# Considerations in the Management of Anonymous Threat Communications (ATC) 2023

This workgroup offers considerations based on current professionally accepted practices and reviewed literature for school safety stakeholders to assist with the management of Anonymous Threat Communications (ATC's) and the unique challenges they represent. It is the intention of this workgroup to present considerations for local decision makers and facilitate the flow of communication and multidisciplinary collaboration before, during, and after events occur.

## Workgroup Membership

The following report was developed with representation from the following agencies and associations:

- Maine Chiefs of Police Association
- Maine Sheriff's Association
- Maine School Superintendents Association
- Maine Information and Analysis Center (MIAC)
- Maine School Safety Center/DOE
- United States Attorney's Office, District of Maine
- Unites States Secret Service
- Federal Bureau of Investigations
- Maine School Resource Officers Association

# Anonymous Threat Communication (ATC)

EXECUTIVE SUMMARY

## Anonymous Threat Communications

- Anonymous Threat Communication (ATC) is one in which an unknown entity conveys information that indicates a forthcoming action that will harm, injure, disrupt, or cause public alarm to a person, organization, or population.
- Schools are becoming targets of ATC's and are responding to an increasing number of threats, which presents unique challenges in the management of these communications.

## Considerations in the Management of ATC's.

- All threats should be reported to Law Enforcement immediately.
- School officials, Law Enforcement, and other safety partners should develop a working relationship and plan prior to the occurrence of ATC's based on the availability of local resources.
- Law Enforcement and School Administration will respond and as soon as possible notify the Maine Information Analysis Center (MIAC) who will notify Maine Department of Education's School Safety Center (MSSC).
- Criminal intelligence analysts within MIAC can provide real time support to ongoing investigations by accessing resources and systems that are readily available. Criminal intelligence analysts will review information received and provide case support to investigators as requested.
- Terms such as "hoax' and "prank" should be avoided due to incorrect messaging and interpretation by both the public and other safety stakeholders. Consider other terms such as "false emergency report" or "false active shooter" to convey a more accurate nature of the event.
- ATC's are received via different means including via phone, verbally, written, or emailed, each with special considerations for management. Please see attached ATC Guidance Slick Sheet for specific recommendations for each modality by which schools may receive an ATC.
- It is recommended that schools incorporate an annex into their Emergency Operations Plan to address the response to ATC's including polices, procedures, and a training plan for involved stakeholders.

## Final Note

Every Anonymous Threat Communication (ATC) requires professional judgment and should be handled in a collaborative manner between school safety stakeholders, including school administration and law enforcement, in accordance with the facility's needs. Site Decision Makers should periodically review federal guidance and work with local first responders to establish an ATC plan that addresses each risk appropriately and is optimal for their building(s) and personnel.

## 1. PLANNING CONSIDERATIONS

- Establish partnerships with key safety stake holders **before** an incident occurs
- **Immediately** notify local law enforcement upon receipt of an ATC. Law Enforcement and /or school personal will notify the Maine Information Analysis Center (MIAC)
- Coordinate with local law enforcement & first responders to ensure smooth handling of an ATC
- Develop clear-cut primary and alternate levels of authority (Referred to in this document as "Site Decision Maker(s)")
- Develop training plan
- Designate control center locations
- Plan for emergency assistance (police, fire, etc.) including the flow of information
- Plans pertaining to specific threats that may require school evacuation and/or reunification should be developed in collaboration with local safety stakeholders and clearly outlined in the School Administrative Unit (SAU) Emergency Operations Plan

## 2. RECEIVING A THREAT

### Phone Threat

- Establish protocol with proper training for individuals who routinely answer phone calls to listen carefully to threat calls and answer specific questions
- **Remain Calm & DO NOT HANG UP**
- If possible, signal other staff members to listen & notify Site Decision Maker(s) and authorities
- If the phone has a display, copy the number and/or letters on the window display
- Write down the exact wording of the threat
- Be polite and show interest
- Keep the caller on the line for as long as possible to gather as much information as you can
- Record, if possible
- Immediately upon termination of call, DO NOT HANG UP, but from a different phone, contact authorities immediately with information and await instructions
- Immediately make notation of specific or distinguishing characteristics of caller or their surroundings (refer to Bomb Threat Procedures Checklist/Information about caller section found at https://www.cisa.gov/sites/default/files/2022-11/Bomb-Threat-Procedure-Checklist_508c_0.pdf)
- Be available for interviews with the building's emergency response team and law enforcement

