TIPS AND LEADS AND THREATS TO LIFE

STANDARD OPERATING PROCEDURES

Global Justice Information Sharing Initiative

This project was supported by Grant No. 2018-DP-BX-K021 awarded by the Bureau of Justice Assistance, in collaboration with the U.S. Department of Justice's Global Justice Information Sharing Initiative. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office of Victims of Crime. Points of view or opinions in this document are those of the author and do not represent the official position or policies of the U.S. Department of Justice.

[*Name of Primary Entity//Name of Secondary Entity*]

Threat to Life (TTL) Initiative: Standard Operating Procedures for the Criminal Intelligence Sharing Node for the [*Name of Region*] Region

[*Effective Date*]

I. Background

The Threat to Life (TTL) Initiative was created to provide a consistent reporting and feedback mechanism for threat-related information in which appropriate law enforcement personnel can quickly vet and mitigate threats. This document was created to outline the TTL reporting process.

The Federal Bureau of Investigation's (FBI's) National Threat Operations Center (NTOC), law enforcement agencies, and/or private sector company partners may report TTL Reports to the ***[Name of Primary Entity].*** TTL Reports describe subject(s) who are believed to be a danger to others or themselves, based on indications of a verbal or visual threat of death or bodily injury to the individual or another person or persons, or to damage or compromise a facility/infrastructure or secured protected site. ***[Name of Primary Entity]*** partners with the ***[Name of Secondary Entity]*** to serve as the focal point for social media companies to submit TTL reports for the ***[Name of Region]. [Name of Primary Entity]*** and ***[Name of Secondary Entity]*** analysts accept TTL Reports, attempt to identify the subject making the threat(s) and the subject's location, and disseminate the information to the appropriate federal, state, local, tribal, territorial (FSLTT) organization, foreign law enforcement agency, and/or appropriate state or major urban area fusion center.

If the Primary Entity operates on a 24/7/365 basis, then a secondary entity is not needed to serve as a backup agency for processing TTLs. Under these circumstances, references to a secondary entity in this SOP may be removed.

II. Definition

For purposes of the TTL Initiative, the term "threat to life" (TTL) is defined as "an emergency involving danger of death or serious physical injury to any person." See Electronic Communication Privacy Act (ECPA), Voluntary Disclosure of Customer Communications or Records, Title 18 U.S.C. §§ 2702 (b)(8) and (c)(4). TTLs involve:

- A threat to kill or seriously injure others.
- A threat to kill or seriously injure oneself.

Such threats may be imminent or potential. Examples of TTLs include but are not limited to threat to public safety, crisis calls, active shooters, and threats to law enforcement.

Threats may be discovered by friends, family members, community members, and/or online platform moderators. Many TTL Reports require immediate action and notification to law enforcement to ensure public safety and/or to mitigate the known or perceived threats.

To ensure that TTL Reports receive immediate attention and notification to law enforcement, most social media companies will reference the Electronic Communication Privacy Act (ECPA), Voluntary Disclosure of Customer Communications or Records, codified in Title 18 U.S.C. §§ 2702 (b)(8) and (c)(4). These provisions allow voluntary disclosure of customer information to law enforcement if the "provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency "

III. Overview of the TTL Reporting Process

TTL Reports may be submitted to the ***[Name of Primary Entity]*** via telephone, tip line, eGuardian, or email. TTL Reports vary in quality, content, and timeliness. Depending on the information provided, an analyst may need to conduct follow-up to clarify a report or acquire additional information. However, it should be noted that the submitter of a TTL Report may not always respond to follow-up emails or phone calls in a timely manner, and the analyst may need to use the information available to conduct a search for a subject's identity or identifying information. TTL Reports may include attachments for images, videos, text messages, subscriber information, or additional context. The information provided in the original submission may be all the information the submitter has available. If the analyst believes additional information may be available, the analyst can request the assistance of a ***[Name of Primary Entity] [Name of Liaison Officer or other Similar Role]*** or other appropriate law enforcement partner to submit an Emergency Disclosure Request (EDR), if deemed appropriate.

[Insert a description of the Primary Entity and the Secondary Entity's hours of responsibility, delineating who will handle the TTL Reports and when.]

IV. Workflow of TTL Reports

A. Objectives

1. A trained intelligence analyst from the ***[Name of Regional Node]*** should immediately review all TTL Reports upon receipt and determine the level of urgency of the information.

2. If an analyst is uncertain about the urgency of the information, he/she is encouraged to seek input from a peer or supervisor.

