- How was the anonymized threat delivered? (e.g. Via social media? If so, what platform? Was it posted to a school or school-related social media site? Via phone?)
- Who is the target of the threat (named and implied)? Is the school in general a target, or is a specific individual or group of individuals the target?
- Does the anonymized threat name or reference any other schools, individuals, or organizations, and what is their relationship to the threat’s primary target?
- How many anonymized threats have targeted the school or individual(s)? During what timeframe? (e.g. Was the school or individual(s) the target of other threats, for instance through different means like phone, social media, etc.?)
- Is this a single, isolated threat or part of a series sent to the same school or individual(s)?
- When did the school first become aware of the anonymized threat, when did the threat originate and how did the school receive notification of the threat?
- When does the anonymized threat say the threatened act of violence will occur?
- Does it appear feasible for the threatening individual to carry out the threatened act? (e.g. Does the threat provide evidence of access to a weapon or physical proximity to the target?)
- What is the significance of any locations or dates named or referenced in the anonymized threat? (e.g. Does the threat refer to a past school shooting location or date?)
- What steps or measures did the individual making the threat take to conceal their identity? (e.g. If it was a social media post, was it created under a vanity name? Did the author remove the post from their social media account?)
- If the anonymized threat targets a specific individual or group of individuals, what details are available about that individual’s or group’s prior history as a victim or target of threats?
- If the anonymized threat targets a specific individual or group of individuals, what is the individual’s or group’s reaction to or assessment of the threat?
- What specific analysis and steps are required moving forward? (e.g. identifying the origin of the anonymized threat, assessing concern for violence, assessing imminence of violence, implementing response actions)

## Detect Patterns

As noted elsewhere in this toolkit, anonymized threats against K-12 schools often come in clusters or waves. During so-called social media challenges or in the aftermath of actual mass shootings, schools can be the target of numerous anonymous threats or multiple schools within one school district might experience threats. In such overwhelming situations, it is important for local education agencies and local law enforcement partners to have a structured method for quickly triaging numerous threats so that hoaxes can be separated from threats that may require more attention. Consider this next set of questions to further help identify any relevant patterns in threats targeting a school (see Simons and Tunkel, 2021):

Are the threats to the school or schools specific or diffuse? Consider factors such as target type (i.e. Are only schools receiving threats?); geography of the targets; timeframe of threats; and references to specific events, issues or modes of violence.

*Widespread threats targeting numerous schools across a district, state or even nationally at the same time are often an indication of hoax threats and thus pose a lower level of concern relative to threats directed at a specific person or just one school.*

Is there any evidence that the threatening individual is in close physical proximity to the targeted school(s)?

*Evidence that the anonymous threats are being issued by someone who is in close physical proximity to the targeted school(s) might be indicative of heightened willingness to carry out the threat, which elevates the level of concern posed by the threats.*

Do the threats appear to be recycled or copy-pasted from other threats targeting other schools in the local area, state or nationally?

*Threats that have been reposted across social media or that use copied language from other threats (past or present) are often indicative of hoax threats. Unique threats that show that an individual has put time into crafting specific, unique language should raise concern relative to recycled threats.*

Are the threats targeting the school(s) associated with a significant event such as a school or other type of mass shooting or another violent event?

*Copycat threats certainly can lead to actual violence; however, waves of similar threats that come in the aftermath of actual acts of violence may not be as concerning as threats indicative of deeply held personal grievances. If language in the threat suggests that the individual is personally affected by the recent violent event, this should elevate concern.*

Does there appear to be a goal associated with the wave or cluster of threats, such as:

- Prompting an evacuation of the targeted school(s);
- Entertainment or amusement;
- Generating media attention;
- Sowing disorder;
- Canceling classes, for instance, during exam times;
- Financial gain; or
- Inciting others to violence?

*Certain motives behind threats can be more concerning than others. Threats that appear to be made as a joke, to wreak havoc or to get students out of school for the day are less concerning.*

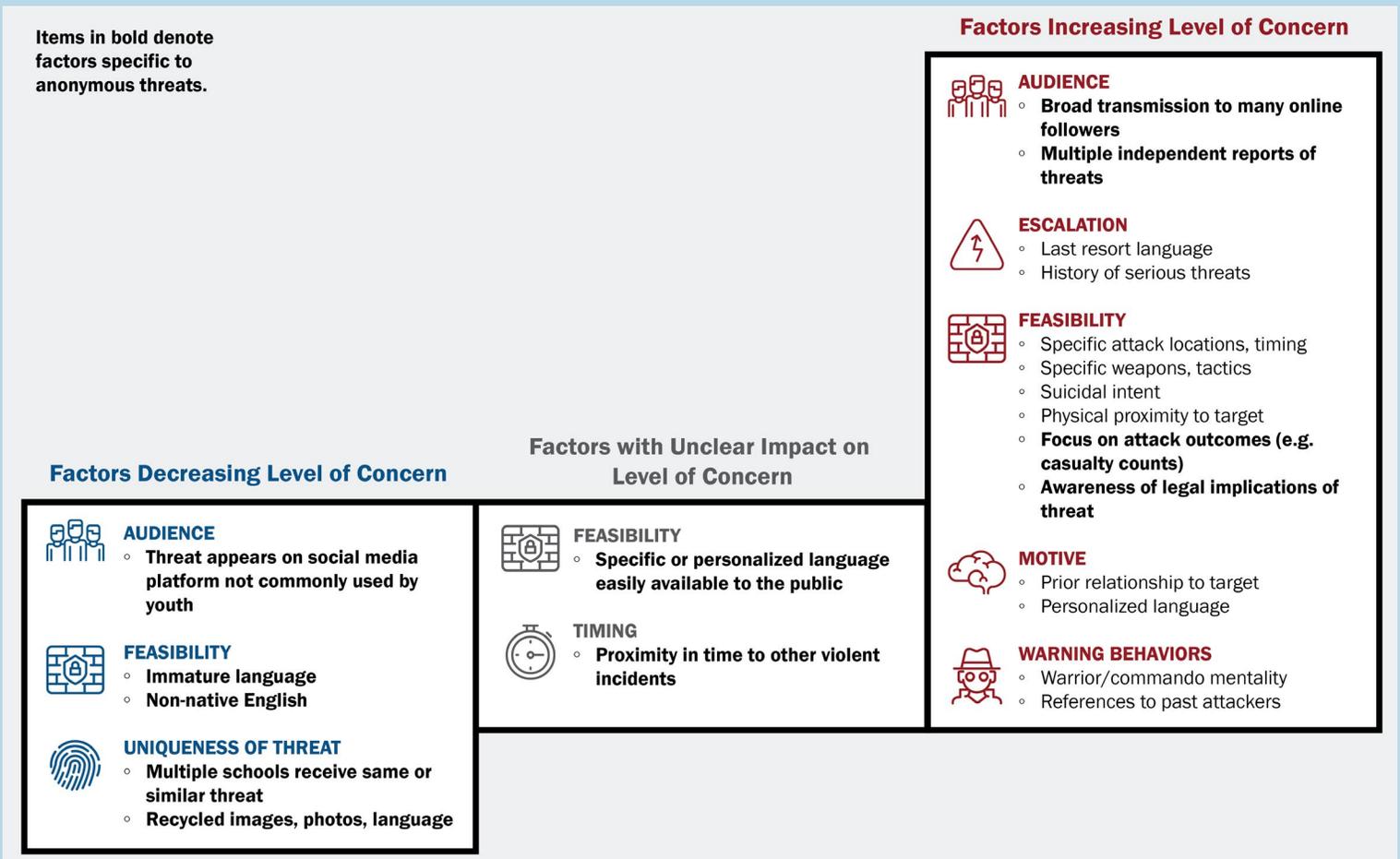
## Identify Signs of Imminence

Determining the imminence of a threat—or the increasing probability that the threatened act of violence will occur during a specific timeframe—is also critically important. The imminence of a threat will inform the speed and level at which response actions should be deployed. School and law enforcement personnel can look for various signs that might indicate imminent violence, including:

- Does the anonymized threat include statements about waning patience or “being tired”?
- Does the anonymized threat suggest that the threatening individual’s opportunity for action is shrinking because of circumstances such as impending death, arrest or declining health?
- Does the anonymized threat refer to violence being the “last resort” or having no other choice but to resort to violence?
- Does the anonymized threat indicate that the threatening individual has also prepared or issued a manifesto, last will or other legacy token meant to stake a long-term claim to their threatened act of violence?

The presence of these or similar indicators in an anonymized threat often call for a rapid response reaction to keep the campus and school community safe (Simons and Tunkel, 2021). As noted throughout this toolkit, school and law enforcement personnel should work together to evaluate the needs for additional awareness or security personnel as well as the need for securing the school campus and building.

Figure 4.2 Weighing the Level of Concern Posed by an Anonymized Threat



SOURCE: HSOAC analysis of interviews with K-12 school stakeholders.

## Assessing Level of Concern Supports Response Until the Threat is Resolved

The initial assessment of an anonymized threat might identify factors that significantly reduce the level of concern that it poses (e.g. if information shows that the threat's origin is far away from the school itself or even from another country). However, other situations may prove more complex if the available information makes it much more difficult to assess a threat (e.g. if the threat uses recycled images or stock photos but still reflects a certain level of specificity or personalization). In such cases, the assessment process should continue in an effort to gather additional information. At the same time, schools and their law enforcement partners should make deliberate efforts to match response actions to keep the school campus and community safe. [Section 5](#) of this toolkit discusses the range of options available to schools when it comes to increasing or decreasing the intensity of response actions as new information elevates or lowers the level of concern associated with a specific threat.

### Box 4.2 Assessing the Urgency of a Threat Against K-12 Schools

#### Setting up threat management teams gauging levels of concern

- The FBI produced guidance on [identifying, assessing and managing threats of targeted violence](#), including assessing levels of concern (e.g. low, medium, high) and factors that can increase the urgency of threats. The resource also includes guidance around setting up threat management teams (Amman et al., 2017). See [Box 1.1](#) for more guidance for reporting threats.
- The Readiness and Emergency Management for Schools Technical Assistance Center (REMS TA) developed a webinar on [integrating social media into threat assessment](#) that highlights key steps for preparedness and planning efforts.