### Verbal Threat

- If the perpetrator leaves, note which direction they went
- Notify the Site Decision Maker(s) and authorities
- Write down the threat exactly as it was communicated
- Note the description of the person who made the threat:
  - Name (if known)
  - Gender
  - Body size (height/weight)
  - Distinguishing features
  - Race
  - Type/color of clothing
  - Hair & eye color
  - Voice (loud, deep, accent, etc.)

### Written Threat

- Handle the document as little as possible
- Notify the Site Decision Maker(s) and authorities
- Rewrite the threat exactly as is on another sheet of paper and note the following:
  - Date/time/location document was found
  - Any situations or conditions surrounding the discovery/ delivery
  - Full names of any personnel who saw the threat
  - Secure the original threat; **DO NOT** alter the item in any way
  - If small/removeable, place in a bag or envelope
  - If large/stationary, secure the location

### Emailed Threat

- Leave the message open on the computer
- Notify the Site Decision Maker(s) and authorities
- Print, photograph, or copy the message and subject line, note the date and time
- **DO NOT** forward the email as information contained in the header of the email provides specifics pertaining to the origin of the email

## 3. THREAT ASSESSMENT

All threats should be carefully evaluated. One must consider the facts and the context, and then conclude whether there is a possible threat.

### Low Risk

**Lacks Realism: A threat that poses a minimum risk to the victim and public safety. Probable motive is to cause disruption.**

- Threat is vague and indirect
- Information contained within the threat is inconsistent, implausible, or lacks detail
- Caller is definitely known and has called numerous times
- The threat was discovered instead of delivered (e.g., a threat written on a wall)

### Medium Risk

**Increased Level of Realism: Threat that could be carried out, although it may not appear entirely realistic.**

- Threat is direct and feasible
- Wording in the threat suggest the perpetrator has given some thought on how the act will be carried out
- May include indications of a possible place and time
- No strong indication the perpetrator has taken preparatory steps, although there may be some indirect reference pointing to that possibility
- Indication the perpetrator has details regarding the availability of components needed to construct a bomb
- Increased specificity to the threat (e.g. "**I'm serious!**" or "**I really mean this!**")

### High Risk

**Specific and Realistic: Threat appears to pose an immediate and serious danger to the safety of others.**

- Threat is direct, specific, and realistic; may include names of possible victims, specific time, and location of device
- Perpetrator provides his/her identity
- Threat suggests concrete steps have been taken toward carrying out the threat
- Perpetrator indicates they have practiced with a weapon or have had the intended victim(s) under surveillance

# Anonymous Threat Considerations for Maine

## I. Purpose

The purpose of this document is to (a) provide an explanation of the unique challenges of anonymous threat communication (ATC) incidents to our schools (b) provide an overview of the most current data of these incidents, and (c) develop operational considerations for public safety and school officials to utilize as a support to their decision making when responding to these events. Ultimately, the final responsibility and decision-making rests with the local authorities including law enforcement and school administration.

## II. Definitions

A. Anonymous Threat Communication (ATC)-An action taken by an unknown entity, that conveys through any means, information that indicates a forthcoming action that will harm, injure, disrupt, or causes public alarm to a person, organization, or population.

B. Types of Anonymous Threats

1. Verbal or telephonic threats
2. Written threats (letter, email, social media)
3. False emergency reports
4. Graffiti (ex. threat on bathroom wall)
5. Third party victimization
6. Cyber based extortion
7. Hitman extortion
8. Blackmail and sextortion
9. Self-victimization
10. Current trends in threat waves

## III. Discussion

Maine schools and public safety officials are increasingly responding to anonymous threats in schools. ATCs are a relatively new event due to the modern world of technology providing many venues for the conveyance of information and opportunities to hide the authorship. The level of disruption and community fear that these incidents create is significant and often leads to a debilitating situation for the school community, both during and after the event.

