Anonymized Threat Response Guidance

A Reference Guide for K-12 Schools

September 2024

Anonymous threats pose significant challenges to kindergarten through grade 12 (K-12) schools across the country. 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 reference guide provides streamlined information for K-12 stakeholders to understand and utilize some key best practices from the full, detailed ***Toolkit*** in terms of how to address and respond to anonymous threats.

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.

What Are the Key Strategies to Address Anonymized Threats?

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

Reference Section 2 of the Toolkit.

Encourage reporting to detect threats early, before they spread. Urge community members to "Report, Don't Repost" threats they see online and be clear about the consequences of making threats, even if they are meant to be jokes.

Develop a partnership structure that will help address anonymized threats.

Reference Section 3 of the Toolkit.

Work with key partners to address anonymized and other threats. In addition to school administrators, law enforcement personnel will play a key role in assessing and responding to threats. Mental health professionals also provide critical resources.

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.

Reference Section 3 of the Toolkit.

Multidisciplinary threat assessment teams have the expertise to evaluate an individual who made a threat or exhibited concerning behavior and to select the appropriate supports and interventions for these individuals to reduce the risk of harm. While the utility of a multidisciplinary threat assessment team may be limited prior to knowing the identity of an individual, 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.

Balance initial steps in response to ensure the campus is safe.

Reference Sections 4 and 5 of the Toolkit.

Treat each threat as initially credible, and determine which assets need to be on scene to keep the campus and school community safe. Consider the intensity and overtness of the response and take a balanced approach, leaving open the potential to scale up rapidly. Communicate clearly to the community, and coordinate messaging with law enforcement.

Triage and determine the level of concern a threat poses.

Reference Section 4 of the Toolkit.

Engage law enforcement to manage threat situations, and decide when to scale response actions up or down. Consider key background and contextual information about a threat, and identify patterns that elevate or decrease the level of concern posed by the threat.

Enhance school preparedness to address future threats.

Reference Section 6 of the Toolkit.

Take steps throughout the school year to prepare for threat situations. Ongoing preparedness and prevention efforts outside of emergencies ensure successful response during an emergency. Establish a response protocol, and conduct age- and developmentally appropriate drills and training exercises.

Flowchart Figure 1: **What To Do Before and After a Threat Emergency**

What To Do Before a Threat

Build and maintain relationships with local first responders through regular communications and training.

- Conduct outreach to include police, fire and EMS.

Develop an emergency operations plan (EOP) that includes an annex specifically for anonymized threat situations.

- Train applicable school staff on how to use the EOP annex.
- Share and validate the EOP with police and other first responders.
- Update the plan annually.

Conduct age- and developmentally appropriate drills.

- Invite police and other first responders to participate as appropriate.

Create and maintain protocols for communicating with families during emergencies.

- Share protocols with police to ensure their communications align with the school's.

Establish a multidisciplinary threat assessment team that meets regularly to assess and manage threats.

- Ensure team members are up-to-date on training.

Maintain access to resources to support the mental well-being of the school community.

What To Do After a Threat

Provide access to resources to address trauma and stress.

- Offer counseling and other mental health services.
- Facilitate opportunities for community feedback.