#### Gathering contextual information and detecting patterns

- Worksheet 2 of this toolkit, [Gathering Information When You Receive a Threat: Where to Start?](#) includes a set of questions for schools and districts to consider as they begin collecting information and outreach actions to support quick turnaround.
- The Illinois Terrorism Task Force School Safety Working Group (2018) provides a one-page list of initial [response and investigative suggestions for school threats](#).
- Safer Schools Together (n.d.) has developed [guidelines for responding to digital threats](#) that highlights key information to gather when the threat maker is known vs. unknown.
- The Washington Office of Superintendent of Public Instruction has developed useful [strategies to address swatting](#) incidents, and describes common patterns and indicators to help identify swatting threats.
- [Fusion centers](#) also provide valuable investigative support to schools, districts and local law enforcement agencies, including a specific social media investigations unit as well as access to information systems among other supports.

## // 4.3 Crisis Communication with the School Community

Communicating in a timely, accurate and equitable way is critical to managing threat emergencies. This is the third key action stream in initial response to a threat. Sharing as much information as possible with parents, school staff and other community members without breaching confidentiality or impeding an ongoing threat investigation can help to manage expectations, keep fear in check and avoid the viral spread of rumors. Social media threats in particular are likely to circulate quickly and widely, and local law enforcement personnel who have responded to what turned out to be swatting incidents have referred to them as “terror without a body count” (Slater, 2023).

### Example Threat Scenario

Shortly after 9 a.m., repeated announcements over a school’s PA system notified everyone inside to lock down and turn out the lights out and that it was not a drill. Within the next minute, police SWAT teams in full gear swarmed the school with weapons drawn. The incident lasted about two hours until law enforcement was able to determine that the phone call placed to police of shots fired inside the school was false. After police cleared the school and the lockdown was lifted, school district administrators sent the following email to families: “The lockdown has now been released and staff and students are safe. Swatting is a criminal harassment tactic of deceiving an emergency service into sending a police or emergency service response team to a school or other place. Swatting causes extreme disruption and can be dangerous. It is also deeply unsettling for anyone affected. This particular incident has impacted several schools and districts across the state today.” School officials planned to debrief the situation with staff and students to ensure access to needed mental health support.

Messages to the broader community can be circulated via email, text message, and/or posted to school or district social media pages and websites. A joint message from the district superintendent and local law enforcement can help ensure it carries the necessary weight. Here are examples of the types of detail such messages might include: <sup>2</sup>

- The nature of the threat;
- The date and time of the threat, if one is specified;
- The fact that school officials immediately contacted local law enforcement and they are jointly investigating the threat (or have completed an investigation);
- The fact that the threat has been deemed not credible, if that has been determined;
- Whether school will be opened or closed (If school is closed, lead with this point.); and
- What additional security measures or actions are being implemented or taken out of an abundance of caution (e.g. more police have been added to school grounds, security checks at building entrances, etc.).

Messages should be tailored for their audiences to ensure inclusion among the entire community and also reassure parents that the safety of students and school staff is the top priority. Additionally, language should be included to demonstrate that school and law enforcement personnel are working together to resolve the threat as quickly as possible. Asking parents and other community members to contact law enforcement if they have any information about the threat is also a good idea. Updated messages should be disseminated with any new developments or when the emergency is resolved. The foundation for effective crisis communication that helps to reduce trauma and support the resolution of threat situations originates in preparedness efforts that inform the school community about school procedures, security efforts, and actions taken to keep students and staff safe ([see Section 6](#)).

<sup>2</sup>This list is adapted from the Illinois Terrorism Task Force School Safety Working Group, “Communications Tips for School Threats” (2018).

## Box 4.3 Using Social Media to Communicate with the School Community

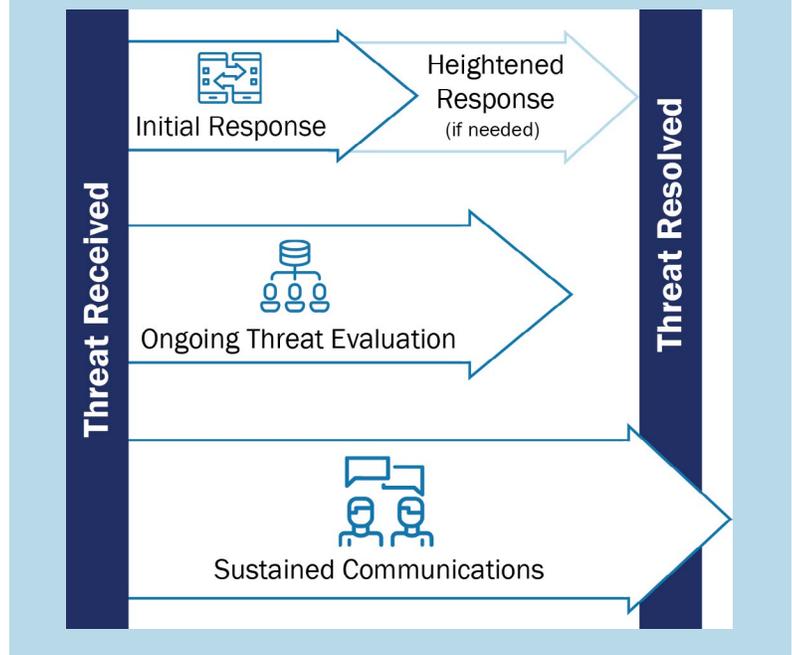
NASP developed a resource for both parents and educators about how to best employ social media before, during and after a crisis incident. [Using Social Media Before, During, and After School Crisis: Tips for Parents and Educators](#) provides guidance on how schools can most effectively use social media across all school emergency operations phases including prevention, protection, mitigation, response and recovery.

# Deliberate Response: Balancing Response Actions for Complex and Uncertain Threats

Implementing a balanced response that keeps the school community safe while minimizing additional trauma is key to addressing anonymized threats. This section details how schools can start with less intensive and less overt actions in response to a threat and integrate options for escalation or de-escalation based on additional information revealed through an investigation.

The wide variation in anonymized threats that target K-12 schools requires a deliberate and measured approach to response so that school communities remain safe and so that disruption and trauma is minimized. As described in the previous section of this toolkit, initial response actions increase safety while limiting effects on students and staff. For threats that pose elevated levels of concern, however, additional and more intense response actions may be necessary. This section builds on the foundation set out in [Section 4](#) to describe the broad menu of options available to schools and their partners when it comes to heightening a response all while emphasizing the ongoing connection between response actions and threat evaluation processes (which will inform response decisions) and sustained communication throughout (and after) a threat situation (Figure 5.1).

Figure 5.1 The Evolution of Action Streams Throughout Response to Anonymized Threats



SOURCE: HSOAC analysis.

## // 5.1 Options Available to Schools to Heighten Response to Anonymized Threats

There is no single, right answer when it comes to responding to anonymized threats. Local expectations, concerns and needs will necessarily shape any initial and subsequent response to a threat. Schools should keep in mind that they have a range of options available to them as well as the option to add or reduce options over the course of the investigation process. Liaising with law enforcement partners upon notification of a threat is a key first step to ensure a balanced and appropriate response. Communicating early with local law enforcement can help determine key steps in the response process, including:

- Which assets need to be on scene to ensure a school campus is safe,
- What safety steps or response options are required to slow down the threat emergency,
- What options exist to scale up a response,
- Roles for school staff and local law enforcement personnel in the response process, and
- Who will be in charge of the response.

## Plan for Response

In addition to considering how a law enforcement presence can help keep the school community safe during an emergency, local education agencies will also need to consider additional safety steps to keep their buildings and campus safe. The “I Love U Guys” Foundation’s Standard Response Protocol (SRP) seeks to promote uniform responses to a wide range of emergencies impacting K-12 schools (“I Love U Guys” Foundation, 2022). It emphasizes five specific actions to help ensure safety:

**HOLD:** “In Your Room or Area, Clear the Halls” (used when hallways need to be cleared of occupants);

**SECURE:** “Get Inside, Lock Outside Doors” (used to safeguard individuals inside the school building);

**LOCKDOWN:** “Locks, Lights, Out of Sight” (used to secure individual rooms inside the school and keep occupants quiet and in place);

**EVACUATE:** Should be followed by a specific location (used to move people from one location to another either inside or outside the school building); and

**SHELTER:** Should be followed by the specific hazard and associated safety strategy (used to protect the group or self from a hazard).

These actions should all be specified in school-wide emergency operations plans (EOPs), as highlighted in [Section 6](#) of this toolkit. As threat emergencies evolve and school staff and their law enforcement partners gather more information, response actions can be sequenced or scaled down as necessary (“I Love U Guys” Foundation, 2022).

## Consider a phased approach to law enforcement and other security responses to reduce trauma and disruption

Whether in reference to a heightened law enforcement presence on campus or to the various action-based options referenced by the “I Love U Guys” Foundation SRP, options for responding to anonymous threats can be varied along two key dimensions. This two-pronged approach provides decisionmakers with options to manage risk to their school community: the intensity and overtness of the response, both of which impact the risks and costs that local education agencies seek to manage.

- The intensity of the response – from lower intensity responses, such as increased door checks or adding a plain clothes officer to school grounds to higher intensity responses involving fully locking down inside a threatened school.
- The overtness of the response – from more subtle responses, such as school “lockouts” or “holds” that may have little impact on students or teaching to very overt responses such as uniformed tactical personnel responding to the threatened school.

While high intensity and overt responses allow for the fastest and most effective response to actual threat incidents, they can also be traumatizing to the school community and risk reinforcing incentives for hoax threateners who deliberately try to trigger highly disruptive responses. By contrast, lower

intensity and less overt responses reduce both the potentially traumatic impact of threats and reduce the incentive to stage hoax threats. However, in the case of real threats, they may delay an effective response.

There are a number of lower-intensity, less overt responses for local education agencies to consider. These various responses can often work in parallel. Figures 5.2-5.4 show how three different categories of responses vary in intensity and overtness and the paths that exist for scaling up response.

Actions in response to most kinds of threats can include:

1. Those involving the addition of security personnel (including law enforcement) to school grounds ([Figure 5.2](#));
2. Those focused on restricting movement within the school as well as into and out of school buildings, including different variations of lockdowns ([Figure 5.3](#)); and
3. Those aimed at keeping weapons out of school buildings and grounds ([Figure 5.4](#)).