ATCs are a unique challenge. In cases where the perpetrator is known, there is ample information and evidence-based procedures to implement to address the event by utilizing Behavioral Threat Assessment and Management (BTAM), specifically employing the Comprehensive School Threat Assessment Guidelines (CSTAG) methodology (See Appendix A). However, there is no official standardized methodology that exists to employ with anonymous threats and no agreed upon decision making matrix to rely upon to make sound determinations on response options. The difference between the two events is significant (*known vs unknown perpetrator/actor*) and this difference cannot be underestimated as to the complexity it brings to the response options for the school.

A. Anonymous Threat Communication Dynamics-Nature of the Incident

Data and research demonstrate anonymous threats are conducted for the purpose of causing disruption, fear, interrupting organizational activities, or furthering ideological or political agendas. The linkage to physical acts of violence is considered minimal. However, regardless of this information all consideration should be taken to realize that nothing precludes an anonymous threat from leading to violence. Therefore, the need to capture, preserve, process, and analyze evidence becomes essential to support subsequent decisions on how to respond to the threat. School partnership and communication with law enforcement and other relevant school safety stakeholders is critical due to the nature of this incident. Together the school officials and law enforcement officials will make more sound decisions on how to proceed based upon a common understanding and analysis of the facts of the incident. Decision making in isolation should be avoided and instead utilize a multi-disciplinary team approach to analyze and respond to an anonymous threat.

B. Communications

Reporting protocols are essential to assure a proper response and to quell public concern. Pre-event proactive communication with law enforcement should take place to determine commonality of expectation on event notification. Anonymous threats take many forms from a handwritten note left on a teacher's desk, graffiti on the bathroom wall, and state-wide swatting incidents, which consist of emergency reports causing first responders to report to a targeted location. Pre-event discussions must take place with law enforcement to determine when the police should be notified and identify subsequent action steps by both parties (school and law enforcement). Regardless of the outcome of these discussions, the following evidence processing protocols should be followed utilizing the triage questions below.

1. How was the communications delivered?
2. How many communications have been received and by whom? During what time frame?
3. Is this a single, isolated communication, or part of a series sent to the same victim?
4. Are there indicators of possible relationship or prior contact between the victim and offender?
5. When did the victim receive the communications and when was it reported to law enforcement?
6. According to the anonymous threatening offender, when will the undesirable threatening act occur?
7. Is it feasible for the offender to carry out the threatened act?
8. Who are the targets, named and implied, of the threatening communication?
9. Who are other persons or organizations named or referenced within the communications and what are their relationship to the primary targeted victim?
10. What is the significance of any named or referenced locations or dates?
11. What steps or measures were taken to conceal the author's identity?
12. What details are available concerning the recipient's victimology?

13. What details are available concerning any personal or professional issues and conflicts experienced by the targeted recipient(s)?
14. What is the victim's assessment of the ATC both for level of concern and authorship?
15. What specific analysis (or combinations thereof will most benefit the primary investigating agency (e.g., assessment of concern of violence, threat and or risk management strategies, target hardening strategies, unknown offender characteristics, investigative suggestions, media strategies)?

Communication with the greater community should be taken with care to avoid needlessly causing public alarm and to inform the public accurately of the event. Many communications may be pre-developed to fit the majority of events and then deployed with little editing during the actual event. Terms indicating the event is a "hoax" or a "prank" should be avoided due to the incorrect messaging and interpretation by both the public and other involved stakeholders. ***Anonymous threats are real events in and of themselves by the above definition*.** Alternate terms, such as "false emergency report" or "false active shooter report", should be considered that convey a more accurate nature of the event.

C. Reporting

Once an event takes place the school should immediately notify local law enforcement, consisting of the local Police Department, County Sheriff's Office, or Maine State Police as applicable to their specific area per protocol. Law enforcement will respond and as soon as possible notify the Maine Information Analysis Center (MIAC) who will notify DOE/MSSC as predetermined by the Maine School Safety Center (MSSC)/MIAC communications agreement (see Appendix B). Any entity may notify MIAC of the event. Any involved agency and or receiving agency should notify MIAC if they determine that MIAC was not informed of the event. This includes school administration who may notify MIAC directly. However, a predetermined communications flow with their primary law enforcement agency is preferred.