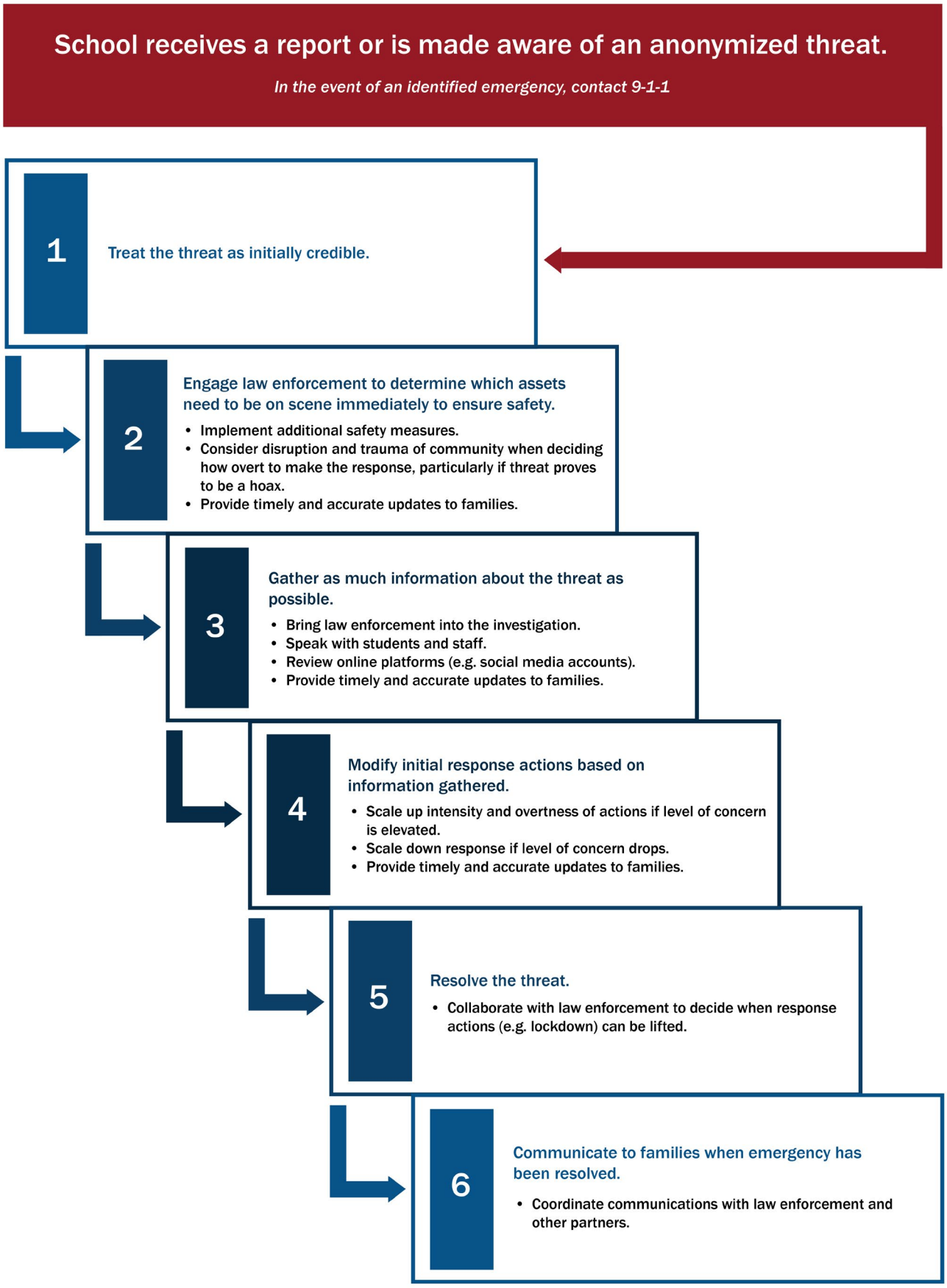
Plan an after-action review of the emergency.

- Incorporate entities from inside the school community and other partners involved in threat response.
- Identify processes that went well and areas for improvement.
- Implement changes to the EOP as necessary.

Continue to communicate about ongoing efforts around safety and recovery.

- Communicate to the school community about new safety measures implemented.
- Offer details about accessing mental health services and ways to provide community feedback.

Flowchart Figure 2: **What To Do During an Anonymous Threat Incident**



Key Themes: Initiating Threat Evaluation to Inform Response

Schools must initially treat all threats they receive as credible. Given the frequency and volume of threats, assessing the viability of a threat and the risk that it poses is a resource-intensive task. Schools and their law enforcement partners can ask 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:

Start by considering background and contextual information.	At the very least, those involved in threat investigation should gather critical background and contextual information about the threat before moving on to a more comprehensive assessment. Investigators should initially determine how the threat was delivered, how the school became aware of the threat, who or what is the target of the threat, when the threatened act of violence is supposed to occur, and whether it is a single threat or one of multiple threats sent to the same school or individual.
Work to detect patterns around the threat.	Many threats against schools come in clusters or waves. It's critically important to identify patterns so hoaxes can be quickly separated from threats requiring more attention. Ask questions that will help determine whether a threat is specific to a school or more diffuse, whether the individual making the threat is in close proximity to the school, whether the threat appears to have been recycled from past threats or is associated with a significant event such as a school shooting, and whether the threat appears to have some kind of goal such as disrupting classes for the day (e.g. during exam times).
Identify signs that the threat is imminent.	Identifying whether there is a probability that an act of violence will occur during a specified timeframe will inform the speed and level at which response actions should take place. Consider whether the threat includes statements about diminishing patience or a shrinking opportunity to engage in violence. Are there references to a "last resort" or is the threat tied to some kind of legacy token such as a manifesto or last will? These could all be indicators of imminent violence.
Continue assessing a threat's level of concern to support response until the threat is resolved.	The steps highlighted above might have identified factors that significantly reduce the level of concern a threat poses (e.g. if information shows that its origin is far from the school itself). In other cases, however, available information makes it much more difficult to assess a threat (e.g. if the threat uses recycled images but still reflects a certain level of specificity or personalization). In such cases, continue the assessment process to gather more information and work with law enforcement partners to implement response actions that will keep your school campus and community safe.

Worksheet 1

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?

Worksheet 2

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.