# VOICES FROM THE FIELD

“[Responding to threats] is essentially a symbiosis: you have to design your physical [safety] protocol to avoid unnecessarily lurching into high gear all the time.”

- K-12 school district-level representative, January 2023

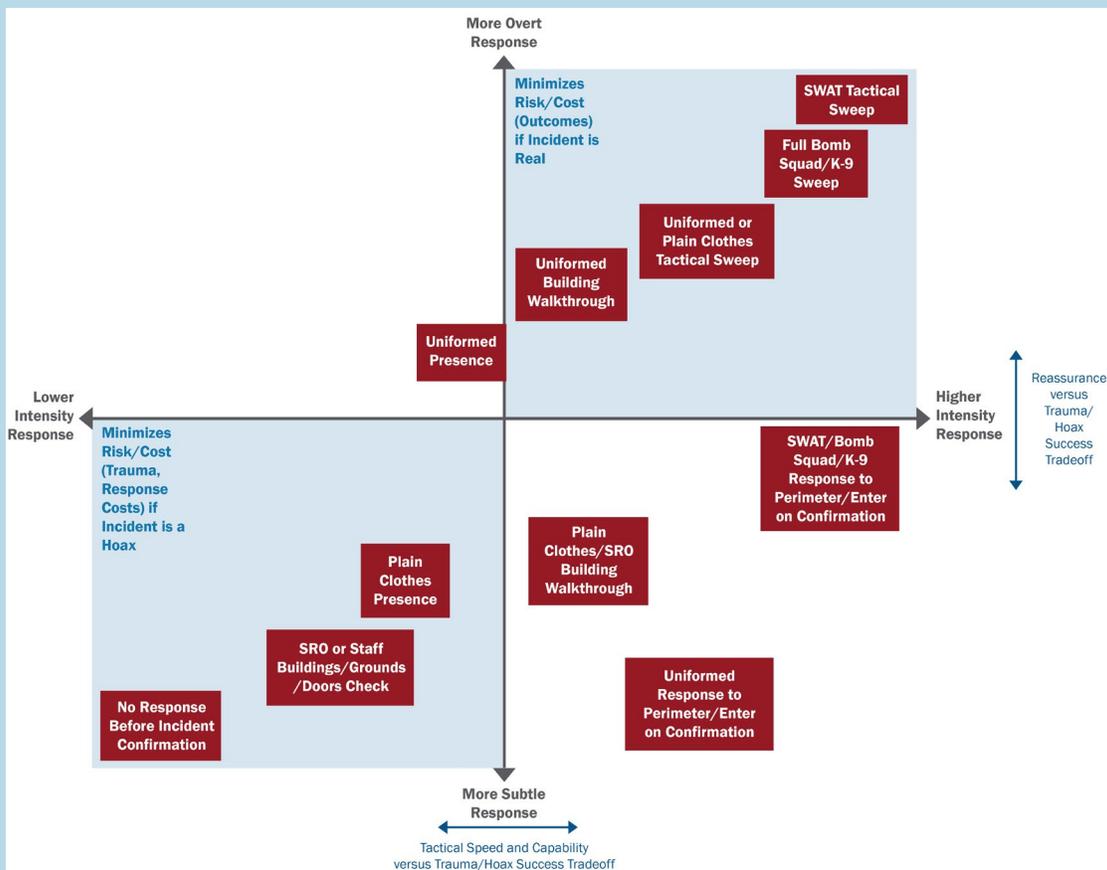
“How [law enforcement] responds matters. Part of [an effective strategy] is having schools lower the temperature of their response but still react sufficiently. When [police] get to a school, the team includes two or three plainclothes officers. So students still only see their SRO at the school and not the other police officers, which might concern them.”

- Law enforcement agency representative, February 2023

## ADDING SECURITY PERSONNEL TO A THREATENED CAMPUS

Increasing police presence at a targeted school is a common initial response to anonymized threats. Lower intensity options in this area include adding anywhere between one and a few plainclothes or uniformed police officers to a school campus. This lower-intensity and lower-profile response can help to reduce the personnel costs associated with responding to a threat, minimize the potentially traumatizing impact of response on the school community and reduce incentives for future hoax threats by maintaining business-as-usual operations.

Figure 5.2 Law Enforcement or Security Personnel Response Options for Threatened Schools



SOURCE: Moore et al., 2024.

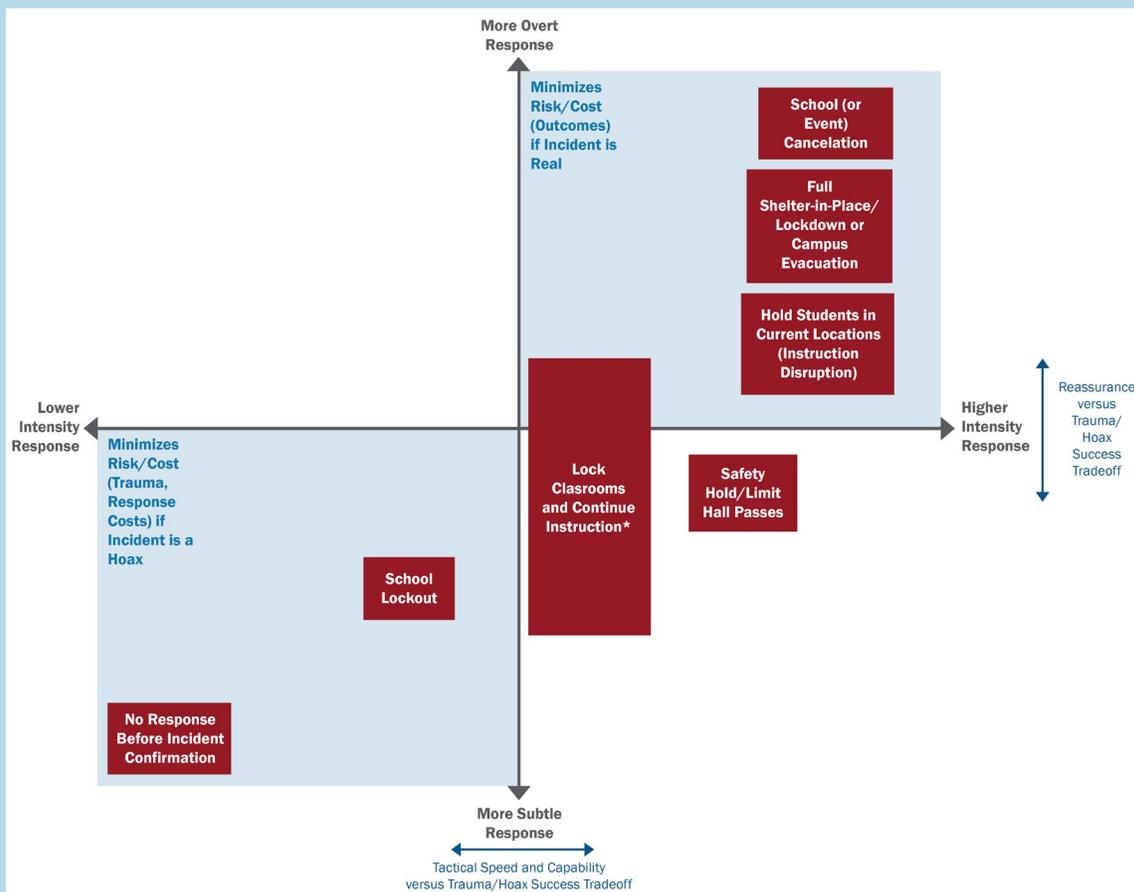
## Example Threat Scenario

A high school added additional police resources in and around campus after reports of an anonymous social media threat of violence against the school. Local police worked with the school to identify the origin of the threat, eventually determining that the threat was not credible and was likely unattributable to a student at the school. Throughout the threat situation, both the school district and local police department issued timely communications to the broader community, specifying that all threats are taken seriously and that making a threat against a school, even as a joke, is a serious crime with consequences. Having determined that the threat was not credible, local police issued the following statement to the community: “We would like to thank the students who saw the post and notified school staff, who then reported it to us. We would encourage all students, parents, and community members to report any threatening messages or suspicious activity they may come across so that our officers can investigate and take appropriate action.”

## RESTRICTING MOVEMENT ON CAMPUS

Early response actions typically also include actions such as implementing secure holds inside the school building, a full lockdown, evacuating students or closing school altogether (Figure 5.3). Some of these actions such as full lockdowns, evacuations and school closures take a heavy toll on students, teachers and the broader school community, in addition to significantly disrupting instruction. Phasing this category of response actions can help to minimize potential negative side effects in the same way as phasing a law enforcement response. As an initial step after receiving a threat, a school might restrict entry onto campus and into school buildings. In this way, instruction can continue inside classrooms as school and law enforcement personnel gather initial information about the threat.