The inclusion of MIAC is an essential part of the response and subsequent investigation to determine the veracity of the threat. MIAC tracks local, regional, and national school threats and may be able to provide critical information quickly to law enforcement and school administration that the current incident is similar to other incidents around the state or country. MIAC will also help connect law enforcement to investigative resources to assist with their investigation (see Appendix C). MIAC'S abilities are particularly helpful in responding to swatting incidents due their ability to inform the police and school of similar incidents which may indicate this is an act to cause disruption and not an act of violence. An efficient and timely reporting protocol may greatly influence the response footprint due to relevant information informing the likelihood the event is not likely to lead to an act of violence.

Additionally, criminal intelligence analysts within the MIAC can provide real time support to ongoing investigations by accessing resources and systems readily available. Criminal intelligence analysts will review any information received and provide case support to investigators as requested.

D. Considerations

One event or singular events with long timeframes between occurrences are easier to address than a series of events in close proximity to one another. A singular event allows for the decision-making authorities to act in a conservative and most protective manner that may significantly disrupt the organization/community for a limited time. However, a series of events in a limited time frame causes additional special considerations due to an ongoing disruption and significant inability for the school to carry out its purpose of providing education. This document is designed to assist both law enforcement and school administrators to make these difficult decisions with the most current information and within national standards.

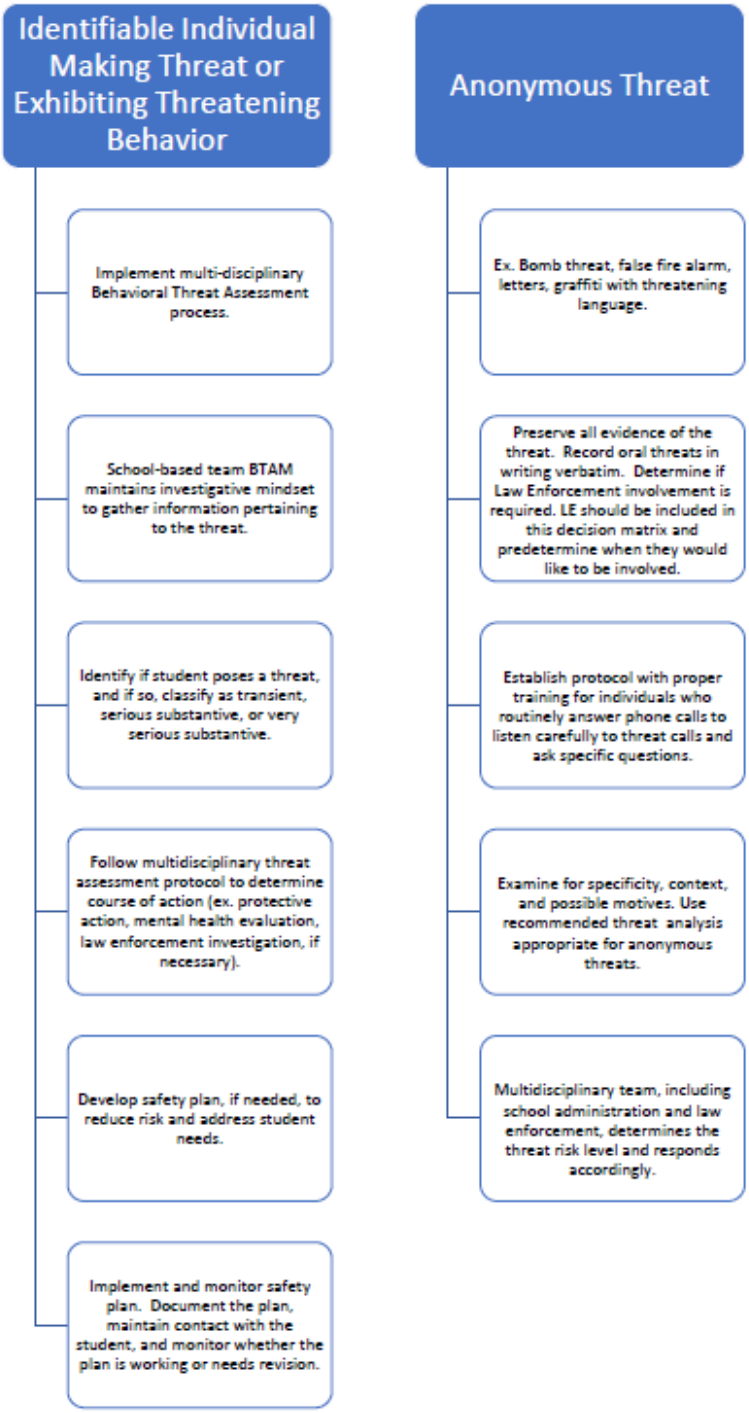
For purpose of a case example, an anonymous threat is discovered at the school via a cryptic note found on a bathroom wall. In this example, MIAC may be able to inform that this is the third threat of this nature statewide in the past 2 days, and on this particular day, exams are taking place and driving conditions are poor. Competing harms should always be considered knowing many threats of this nature are not substantive, and in this case, a school-wide evacuation may not be warranted nor the safest action. The decision will always be made at the local level collaboratively between school administration and the local police authority. Armed with this information and following investigative protocols may quickly determine this communication has a low level of concern (see Appendix C) and therefore the following response does not significantly disrupt the school day. Other protective actions could take place such as conducting a building sweep for objects that do not belong, increasing law enforcement presence, limiting school activities without a total shutdown, etc. It is recommended that schools incorporate an annex into their Emergency Operations Plans to address the response to anonymous threats including policies, procedures, and training planned for involved stakeholders.

