



Virtual (Anonymous) Threat Checklist

Notifications Date/time <input type="checkbox"/> Principal _/_/_ _ <input type="checkbox"/> School Leadership _/_/_ _ <input type="checkbox"/> Law Enforcement _/_/_ _ <input type="checkbox"/> Other _/_/_ _ (Please specify):	Type of Threat: <input type="checkbox"/> Social Media <input type="checkbox"/> Site _____ <input type="checkbox"/> User Name _____ <input type="checkbox"/> Additional Recipients? _____ <input type="checkbox"/> E-mail _____ <input type="checkbox"/> Text # _____ <input type="checkbox"/> Written <input type="checkbox"/> Date/ Time _/_/_ _ <input type="checkbox"/> Other (Please specify):	Threat received by: <hr/> Additional Search Efforts included: <input type="checkbox"/> Reverse image search _____ <input type="checkbox"/> Specialized Google search _____ <input type="checkbox"/> Social media search app. _____ <input type="checkbox"/> IP Address _____ <input type="checkbox"/> Locators and look-up tools _____
---	--	--

*** Please complete this document as detailed as possible. Do not leave a question blank. (Use N/A or unknown if needed.)*

1. What was the threat? (use exact wording if possible.)

2. If there was a picture(s)/graphic(s) included in the threat please upload image here and/or include a description of the threat. (If there is a video, please use your phone to record, upload to google drive and link here.)

3. Is there information that can be used to identify the person making the threat?

4. Indicate the threatener (if known). (If that person is a KUSD student, please ensure a full CSTAG threat assessment will be completed.)

<u>Name:</u> <u>Address:</u> <u>Phone:</u> <u>DOB:</u> <u>Student ID:</u> <u>Parent Names:</u> <u>2nd parent address?:</u>	<u>If not known:</u> - Please list suspects, and what makes them a suspect. - Accomplices?
--	--

5. Was there a specific target, location and/or time specified in the threat?

Target:
Location:
Time:
Other specifics shared:

6. What other prior contact has there been between the victim and the threatener?

7. If known, does the threatener have motive for violence? (Please list evidence of a motive or identifiable grievance?)

8. Have we conducted a threat assessment on this individual before?

9. Does the threatener have a history of concerning behaviors, mental health, suicidal ideation or a history of violence?

10. Does the threatener have access to weapons? (Please indicate if/how it is feasible for the threatener to carry out the threat?):

11. How much effort was employed to deliver the threat? (Was there any effort to follow up or were there additional steps taken to advance the threatening communication? If so, please describe.)

12. How much effort or risk did the threatener take when delivering the threat? (Did the threat involve physically approaching the private space or the location of the targeted victim?)

*Questions on this form have been adapted from the **Homeland Security National Threat Evaluation and Reporting Office Behavioral Threat Assessment and Management Tool Kit: 05 TOOLKIT – Assessing Anonymous Threatening Communications**

Sources:

Dept of Justice, Federal Bureau of Investigation, Behavioral Analysis Unit, "Making prevention a reality: Identifying, assessing, and managing the threat of targeted attacks," 2017.
 Simons, Andre, and Ronald Tunkel. "The assessment of anonymous threatening communications." International Handbook of Threat Assessment (2014): 195-213.

Using this document to make a decision.

- Look at highest priority categories (red font). What factors are we considering?:
- Is the threat specific? (School name, how, when, why? other?)
- Is the suspect at large? (with capability to carry out the threat?)
- If the suspect is unknown, or if the threat isn't specific, what steps can we take to make school safer?
- What follow up steps are needed?

➔ RESPONSE MEASURES^{6,7}

Fortunately, many social media threats can be traced, allowing law enforcement to follow up with the individual who posted the threat and conduct an interview to determine credibility. **It is a criminal offense to make a threat against a school system and it is possible that the person in question could be charged with a felony.** Police advise treating every threat seriously.

FIRST STEPS

- 1 Implement Your EOP**
 - **Activate the EOP** determined by the Core Planning Team made up of school staff and stakeholders (local law enforcement, community organizations, families, etc.).
 - **Determine the type of threat** (bombing, fire as a weapon, shooting, etc.) and follow the necessary protocols as indicated by the EOP.
 - **Alert school authorities, personnel, parents,** etc. of all threats via the proper communications channels and keep them up to date until all threats have been resolved.
 - **Follow procedures for appropriate response** (lockdown, evacuation, school closing, etc.).
- 2 Treat All Threats Seriously**
 - **Report to local authorities** as quickly as possible.
 - **If there is a possibility of immediate danger, call 9-1-1.**

ADDITIONAL ACTIONS

- Threats of Violence on Social Media**
 - **Immediately notify law enforcement** that a threat was received.
 - **Do not delete or share the post and preserve all electronic evidence.** Print, photograph, screenshot or copy the message information (subject line, date, time, sender, etc.).
 - **Follow authorities' instructions and be available for interviews.** Law enforcement will assess the situation and provide guidance regarding facility lockdown, search and/or evacuation.
- Bomb Threats Received via Social Media**
 - **Remain calm.**
 - **Notify authorities immediately:**
 - Call 9-1-1.
 - Notify facility supervisor, administrator, or follow the facility EOP.
 - **Refer to the DHS Bomb Threat Checklist** for guidance.
 - **Follow authorities' instructions and be available for interviews.** Facility supervisors and/or law enforcement will assess the situation and provide guidance regarding facility lockdown, search and/or evacuation.

➔ After The Incident

- Take appropriate disciplinary and criminal enforcement steps.
- Document threats and actions taken for internal evaluation.
- Enhance security measures and planning procedures, as appropriate, to ensure the safety of all students, staff and facilities based on evaluation.
- Debrief emergency services and assist in coordinating further actions.
- Site Decision Maker(s) should remain on-scene until the situation is resolved or until relieved by another administrator.