Figure 5.3 Campus Movement Restriction and Closure Options for Threatened Schools



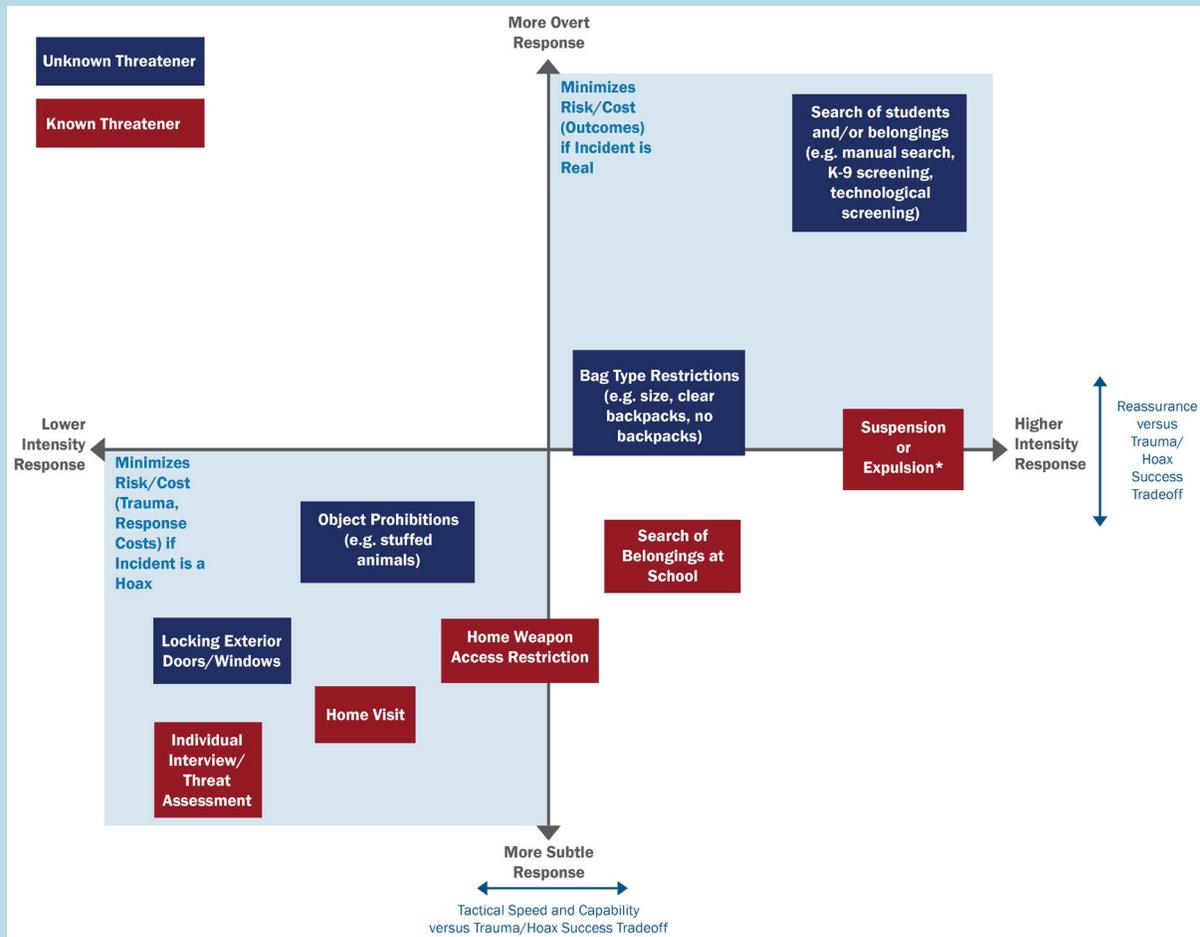
SOURCE: Moore et al., 2024.

\*Note: How overt or subtle locking classrooms and continuing instruction is depends on standard practice for a specific school. For instance, in a school where teachers did not lock classrooms routinely, having them do so could be a somewhat overt action suggesting to students that something was wrong. By contrast, if locking classroom doors was an everyday practice at the school, having a teacher do so in response to a threat would have little to no effect on students.

## PREVENTING WEAPONS FROM ENTERING CAMPUS

Responses to threats can also involve actions designed to keep weapons or armed individuals out of school buildings (Figure 5.4). These actions differ significantly depending on whether the identity of the threatening individual is known or the threat is anonymous. The least overt and intense options in this area focus on the school's physical perimeter, making sure that gates and doors that are supposed to be locked are indeed closed and secured. Intermediate options can include restricting individuals from bringing specific items that could conceal weapons into school buildings (e.g. stuffed animals, certain size backpacks, or requiring that students use transparent backpacks). Even more intense and overt options include searching students and their belongings as they enter school or using metal detectors or wands. Searches can cause disruption to teaching and learning, given the time and staff required to conduct them, especially in large schools.

Figure 5.4 Options for Preventing Weapons on Campus in Threatened Schools



SOURCE: Moore et al., 2024.

\*Note: In addition to school discipline measures that could remove a threatening student, criminal justice action might also be taken. In the event of an identified adult threatening a school, those actions would be primary, though the adult would also likely be banned from entry to the school.

## Use a Specific Protocol to Organize and Escalate Responses to Threats

As noted in [Section 3](#) of this toolkit, coordination between school and law enforcement personnel is key to appropriately responding to threats. All partners should be aware of the specific response protocol used in threat situations and of the options for escalating response options if new information adds weight to a threat. While low intensity, less overt response actions may reduce some negative impacts on students and staff, schools should have processes in place that allow for rapid scaling up of response efforts to reduce risk in the event of an actual incident. Processes that enable quick, on-scene information gathering at the targeted school (e.g. by an SRO or other designated school staff member) and relaying relevant, up-to-date information to law enforcement are necessary to enable quickly scaling up a threat response. Practicing these components of responding to a more complex emergency could be integrated into annual drills and exercises that many schools are already required to carry out, ensuring that all parties needing to collaborate in a response are on the same page.

Using common vocabulary or common language when coordinating and communicating about response is also critical to ensuring an efficient response. As noted in the “I Love U Guys” Foundation SRP, standard vocabulary ensures that all stakeholders understand the response to and status of the threat emergency and adds an element of predictability to what can otherwise be a chaotic situation (“I Love U Guys” Foundation, 2022). Specific terms included in a school response protocol should link to specific actions: active participants to the response—students, teachers, others in the school building—should know what actions are to be performed when they hear specific terms.

### AVOIDING COMPLACENCY IN ADDRESSING THREATS

School safety experts and school-based personnel have noted that the overwhelming number of threats targeting K-12 schools across the country have, in some cases, contributed to increased complacency when it comes to responding to threats. The repeated use of lockdowns or school cancellations as a blanket response can become repetitive and reduce staff readiness in the event of real emergencies. Local education agencies, therefore, need to stay aware of the potential for complacency among staff and students alike if they are the target of repeat threats.

## // 5.2 Ongoing Threat Evaluation to Inform Response Changes

How do local education agencies decide whether initial responses are sufficient or whether they need to be supplemented with more significant resources? Conversely, when can they relax response measures? Throughout the process of triaging anonymous threats, school personnel should always engage law enforcement partners. SROs, school police officers, local police and other law enforcement personnel are trained to identify priority information that can help triage threats and assess the level of concern that they pose to a school community. Their expertise is critical to managing threat situations and helping schools make decisions around when response actions need to be scaled up or down.

Other partners may also be necessary, as highlighted in [Section 3](#) of this toolkit. Fusion centers can provide valuable information about other threats affecting K-12 schools (past and present, and within and outside the state). Social media companies can provide the posting histories of specific accounts, internet protocol (IP) addresses to help identify the origin of the post and other valuable information when threats are posted to social media. School-based and other mental health professionals, including those serving on behavioral threat assessment teams, are also key players in the triage

process, especially if and when the identity of the threatening individual is made known. In general, having multiple parties representing diverse disciplines involved in the threat triage process will lead to a more robust, actionable and defensible evaluation of the situation at hand (Simons and Tunkel, 2021).

This ongoing threat assessment effort continues the process described in [Section 4](#), seeking out new information and data that either could increase or decrease the perceived credibility and level of concern about a threat. If the threat assessment effort ends up uncovering the identity behind an otherwise anonymous threat (or determining the location from which the threat was made), it may quickly increase certainty around the possibility of resolving that threat. In such instances, schools and their law enforcement partners may decide to halt response efforts. In more complex cases, additional information obtained during the assessment process could guide choices over whether to move up or down the spectrum of response options shown in Figures 5.2-5.4. New information suggesting that a threat poses more concern than originally believed could call for more overt and intensive response actions, even at the cost of disrupting school operations or activities.

## VOICES FROM THE FIELD

**“Keep eyes and ears open, and share information with key partners. Sitting in a room together with partners is so critical. Partners from different disciplines need to be together to understand what each can offer.”**

*- Representative from county-level criminal justice agency, February 2023*

## VOICES FROM THE FIELD

“Involving LE [law enforcement], especially when you don’t know who’s making the threat, is important.”

- County-level criminal justice agency representative, February 2023

### // 5.3 Communication as the Threat is Resolved and Beyond

Communication with the school community will remain critical until the threat situation is resolved and in the aftermath of threat situations. As school-based law enforcement and other experts work to evaluate the level of concern that a threat poses and adjust response actions as appropriate, school and district leaders should make sure that they continue to disseminate timely and accurate information about what is happening. As noted in [Section 4](#), specific details about crisis intervention measures, available resources (such as mental health resources), delays, evacuations, closures and family reunification plans can be critical to minimizing further trauma and panic. Once the threat is resolved, send an “all clear” to the community informing them that the issue has been resolved and detailing what next steps will look like. At that point, messages to the community can specify the dates, times and locations of any face-to-face community meetings about the situation as well as details about school reopening procedures and where to find additional resources. Communications from school officials can also provide detail about any other school outreach efforts to address the threat situation as well as information about how the school is recovering from the incident. For more information about what to include in community-wide communications as a threat situation is being resolved as well as in the aftermath of such situations, see NASP’s resource, [Using Social Media Before, During, and After School Crises](#).

# Preparedness to Enhance Schools' Capabilities to Manage Anonymized Threats

Schools can take steps throughout the school year to better prepare themselves for a wide array of emergencies, including anonymized threats. This section discusses how developing emergency operations plans (EOPs) and protocols for communicating with families, holding regular drills and training exercises, and ensuring access to critical resources can minimize the impacts of threats when they do occur.

K-12 schools can take steps throughout the school year to better prepare themselves in case they do become the target of an anonymized threat. Successful response during an emergency begins with ongoing preparedness and prevention efforts outside of emergencies. In many respects, various preparedness efforts help to set expectations across an entire school community about what will happen if and when the school is faced with a threat. These efforts can help alleviate some of the additional stress that threat incidents often induce.

Anonymized threats are not the only types of threats or safety concerns schools must prepare to address. A key to knowing what to do when a school becomes the target of an anonymized threat is being prepared to address a wide range of emergencies. In this regard, well-developed Emergency Action Plans (EAPs) or EOPs are critical. This section focuses on four components of emergency response:

- Establishing a response protocol that addresses threat situations,
- Conducting age- and developmentally appropriate drills and training exercises to help prepare for responding to threats,
- Establishing protocols for communicating with families before and during a threat situation, and
- Preplanning access to resources critical to addressing the impacts of threats.