## IV. Conclusion

Understanding the nature of an Anonymous Threat Communication (ATC) will greatly enhance the ability of local authorities to make more efficient decisions on response modality. Key actions steps, resources, and investigative protocols are attached in the following pages. Utilizing these resources, operating in a multidisciplinary manner, and following the outlined investigative steps will provide for sounder decision making and ultimately the possibility of a less disruptive response to our schools and communities.

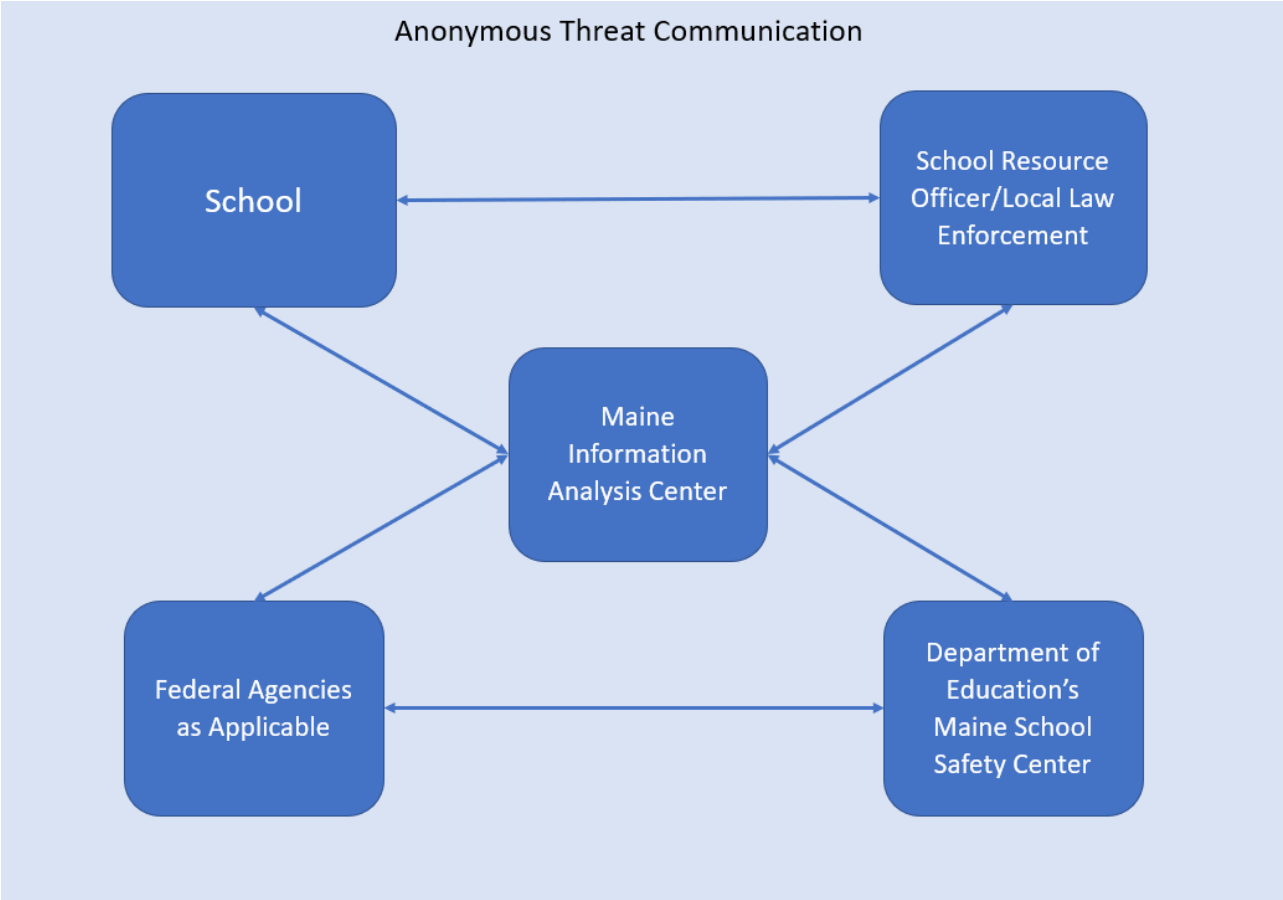
# Appendix A

## Targeted School Violence Threat Protocol



# Appendix B

## Anonymous Threat Communication



# Appendix C

## Agencies That May Be Involved in Anonymous Threat Communication (ATC) Events

- Local law enforcement
    - Police Department
    - County Sheriff Office
    - State Police
- Federal Bureau of Investigation
- U.S. Secret Service
- Department of Homeland Security
- Bureau of Alcohol Tobacco and Firearms
- Maine Information and Analysis Center
- Other as Applicable

# Appendix D

## Levels of Concern

**LOW** Level of Concern: Risk to students, employees and visitors appears to be minimal. Threat is vague and indirect in nature. Information within threat is inconsistent, implausible, or lacks detail. Threat is not realistic in nature/presentation. Available information suggests person of concern is unlikely to act violently.

**MEDIUM** Level of Concern: Risk to students, employees and visitors appears to be moderate. Violent action is possible, but not probable. Threat is still not entirely realistic in nature. Analysis of threat suggests some thought/action on how to go forward by person of concern, i.e.