3. Analysts should attempt to complete urgent potential TTL Reports within ***[Number of Hours]*** hours of receipt when possible.

B. Downgrading an Urgent Potential TTL Report

If the content of the TTL Report (either upon initial submission or after a workup) is complete and does not warrant an emergency response by law enforcement, the TTL can be downgraded from an urgent TTL Report. The ***[Name of Primary Entity]*** analyst should adhere to the applicable standard operating procedures (SOPs) for classifying, documenting, storing, and (if appropriate) disseminating this type of information and will work downgraded incidents as part of the analyst's normal work duties.

C. Description of the TTL Workflow Process

1. The analyst is expected to immediately accept any TTL Reports submitted to the ***[Name of Regional Node]***.

2. TTL Reports that are dual routed from the NTOC will be preceded by a telephone call and an email notification to the ***[Name of Primary Entity]*** and must be acknowledged by the accepting analyst in eGuardian.

3. The analyst will check the TTL submission for attachments and accessibility.

4. Using his/her training and experience, the analyst will evaluate whether the information received by the social media company is sufficient by:
   a. Examining whether the incident constitutes a TTL, as defined in the SOPs.
      i. **[*Insert guidance on what constitutes a threat to life.*]**
   b. Determining whether the subject/victim/witness and/or his/her location is or can be identified.

Each regional node should confer and develop clear guidance for analysts regarding TTL issues (e.g., what constitutes a threat to life, what constitutes an "emergency" for purposes of an EDR, and what the legal process is for supporting an EDR). These considerations may be unique to each jurisdiction.

In addition, analysts should have access to their entities' legal counsel and P/CL officers, as needed.

5. If the information is insufficient, the analyst may assess whether submitting an EDR is appropriate under applicable federal and state law.[1]
   a. [*Insert an explanation of what constitutes an emergency under applicable law.*]

[1] If an EDR is needed, it may be submitted by the primary entity or the assisting/responding local law enforcement agency. This may include coordinating with terrorism liaison officers (TLOs) to identify the best agency for submitting a warrant, subpoena, or court order for that information. Alternatively, the FBI has authority to issue an EDR for voluntary communications or records under 18 U.S.C. § 2702(b)(8) and to seek a court order for disclosure under 18 U.S.C. § 2703 to require the disclosure of customer communications or records (based on "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation").
For information about the interpretation of exigent circumstances, refer to the Frequently Asked Questions.

b. [*Insert guidance on the requirements for legal process for the states in the region.*]

i. [*Include guidance to address situations in which the information may be so insufficient that the agency cannot establish the predicate under state law to seek a subpoena or a warrant (e.g., in some states, suicide is not a crime).*]

6. If appropriate, when a physical address and/or subject is identified, the analyst will contact the law enforcement agency with the investigative lead and relay the deconflicted TTL information. Deconflicted TTL Reports which resolve to **[*Name of the Region for which the Primary and Secondary Entities are responsible*]** will be forwarded to the state or major urban area fusion center for the Area of Responsibility (AOR) where the threat was located and will be followed up with a phone call to ensure that the TTL Report was received.

7. If the incident involves federal violations of law, the intelligence analyst will send it to the local FBI field office for triage and/or deconfliction.

8. If the incident qualifies as an Information Sharing Environment-Suspicious Activity Report (ISE-SAR), the intelligence analyst at the regional node will submit the report to the eGuardian SAR Data Repository (SDR).

9. Duplicate reporting may occur when reporting parties forward information to multiple law enforcement entities.

10. If a TTL Report does not have enough information to be analyzed and/or the analyst has exhausted all research options and is unable to identify a subject/victim/witness and/or his/her location, this information should be thoroughly documented per the SOPs for the ***[Name of the Primary Entity]***.

11. The ***[Name of the Primary Entity]*** analysts will document the TTL Report according to the ***[Name of the Primary Entity]*** SOPs, including those worked by ***[Name of Secondary Entity]***.

12. ***[Insert description of the process for providing feedback[2] to the submitting party regarding the TTL's disposition.]***

13. If a state or major urban area fusion center, police department, sheriff's office, or state police agency refuses to accept the TTL Report, regardless of the time of day or reason, the analyst will forward the information to the appropriate state or major urban area fusion center and/or FSLTT agency with a comment that the information is being sent for "situational awareness and visibility only." Any refusal to accept a TTL Report will be documented in accordance with the ***[Name of the Primary Entity's]*** SOPs.