## Box 6.1 Emergency Operations Plans Resources for K-12 Schools

Various resources at the federal government level exist to help schools develop comprehensive and effective EOPs or EAPs:

The U.S. Department of Education-sponsored REMS TA Center maintains a suite of interactive tools to help diverse stakeholders, including K-12 schools and school districts, develop such plans, conduct site assessments, revise their plans, improve their capabilities and engage in learning opportunities so that emergency planning practices align with those at the national, state and local levels. The tools are intended for use by school and district-level staff with any level of experience in emergency management. The full suite of tools listed below can be accessed at the [REMS TA Center's EOP Interactive Tools webpage](#):

- Site Assess
- EOP Assist
- EOP Assess
- EOP Assist Interactive Workbook
- EOP Evaluate

The U.S. Department of Education, Federal Emergency Management Agency (FEMA), Department of Justice, FBI, and Department of Health and Human Services also published the comprehensive [Guide for Developing High-Quality School Emergency Operations Plans](#). The resource intends to guide school- and school district-based planning teams in their efforts to develop and revise school EOPs and provides information and guidance on the following topics:

- The principles of school emergency management planning;
- Developing, implementing and continuously refining a school EOP with community partners;
- The form, function and content of EOPs; and
- Areas that support emergency planning, such as addressing an active shooter emergency, the importance of school climate, psychological first aid and information sharing.

A companion product, [The Role of Districts in Developing High-Quality School Emergency Operations Plans](#), specifies roles and responsibilities for school district-level administrators and staff, including coordinating with schools and community partners to make EOPs a collaborative effort, providing planning parameters for use across all district-wide schools, and supporting schools at each step as they develop and revise EOPs.

## // 6.1 Establish a Threat Response Protocol for Addressing Anonymized Threats

Deciding on how to respond to a threat when its source and credibility are uncertain can be very challenging. While keeping the school community safe is of utmost importance, treating every threat as an incident in progress with full tactical response will both traumatize students and staff and rapidly become untenable if threats are frequent. Instead, local education agencies should maintain response plans and threat protocols outside of threat situations to prepare decisionmakers to deal with uncertainty. Such protocols lay the groundwork needed for a school and their key partners to assess and respond quickly to threats when they arise.

This groundwork should include response plans that give decisionmakers a range of options for responding to anonymized threats. As discussed in detail in [Sections 4 and 5](#) of this toolkit, responses to anonymous threats often involve tough risk decisions. Having a range of protective actions to choose from that represent different levels of intensity and overtness can help school leaders act more quickly and effectively. Developing and building consensus about different response options must be done as part of planning well before a threat is received. This planning process needs to identify common terminology for response options—e.g. what specifically is meant when the term “lockdown” is used and what terms indicate different levels or intensities of law enforcement response to the targeted school? Planning should also build consensus around what should prompt scaling up a response as new information about a threat develops. Establishing common terminology is also important to ensure that partners from different disciplines can communicate clearly under pressure. It will also reduce the potential for confusion to hinder an effective and efficient response. The U.S. Department of Education’s REMS TA Center provides several sample annexes to support emergency management planning before, during and after incidents (see e.g. [Lockdown Sample Annex: A Fictional Example for Schools Before, During, and After a Lockdown](#)).

## VOICES FROM THE FIELD

**“The first step [in ensuring preparedness] is to identify key partners. Local law enforcement, fusion centers, other agencies are key. These partners bring additional resources [to schools]. Schools need to bring these people together and be on the same page as them. There can’t be silos.”**

*- County-level criminal justice agency representative, February 2023*

Local education agencies should build their threat response protocols with input from their key threat response partners. Elements of the response protocol will include key team contacts at the school and in the broader community (e.g. superintendent, principal, SRO, municipal law enforcement representative, school board member); a list of first steps to take when the school is notified of a threat; role assignments specifying who will lead communication during the incident and have control over next steps (e.g. school security officer, local law enforcement); and other key details, such as identifying designated areas for evacuations. Training on school-specific response protocols will be critical to familiarizing school and district staff as well as key partners with common threat response terminology (e.g. “hold” vs “lock-down”) and logistics prior to an actual incident (Moore et al., 2024). Making these contacts and standing up a response to a threat could be practiced as part of other required emergency exercises or drills that schools carry out during the year.

Efforts to build relationships with key partners are necessary to assess and respond to threats. Assessing the level of urgency and credibility of a threat may require expertise from many different fields, including school professionals, counselors, mental health providers, law enforcement, and other sources of knowledge and capability. Discussed in greater depth in [Section 3](#), these relationships should be put in place long before a school is the target of a threat so that it is not struggling to determine who to connect with and how to get assistance during an actual threat emergency. Establishing trusting partnerships between local

education agencies and local law enforcement agencies is key to enabling measured responses to social media threats ([Guidance from the Department of Justice Community Oriented Policing Services \[COPS\], Newman, 2011](#)). Some partners, including federal law enforcement organizations or fusion centers, can provide additional key capabilities that can aid in assessing the level of concern that a threat poses. Ensuring quick access to these types of capabilities will depend on preexisting relationships and communication paths between the local education agency and law enforcement. Outlining processes for sharing information across local, state and federal law enforcement partners can also ensure quick access to relevant information, such as whether other schools or districts received similar threats.

Finally, because threats can target schools at any time of day or night, including outside of school hours, connections between school leaders and outside experts from law enforcement, fusion centers and other disciplines need be available 24/7. When a school is notified of a threat late at night, for instance, decision-making about how to respond must occur before the start of the next school day. Discussion cannot wait until normal business hours. School personnel who are notified of a threat need to be able to rapidly connect with their law enforcement contacts as well as other experts as necessary and vice versa so that when a threat needs to be weighed, it can be done quickly. For many schools, existing threat assessment teams that evaluate threats made directly by students (i.e. where the threatener is known rather than anonymous) will provide these links and also be the avenue for assessing anonymous threats.

## // 6.2 Engage in Training and Drills Covering Different Options for Threat Response

Repeated practice and drills over what to do during an incident, such as an active shooter event, can help school communities improve their readiness when it comes to responding to an actual threat. Exercises and drills can also be a part of preparing the school community—particularly leadership, threat assessors and partners like law enforcement—to respond to anonymized threats. Depending on the nature of a threat and as discussed in [Section 5](#) of this toolkit, responses to a threat can range from options largely unnoticeable to students (e.g. a modest

increase in police presence at a school) to much more overt actions like bag searches at school entrances. Though drills and exercises often focus on full responses to actual confirmed incidents, practice across the full range of response options can also help schools enhance their preparedness. For example, a drill convening decisionmakers to assess an uncertain threat where the response defined in the school’s emergency operations plan is more limited will have little or no impact on students, even if it is held during a school day.

Including drills across the full range of response options can also limit the potential for preparedness efforts, particularly realistic incident response exercises, to cause trauma for students and staff (Mascia, 2022; Schildkraut and Nickerson, 2022). [The National Association of School Resource Officers \(NASRO\), NASP, and Safe and Sound Schools](#) developed best practices guidance to support local education agencies in planning drills in a way that minimizes impacts on students and staff as well as disruptions to teaching and learning (NASP, NASRO, and Safe and Sound Schools, 2021). For example, NASP and NASRO and others recommend non-sensorial drills, avoiding simulation-like exercises, and integrating sequenced practice activities, such as

developmentally appropriate discussion exercises, before initiating more complex drills (NASP, NASRO, and Safe and Sound Schools, 2021; Schildkraut and Nickerson, 2022). Utilizing these trauma-informed practices can help to avoid the potential adverse impacts of response exercises.

In addition to drills, integrating less intense actions, such as soft lockdowns (e.g. locking classroom doors) or uniformed law enforcement responses to nonviolent events (e.g. medical emergencies), can help to familiarize students to certain measures, which may reduce the extent to which responses to actual threats induce trauma.

## // 6.3 Inform Families of Basic Threat Response Plans and Prepare to Communicate with the School Community When Threats Occur

While local education agencies should not share exact details of their response protocols with families for security reasons, communicating what a response operation may look like before a situation occurs can help enhance preparedness among families and students (Perez, 2022; Witsil, 2022). Such efforts can also familiarize the whole school community with the range of options schools will be drawing from depending on the nature of a threat. For example, several states and large school districts post standard response protocols to their websites and also send copies home so that children and parents can talk about readiness at home (e.g. [Texas School Safety Center](#), [New York City Public Schools](#)). When a school is the target of a threat, it is common for information and rumors to circulate rapidly across the school community, stoking uncertainty and concern among parents and students about how the school is responding. Transparency with the community about how the school will respond helps build trust and limit concern that a threat is not being taken seriously enough or that the response is

insufficient. Response actions can also flow more smoothly when families know the basics of the response plan, such as who to contact with questions and where to access the most up-to-date information during a threat situation. This early awareness outside of a stressful situation can also help to alleviate some of the panic and chaos that threat situations induce (Blad, 2022).

As noted in [Sections 4 and 5](#) of this toolkit, a key practice for supporting threat response is communicating effectively and promptly with families during and after a threat incident. Local education agencies should prepare protocols for how and when communication with families will occur during a threat emergency, what information to disseminate, and who will disseminate it. Message templates can be part of emergency response planning documents. Refer back to [Sections 4 and 5](#) to see what kind of information is critical to include in messages to the community during a threat emergency.

## // 6.4 Prepare to Provide Support Resources to Address the Impacts of Threats

An important part of preparedness efforts is planning for what happens *after* a threatening incident is resolved and the school community is expected to return to normal. While the need for post-incident support is well recognized in the aftermath of actual violent incidents, multiple actions that take place in response to a threat (e.g. lockdowns, increased police presence, evacuation) in addition to the threat itself can have negative impacts on students and staff (Rich & Cox, 2018; Perez, 2022; Kentucky Center for School Safety, n.d.; Yechivi, 2022). As a result, planning for post-incident support should be a component of preparedness efforts designed to address instances when a school is the target of a threat but not necessarily an act of violence.

Local education agencies need to be prepared to provide mental health resources and other forms of assistance to students and staff in the wake of a threat (Rich & Cox,

2018; Perez, 2022). [The National Association of Secondary School Principals \(NASSP\) Principal Recovery Network Guide to Recovery](#) suggests that local education agencies build relationships with local mental health organizations, community therapists and mental health counselors prior to an incident occurring. Teachers should also be provided guidance on how to transition back to instruction after a threat incident. In addition to these supports, the NASSP Principal Recovery Network (2022) also stresses the importance of setting up a structure that allows multiple opportunities for students to voice their needs and opinions. For example, practices may include forming student groups and committees, designating time for students to talk with classmates and friends in addition to mental health professionals, and giving students the opportunity to provide feedback on threat emergencies via discussion sessions or anonymous surveys (NASSP Principal Recovery Network, 2022).