-a specific time and location noted for actions. No clear indication of preparatory steps taken by person of concern. Person of concern may attempt to convey seriousness of situation, e.g. – "I'm very serious," "I'm not kidding," etc.

**HIGH** Level of Concern: Risk to students, employees and visitors appears to be serious and imminent. Threat is specific and plausible. Person of concern notes a specific 'target' and has the capacity to act. Person of concern has taken specific steps in furtherance of threat, e.g.-surveillance of target, weapon acquisition/practice, etc. Documented information notes strong possibility of violent behavior

# References and Additional Resources


Cornell, D. G. (2018). *Comprehensive school threat assessment guidelines*. Charlottesville: School Threat Assessment Consultants LLC.

https://www.cisa.gov/resources-tools/resources/dhs-bomb-threat-checklist

https://www.maine.gov/doe/safety

https://www.maine.gov/dps/msp/specialty-units/MIAC

Mehrotra, D. (2022). Hot on the trail of a Mass-School-Shooting Hoaxer.

Meloy, J. R., & O'toole, M. E. (2011). The concept of leakage in threat assessment. *Behavioral sciences & the law*, *29*(4), 513-527.

Simons, A., & Tunkel, R. (2014). The assessment of anonymous threatening communications. *International handbook of threat assessment*, 195-213.

Slemaker, A. (2022). Studying mass shooters' words: Warning behavior prior to attacks. *Journal of Threat Assessment and Management*.

Spitzberg, B. H., & Gawron, J. M. (2016). Toward online linguistic surveillance of threatening messages. *Journal of Digital Forensics, Security and Law*, *11*(3), 7.