## // 6.5 Conclusion

Threats made to schools are an increasing problem and significantly disrupt school operations and traumatize school communities. Drawing on the expertise of educators, law enforcement and other experts from across the country, this toolkit seeks to provide schools with information to both protect school communities and limit the disruption and trauma that can be caused by such threats. By providing options to respond to threats in a scaled way and guidance to shape decision-making about the urgency and credibility of individual threats, readiness efforts can help prepare school and public safety leaders to effectively balance the full range of risks faced by schools in an era of all-too-common school violence.

# Additional Resources

## // Threat Assessment

Cornell, Dewey G., and Jennifer Maeng. Student Threat Assessment as a Safe and Supportive Prevention Strategy, Final Technical Report. Charlottesville, VA: Curry School of Education, University of Virginia, 2020. As of April 26, 2022: <https://www.ojp.gov/pdffiles1/nij/grants/255102.pdf>

Meloy, J. Reid, and Jens Hoffman. International Handbook of Threat Assessment. Second Edition. New York: Oxford University Press, 2021.

United States Department of Education, Readiness and Emergency Management for Schools Technical Assistance (REMS TA) Center. School Behavioral Threat Assessments: An Introduction. Available at: [https://rems.ed.gov/Docs/Threat\\_Assessment\\_Website\\_Marketing\\_Flyer\\_508C.pdf](https://rems.ed.gov/Docs/Threat_Assessment_Website_Marketing_Flyer_508C.pdf)

Van Brunt, Brian, W. Scott Lewis, and Jeffrey H. Solomon. An Educator's Guide to Assessing Threats in Student Writing: Social Media, Email, and other Narrative, 2020. Routledge. Available at: <https://doi.org/10.4324/9781003001096>

## // Preparedness and Prevention

Cybersecurity and Infrastructure Security Agency (CISA). "Bombing Prevention." webpage. n.d. Available at: <https://www.cisa.gov/topics/physical-security/bombing-prevention>

Dwyer, K., and David Osher. "Safeguarding Our Children: An Action Guide." Washington, D.C.: U.S. Departments of Education and Justice, American Institutes for Research, 2020. As of April 26, 2022: [https://www2.ed.gov/admins/lead/safety/actguide/action\\_guide.pdf](https://www2.ed.gov/admins/lead/safety/actguide/action_guide.pdf)

International Association of Chiefs of Police. School-Police Partnerships. June 2020. As of August 4, 2023: <https://www.theiacp.org/sites/default/files/2020-07/School-Police%20Policy%20-%20FULL%2007092020.pdf>

National Association of School Psychologists (NASP), National Association of School Resource Officers (NASRO), and Safe and Sound Schools. Best Practice Considerations for Armed Assailant Drills in Schools. April 2021. As of April 13, 2023: <https://www.nasponline.org/Documents/Research%20and%20Policy/Advocacy%20Resources/Armed-Assailant-Guide-FINAL.pdf>

National Association of School Resource Officers (NASRO), and Safe and Sound Schools, "Surge in School 'Swatting' Calls Considerations for School Resource Officers," September 2022. As of April 28, 2023: <https://www.nasro.org/news/2022/09/26/news-releases/surge-in-school-swatting-calls-considerations-for-school-resource-officers/>

## // Reporting Tools

Carlton, Mary Poulin, "School Safety: Research on Gathering Tips and Addressing Threats," NIJ Journal, Vol. 283 (2021). Available at: <https://www.ojp.gov/pdffiles1/nij/300306.pdf>

Cybersecurity and Infrastructure Security Agency (CISA) and National Threat Assessment Center (NTAC). Improving School Safety Through Bystander Reporting: A Toolkit for Strengthening K-12 Reporting Programs. 2023. As of June 8, 2023: [https://www.cisa.gov/sites/default/files/2023-05/CISA-USSS%20K-12%20Bystander%20Reporting%20Toolkit\\_508.pdf](https://www.cisa.gov/sites/default/files/2023-05/CISA-USSS%20K-12%20Bystander%20Reporting%20Toolkit_508.pdf)

Planty, M., Cutbush, S., Banks, D., and D’Arcangelo, D. School Safety Tip Line Toolkit. Research Triangle Park, NC: RTI International, 2021. Available at: <https://www.rti.org/publication/school-safety-tip-line-toolkit/fulltext.pdf>

U.S. Department of Justice, Federal Bureau of Investigation. “Internet Crime Complaint Center (IC3).” webpage. n.d. Available at: <https://www.ic3.gov/>

U.S. Department of Justice, Federal Bureau of Investigation. “Electronic Tip Form.” webpage. n.d. Available at: <https://tips.fbi.gov/home>

U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division. “Swatting VCC Information.” webpage. n.d. Available at: <https://rocic.riss.net/wp-content/uploads/2023/07/FBI-NCOP-VCC-Swatting.pdf>

Schoolsafety.gov. “Threat Assessment and Reporting.” webpage. n.d. Available at: <https://www.schoolsafety.gov/threat-assessment-and-reporting>

## // Responding to School Threats

Cornell, Dewey G. "Guidelines for responding to student threats of violence." Journal of Educational Administration, Vol. 41, 2003, pp. 705-719.

Cybersecurity and Infrastructure Security Agency. Social Media Threat Guidance for School Staff and Authorities Infographic. December 14, 2023. As of May 20, 2024: <https://www.cisa.gov/resources-tools/resources/social-media-threat-guidance-school-staff-and-authorities-infographic>

“I Love U Guys” Foundation. The Standard Response Protocol, K12 Schools and Districts v4.1. June 15, 2022. As of May 2, 2023: <https://iloveuguy.org/downloads/SRP-K12-2023-Operational-Guidance.pdf>

Washington Office of Superintendent of Public Instruction. “Swatting: Mitigation Strategies and Reporting Procedures.” webpage, n.d.. As of July 30, 2024: <https://ospi.k12.wa.us/sites/default/files/2023-08/swatting-resources.pdf>

Newman, Graeme. R. Bomb Threats in Schools. U.S. Department of Justice, Problem-Oriented Guides for Police: Problem-Specific Guides Series Guide, No. 32, August 2011. As of April 28, 2023: <https://www.popcenter.org/sites/default/files/problems/PDFs/BombThreats.pdf>

Maine Department of Education, “Anonymous threats, swatting, and more,” webpage, n.d.. As of July 20, 2023: <https://www.maine.gov/doe/safety/threatassessmentlinks>

Vermont School Safety Center. “Communication Resources for School Swatting Calls.” webpage, n.d.. As of July 20, 2023: <https://schoolsafety.vermont.gov/news/communication-resources-school-swatting-calls>

# Taking Stock of Anonymized Threats at Your School

Addressing anonymized threats is a dynamic, multiphase process that includes becoming aware of a threat, assessing the level of concern that it poses, deciding on an appropriate response, keeping the community up to date and establishing partnerships. Steps to heighten resilience to threats, such as preparedness efforts and activities centered on threat detection and deterrence, are also a critical part of the process. Think about the following questions to assess current trends in anonymized threats in your school or district.

**1**

Has your school/district and/or an individual in your school community been the target of threatening, anonymous communications?

**2**

How has your school/district become aware of anonymous and other threats?

**3**

Have you learned of potential threats from your district's technology scanning software?

**4**

Have students or other members of the school community reposted or shared anonymized threats (e.g. on their own social media accounts/pages) to warn others of a potential threat?

**5**

Have anonymized threats been primarily assessed as hoaxes or as authentic?

**6**

Have students in your school/district made anonymized threats using social media or other mediums? Have individuals from outside your immediate school community targeted your school or district with threats, anonymously or otherwise?

**7**

Has your school or district experienced disruptions to the school day due to an anonymized threat? (e.g. delayed arrival or dismissal, paused classes to conduct a search, closed school or canceled events, etc.)

**8**

Have families kept their children out of school due to an anonymized threat? Are you able to confirm the intent as opposed to general truancy?

**9**

How do you communicate with families and the broader school community when your school/district is the target of a threat?

**10**

What outreach or education efforts does your school/district have in place to warn students and others about dangerous or threatening activity they might encounter online and on social media?

# Gathering Information When You Receive a Threat: Where to Start?

What partners have you engaged after receiving notification that your school is the target of an anonymized or other threat?

Who is your primary law enforcement contact? Can they facilitate a connection to a recognized fusion center in your state?

What other partners are you reaching out to?

If the anonymized threat was made on social media, can you trace the original internet protocol (IP) address where the threat was made?

Law enforcement partners and sometimes social media companies can help.

If the IP address is outside your local area or outside the country, the threat may be less concerning.

If the anonymized threat came in over the phone, was the caller's number visible or blocked, and was the caller able to answer follow-up questions about the supposed incident or local area?

Blocked, unavailable, or otherwise spoofed numbers (e.g. all nines or zeros) are often indicators of swatting calls.

If a caller is unable to answer follow-up questions about an incident, such as their full name, phone number or current location (or mispronounces names of local streets or buildings), this could be an indication of a swatting call.

Reach out to law enforcement partners with as much detail about the caller/call as possible and coordinate an appropriate response.

If the anonymized threat came in over the phone, was the caller's number visible or blocked, and was the caller able to answer follow-up questions about the supposed incident or local area?

Connecting with other schools or districts in your area or across your state can also help you assess whether the call is a hoax that is also targeting other locales.

What images, photos and/or language does the anonymized threat include? Are these original to the threat or reused from other threats (past or present)?

Reverse image searches can help identify readily available stock photos from the internet, suggesting the threat may be less concerning.

Reach out to local, state or other law enforcement partners to see if they maintain a database of past or ongoing threats. They can help you determine whether material from an anonymized threat has been recycled.

Reach out to neighboring schools or school districts to ask whether they have also received threats. Those that come in clusters are often less concerning than one-off, unique threats.

Visuals that suggest the threatener is in close proximity to your school (e.g. photos or videos of school events as they are underway) increase the urgency of threats.

What trends are developing around the anonymized threat?

If the threat was posted to social media, who has "liked" the post? Who (e.g. which students) follows the threatening account?

Do the likes or connections to the post help you narrow down the potential source of the threat?

**What trends are developing around the anonymized threat?**

**Reach out to students who might know something about the post.**

**Has local media reported on the threat?**

**Communicate appropriate information about the threat to the school community.**

**Have mental health supports on hand and available to school community members.**

# Abbreviations

ACRONYM	Full Form
CISA	Cybersecurity and Infrastructure Security Agency
COPS	Community Oriented Policing Services
DHS	U.S. Department of Homeland Security
EAP	Emergency Action Plan
EOP	Emergency Operations Plan
FBI	Federal Bureau of Investigation
IP	internet protocol
K-12	kindergarten through grade 12
NASP	National Association of School Psychologists
NASRO	National Association of School Resource Officers
NTAC	National Threat Assessment Center
NYCPS	New York City Public Schools
REMS TA	Readiness and Emergency Management for Schools Technical Assistance Center
SRO	School Resource Officer

# References

- Amman, M., Bowlin, M., Buckles, L., Burton, K. C., Brunell, K. F., Gibson, K. A., Robins, C. J. Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks. Washington, DC: U.S. Department of Justice, 2017. As of April 26, 2022: <https://www.fbi.gov/file-repository/making-prevention-a-reality.pdf>
- Balsamo, Michael. "Threats to schools across U.S. may be coming from overseas." The Associated Press, November 14, 2022. As of June 14, 2023: <https://apnews.com/article/shootings-race-and-ethnicity-government-politics-cea91facd-dabed823513f205073a441f>
- Blad, Evie. "'Swatting' Hoaxes Disrupt Schools Across the Country. What Educators Need to Know." Education Week, September 21, 2022. As of May 2, 2023: <https://www.edweek.org/leadership/swatting-hoaxes-disrupt-schools-nationwide-what-educators-need-to-know/2022/09>
- Case, Angela. "Swatting calls came into Colorado schools in alphabetical order." 9News, February 22, 2023. As of March 21, 2023: <https://www.9news.com/article/news/crime/colorado-high-school-lock-downs/73-3981a7dc-b1fc-45f3-9edf-8e7a46eb3f29>
- Chabria, Anita. "Column: A school threat. Do you send your child or keep them home?" The Los Angeles Times, February 16, 2023. As of March 21, 2023: <https://www.latimes.com/california/story/2023-02-16/column-a-credible-threat-to-a-school-five-years-after-parkland>
- Cornell, Dewey G., and Jennifer Maeng. Student Threat Assessment as a Safe and Supportive Prevention Strategy, Final Technical Report. Charlottesville, VA: Curry School of Education, University of Virginia, 2020. As of April 26, 2022: <https://nij.ojp.gov/library/publications/student-threat-assessment-safe-and-supportive-prevention-strategy-final>
- Cybersecurity and Infrastructure Security Agency (CISA), "Bomb Threat Checklist," n.d. As of April 9, 2024: <https://www.cisa.gov/resources-tools/resources/bomb-threat-checklist>
- Cybersecurity and Infrastructure Security Agency (CISA) and National Threat Assessment Center (NTAC). Improving School Safety Through Bystander Reporting: A Toolkit for Strengthening K-12 Reporting Programs. 2023. As of June 8, 2023: [https://www.cisa.gov/sites/default/files/2023-05/CISA-USSS%20K-12%20Bystander%20Reporting%20Toolkit\\_508.pdf](https://www.cisa.gov/sites/default/files/2023-05/CISA-USSS%20K-12%20Bystander%20Reporting%20Toolkit_508.pdf)
- Federal Bureau of Investigation (FBI). "Think Before You Post: Hoax Threats are Serious Federal Crimes." October 5, 2018. As of May 2, 2023: <https://www.fbi.gov/news/stories/hoax-threats-awareness-100518>
- Glass, Sloane. "Why 'swatting' calls to U.S. schools are becoming a big concern." The Hill, March 30, 2023. As of August 15, 2023: <https://thehill.com/blogs/blog-briefing-room/3926322-why-swatting-calls-to-us-schools-are-becoming-a-big-concern/>
- "I Love U Guys" Foundation. The Standard Response Protocol, K12 Schools and Districts v4.1. June 15, 2022. As of May 2, 2023: <https://iloveguys.org/downloads/SRP-K12-2023-Operational-Guidance.pdf>
- Illinois Terrorism Task Force School Safety Working Group. "Communications Tips for School Threats." March 2018. As of July 29, 2024: <https://ilschoolsafety.org/wp-content/uploads/2022/03/Comm-Tips-For-School-Threat.pdf>
- Illinois Terrorism Task Force School Safety Working Group. "Response and Investigative Suggestions for School Threats." March 2018. As of April 12, 2023: <https://ilschoolsafety.org/wp-content/uploads/2022/03/Response-For-School-Threat-ver-2.pdf>
- Jackson, Brian A., Melissa Kay Diliberti, Pauline Moore, and Heather L. Schwartz. Teachers' Views on School Safety: Consensus on Many Security Measures, But Stark Division About Arming Teachers. RAND Corporation, RR-A2641-1, 2023. As of August 4, 2023: [https://www.rand.org/pubs/research\\_reports/RRA2641-1.html](https://www.rand.org/pubs/research_reports/RRA2641-1.html)

- Jojola, Jeremy and Steve Staeger. "Calls reveal swatter threats that caused emergency response to 17 Colorado schools." 9News, February 23, 2023. As of March 21, 2023: <https://www.9news.com/article/news/local/calls-reveal-swatters-threats-caused-emergency-responses-colorado-schools/73-b3df66b2-9284-47ed-950d-4737d5b98d74>
- Keierleber, Mark. "Exclusive Data: An Inside Look at the Spy Tech That Followed Kids Home for Remote Learning—and Now Won't Leave." The 74 Million, September 24, 2021. As of April 6, 2023: <https://www.the74million.org/article/gaggle-spy-tech-minneapolis-students-remote-learning/>
- Kentucky Center for School Safety. Elementary School Lockdown Workbook. n.d. Available at: <https://kycss.org/ns/wp-content/uploads/2022/03/EMP-KCSS-Lockdowns-and-Elementary-Schools-Workbook.pdf>
- Klein, Alyson. "TikTok Challenges Are a Nightmare for Schools. How Should Educators Respond?" Education Week, October 6, 2022. As of August 8, 2023: <https://www.edweek.org/technology/tiktok-challenges-are-a-nightmare-for-schools-how-should-educators-respond/2022/10>
- Mak, Aaron. "The likely truth about the 'National Shoot Up Your Schools Day' TikTok trend." Slate, December 18, 2021. As of July 3, 2023: <https://slate.com/technology/2021/12/tiktok-shoot-up-your-school-trend-evidence.html>
- Mascia, Jennifer. "How lockdown drills can retraumatize kids who have experienced domestic violence," The Trace, October 12, 2022. As of April 7, 2023: <https://www.thetrace.org/2022/10/lockdown-drills-trauma-domestic-violence/>
- Meloy, Reid J., Jens Hoffman, Lynne Bibeau, and Angela Guldiman. "Warning behaviors." in J. Reid Meloy and Jens Hoffman, eds. International Handbook of Threat Assessment, Second Edition, New York, Oxford University Press (2021): pp. 45-67.
- Mitchell, Melanie, and Gavan Palk. "Traversing the space between threats and violence: A review of threat assessment guidelines." Psychiatry, Psychology and Law, Vol. 23, No. 6 (2016): pp. 863-871.
- Monagas, Enrique A., and Carlos E. Monagas. "Prosecuting Threats in the Age of Social Media." Northern Illinois University Law Review, Vol. 36, (2015): p. 57.
- Moore, Pauline, Brian A. Jackson, Jennifer T. Leschitz, Nazia Wolters, Thomas Edward Goode, Melissa Kay Diliberti, and Phoebe Felicia Pham. Developing Practical Responses to Social Media Threats Against K-12 Schools: An Overview of Trends, Challenges, and Current Approaches. Santa Monica, CA: RAND Corporation, April 10, 2024: [https://www.rand.org/pubs/research\\_reports/RRA1077-5.html](https://www.rand.org/pubs/research_reports/RRA1077-5.html)
- Moreschi, Angie. "School Violence Threats on Social Media Becoming Disruptive Trend." 11 News, February 18, 2022. As of May 2, 2023: <https://www.wpxi.com/news/investigates/school-violence-threats-social-media-becoming-disruptive-trend/4f1ac1b9-b379-4478-a49f-573ba1088c5f/>
- Natanson, Hannah and Laura Meckler. "School threats and social media hoaxes are forcing closures, time-consuming investigations." The Washington Post, December 20, 2021. As of June 14, 2023: <https://www.washingtonpost.com/education/2021/12/20/school-threats-oxford-shooting-tiktok/>
- National Association of School Psychologists (NASP). "Social Media and School Crises: Brief Facts and Tips." n.d. As of August 15, 2023: [https://www.nasponline.org/assets/Documents/Resources and Publications/Resources/Crisis/Social Media Crisis\\_Brief\\_FactsTips\\_FINAL.pdf](https://www.nasponline.org/assets/Documents/Resources and Publications/Resources/Crisis/Social Media Crisis_Brief_FactsTips_FINAL.pdf)
- National Association of School Psychologists (NASP), National Association of School Resource Officers (NASRO), and Safe and Sound Schools. Best Practice Considerations for Armed Assailant Drills in Schools. April 2021. As of April 13, 2023: <https://www.nasponline.org/Documents/Research%20and%20Policy/Advocacy%20Resources/Armed-Assailant-Guide-FINAL.pdf>
- National Association of School Resource Officers (NASRO). "Surge in School 'Swatting' Calls Considerations for School Resource Officers." September 26, 2022. As of April 28, 2023, <https://www.nasro.org/news/2022/09/26/news-releases/surge-in-school-swatting-calls-considerations-for-school-resource-officers/>
- National Association of School Secondary Principals (NASSP) Principal Recovery Network. The NASSP Principal Recovery Network Guide to Recovery. August 22, 2022. As of July 12, 2023: <https://www.nassp.org/wp-content/uploads/2022/08/PRN-Guide-FINAL.pdf>

- National Threat Assessment Center (NTAC). Enhancing school safety using a threat assessment model: An operational guide for preventing targeted school violence. U.S. Secret Service, Department of Homeland Security, 2018: [https://www.secret-service.gov/sites/default/files/reports/2020-10/USSS\\_NTAC\\_Enhancing\\_School\\_Safety\\_Guide.pdf](https://www.secret-service.gov/sites/default/files/reports/2020-10/USSS_NTAC_Enhancing_School_Safety_Guide.pdf)
- National Threat Assessment Center (NTAC). Protecting America's Schools: A U.S. Secret Service Analysis of Targeted School Violence. Washington, DC: U.S. Department of Homeland Security, 2019: [https://www.secretservice.gov/sites/default/files/2020-04/Protecting\\_Americas\\_Schools.pdf](https://www.secretservice.gov/sites/default/files/2020-04/Protecting_Americas_Schools.pdf)
- National Threat Assessment Center (NTAC). Averting Targeted School Violence: A U.S. Secret Service Analysis of Plots Against Schools. Washington, DC: U.S. Department of Homeland Security, 2021: <https://www.secretservice.gov/newsroom/reports/threat-assessments/schoolcampus-attacks/details-0>
- New York City Public Schools. "Digital Citizenship." n.d. As of August 4, 2023: <https://www.schools.nyc.gov/school-life/school-environment/digital-citizenship>
- New York City Public Schools. "Emergency Readiness." n.d. As of August 4, 2023: <https://www.schools.nyc.gov/school-life/safe-schools/emergency-readiness>
- Patton, Desmon Upton, Jun Sung Hong, Megan Ranney, Sadiq Patel, Caitlin Kelley, Rob Eschman, and Tyreasa Washington. "Social media as a vector for youth violence: A review of the literature." *Computers in Human Behavior*, Vol. 35 (June 2014): pp. 548-553.
- Perez, Angela Cordoba. "What Phoenix police, districts are doing about recent threats in schools." *Arizona Republic*, September 20, 2022. As of April 28, 2023: <https://www.azcentral.com/story/news/local/arizona-education/2022/09/21/what-phoenix-police-doing-recent-threats-schools/10429127002/>
- Readiness and Emergency Management for Schools Technical Assistance (REMS TA) Center. Use of Social Media in School Behavioral Threat Assessments. n.d. As of July 14, 2023: [https://rems.ed.gov/docs/Social\\_Media\\_Threat\\_Assessment\\_Webinar\\_Slides\\_508C%5B1%5D.pdf](https://rems.ed.gov/docs/Social_Media_Threat_Assessment_Webinar_Slides_508C%5B1%5D.pdf)
- Readiness and Emergency Management for Schools Technical Assistance (REMS TA) Center. Lockdown Sample Annex: A Fictional Example for Schools Before, During, and After a Lockdown. n.d. As of August 18, 2023: [https://rems.ed.gov/docs/LockdownSampleAnnex\\_508c.pdf](https://rems.ed.gov/docs/LockdownSampleAnnex_508c.pdf)
- Regehr, Cheryl, Graham D. Glancy, Andrea Carter, and Lisa Ramshaw. "A comprehensive approach to managing threats of violence on a university or college campus." *International Journal of Law and Psychiatry*, Vol. 54 (2017): pp. 140-147.
- Reynolds, Cristin Lee, R. Eric Platt, Lenore Malone Schaffer, and Holly Foster. "Social media and higher education: the problem of anonymous electronic threats to the campus community." *Journal of Cases in Educational Leadership*, Vol. 20, No. 4 (2017): pp. 58-71.
- Rich, Steven and Cox, John Woodrow. "What if someone was shooting?" *The Washington Post*, December 26, 2018. As of May 2, 2023: <https://www.washingtonpost.com/graphics/2018/local/school-lockdowns-in-america/>
- Safer Schools Together. Basic Digital Threat Assessment Guide. 2019. As of May 2, 2023: <https://saferschoolstogether.com/product/digital-threat-assessment-training/>
- Safer Schools Together. Guidelines for Responding to Digital Threats. n.d. As of April 27, 2023: <https://saferschoolstogether.com/wp-content/uploads/2020/07/GUIDELINES-FOR-RESPONDING-TO-DIGITAL-THREATS.pdf?x89820>
- Safer Schools Together. Raising Digitally Responsible Youth: A Guide for Parents and Caregivers. September 2023. As of August 3, 2023: <https://resources.saferschoolstogether.com/link/352883/>
- Safer Schools Together. Social Media Parents Checklist. n.d. As of August 4, 2023: <https://locker.txssc.txstate.edu/6605488455e53fc500eed949652c46e/Social-Media-Parents-Checklist.pdf>
- Safer Schools Together, Texas School Safety Center, and International Center for Digital Threat Assessment. Texas School Personnel's Guide to Social Media. 2022. As of June 12, 2023: <https://resources.saferschoolstogether.com/view/1040798953/2/>

- Santucci, Jeanine. "Schools across U.S. hit with dozens of false shooting, bomb threats. Experts say it's a 'cruel hoax.'" USA Today, September 18, 2022. As of May 2, 2023: <https://www.usatoday.com/story/news/nation/2022/09/18/fake-school-shooting-threats-us-fbi/10400404002/>
- Schildkraut, Jaclyn and Amanda B. Nickerson, "Effects of lockdown drills on students' fear, perceived risk, and use of avoidance behavior: A quasi-experimental study," *Criminal Justice Policy Review*, Vol. 33, No. 8, 2022, pp. 787-813.
- Simons, Andre and Ronald F. Tunkel, "The assessment of anonymous threatening communications," in J. Reid Meloy and Jens Hoffman, eds., *International Handbook of Threat Assessment*, Second Edition, New York, Oxford University Press, 2021, pp. 235-256.
- Slater, Joanna, "Coordinated 'swatting' effort may be behind hundreds of school shooting hoaxes," *The Washington Post*, October 4, 2023. As of November 20, 2023: <https://www.washingtonpost.com/nation/2023/10/04/school-swatting-hoax-active-shooter/>
- St. George, Donna. "In a crisis, schools are 100,000 mental health staff short." *The Washington Post*, August 31, 2023. As of September 12, 2023: <https://www.washingtonpost.com/education/2023/08/31/mental-health-crisis-students-have-third-therapists-they-need/>
- Stephenson, Cassandra. "Nashville shooting sheds light on how to handle suicide threats, what to expect from police." *The Tennessean*, March 31, 2023. As of April 17, 2023: <https://www.tennessean.com/story/news/2023/03/31/nashville-covenant-school-shooting-sheds-light-on-how-police-handle-suicide-threats/70064308007/>
- Texas School Safety Center. *Standard Response Protocol*. n.d. As of August 15, 2023: <https://txssc.txstate.edu/videos/srp/>
- Trump, Kenneth. "Study finds rapid escalation of violent school threats," *National School Safety and Security Services*, 2016. As of April 28, 2023: <https://www.schoolsecurity.org/2015/02/study-finds-rapid-escalation-violent-school-threats/>
- U.S. Department of Education, Office of Elementary and Secondary Education, Office of Safe and Healthy Students. *Guide for Developing High-Quality School Emergency Operations Plans*. Washington, DC, 2013. As of July 14, 2023: [https://rem.ed.gov/docs/School\\_Guide\\_508C.pdf](https://rem.ed.gov/docs/School_Guide_508C.pdf)
- U.S. Surgeon General's Office. *Social Media and Youth Mental Health: The U.S. Surgeon General's Advisory*. 2023. As of June 8, 2023: <https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf>
- Van Brunt, Brian. "Assessing threat in written communications, social media, and creative writing." *Violence and Gender*, Vol. 3, No. 2 (2016): pp. 78-88.
- Van Brunt, Brian, W. Scott Lewis, and Jeffrey H. Solomon. *An Educator's Guide to Assessing Threats in Student Writing: Social Media, Email, and other Narrative*. 2020, Routledge. Available at: <https://doi.org/10.4324/9781003001096>
- Vogels, Emily A., Rise Gelles-Watnick, and Navid Massarat. "Teens, Social Media and Technology 2022." *Pew Research Center*, August 10, 2022. As of March 20, 2023: <https://www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022/>
- Ward, Micah. "How an onslaught of social media threats is disrupting and terrorizing schools." *District Administration*, May 9, 2023. As of July 3, 2023: <https://districtadministration.com/how-an-onslaught-of-social-media-threats-is-disrupting-and-terrorizing-schools/>
- Washington Office of Superintendent of Public Instruction. "Swatting: Mitigation Strategies and Reporting Procedures." webpage, n.d.. As of July 30, 2024: <https://ospi.k12.wa.us/sites/default/files/2023-08/swatting-resources.pdf>
- Williams, Kevin, Nicholas Bogel-Burroughs, and Tim Arango. "Gunman who killed five in Louisville left note and bought rifle legally." *The New York Times*, April 11, 2023. As of April 17, 2023: <https://www.nytimes.com/2023/04/11/us/louisville-shooting-gunman.html>

- Witsil, Frank. "School Threats Happening Daily Across Metro Detroit, Putting Students, Parents on Edge." Detroit Free Press, November 17, 2022. As of July 29, 2024: <https://www.freep.com/story/news/local/michigan/2022/11/17/school-gun-threats-in-ferndale-spread-wildly-by-social-media-spark-fears/69652913007/>
- Wong, Q. "Schools, police warn of US school shooting threats on TikTok." CNET News, December 17, 2021. As of April 28, 2023: <https://www.cnet.com/tech/mobile/schools-police-warn-of-us-school-shooting-threats-on-tiktok/>
- Yechivi, Hannah. "Active shooter hoax continues to haunt Maine schools." December 1, 2022. As of July 29, 2024: <https://www.newscentermaine.com/article/news/education/active-shooter-hoax-maine-sanford-two-weeks-later/97-3d031fa2-3805-4031-b26f-ec3218ab5281>
- Yousef, Odette, "False calls about active school shooters are rising. Behind them is a strange pattern," NPR, October 7, 2022. As of July 5, 2023: <https://www.npr.org/2022/10/07/1127242702/false-calls-about-active-shooters-at-schools-are-up-why>