[2] The term "feedback" refers to baseline information such as that the person was contacted, assistance was provided, or an arrest was made relating to the TTL incident.

14. Analysts or outreach officers may adopt the following practices when communicating with local law enforcement agencies:
    a. Use the ***TTL Boiler Plate Language Guide*** as a starting point for drafting or communicating your response to other agencies. (See Appendix I)
    b. Introduce yourself using your full law enforcement agency title and your association to your parent law enforcement agency, since the personnel may not be familiar with the ***[Name of the Primary Entity]*** or **[*Name of the Secondary Entity*]**.
    c. During verbal and written communications, describe the level of confidence in plain language, citing inconsistencies in findings, and avoid using abbreviations.

15. If an agency reports an update on a TTL Incident, the analyst receiving the update is responsible for ensuring that:
    a. Supervisors, analysts, law enforcement agencies, and reporting parties are updated as appropriate.
    b. The ***[Name of Primary Entity]*** TTL Report and supporting documentation is updated with the new information.

16. The collection, triage, analysis, dissemination, and feedback related to TTLs will comply with applicable privacy, civil rights, and civil liberties laws, regulations, and policies.[3]

[3] See, e.g., *Fusion Center Privacy, Civil Rights, and Civil Liberties Policy Development Template* (March 2019*); Real-time and Open Source Analysis Resource Guide* (2017). For further information, refer to the *Frequently Asked Questions* and *Promising Practices*.

Appendix I
Threat-to-Life Boiler Plate Language Guide

I. When local law enforcement has already been contacted (both urgent and nonurgent TTLs)

This potential threat-to-life report is being forwarded to you for your situational awareness only. ***[Name of local law enforcement entity]*** has already been informed of this information.

II. When local law enforcement has NOT been contacted

A. URGENT TTL

1. Unable to definitively identify a subject (telephone phone call is necessary)

   Preliminary analysis indicates that this information is **URGENT and may require **immediate action**.** This potential threat-to-life report is being forwarded to you, since analysis indicates the subject may reside within your jurisdiction. Based on the information provided, we were unable to definitively identify a subject, so the information is being passed to your center for further research, if appropriate.

   An analyst will call your center to confirm receipt of this potential threat-to-life report. Local law enforcement has **NOT** been contacted. ***[Name of Primary Entity]*** and ***[Secondary Entity]***, serving as the regional node for the ***[Name of Region]***, **WILL NOT** be taking further action on this matter. Please review the information and take any action you deem appropriate.

2. Urgent TTL POSSIBLE—The subject has been identified, but there is insufficient information to call local law enforcement (telephone call to the state or major urban area fusion center necessary).

   Preliminary analysis indicates that this information is **URGENT and may require **immediate action**.** This potential threat-to-life report is being forwarded to you, since analysis indicates the subject may reside within your jurisdiction.

   Based on the information provided, we were unable to definitively identify a subject; however, a POSSIBLE subject has been identified. Please see the attachments/email for details. An analyst will call your center to confirm receipt of this potential threat-to-life report. Local law enforcement has **NOT** been contacted.

   [Name of Primary Entity] and ***[Secondary Entity]***, serving as the regional node for the ***[Name of Region]***, **WILL NOT** be taking further action on this matter. Please review the information and take any action you deem appropriate.

B. NONURGENT TTL (telephone call is <u>not</u> necessary)

1. Unable to definitively identify a subject

   This potential threat-to-life report is being forwarded to you, since analysis indicates the subject may reside within your jurisdiction. Based on the information provided, we were unable to definitively identify a subject, so the information is being passed to your center for further research, if appropriate.

   Preliminary analysis indicates that this information is **NOT** urgent and does **NOT** require immediate after-hours action. Local law enforcement has **NOT** been contacted.

   [Name of Primary Entity] and ***[Secondary Entity]***, serving as the regional node for the ***[Name of Region]***, will not be taking further action on this matter. Please review the information and take any action you deem appropriate.

2. A POSSIBLE subject has been identified, but there is not enough information to call local law enforcement (telephone call to the state or major urban area fusion center is not necessary).

   This potential threat-to-life report is being forwarded to you, since analysis indicates the subject may reside within your jurisdiction. Based on the information provided, we were unable to definitively identify a subject; however, a POSSIBLE subject has been identified.

   Please see the attachments/email for details. Preliminary analysis indicates that this information is **NOT** urgent and does **NOT** require immediate after-hours action. Local law enforcement has **NOT** been contacted.

   [Name of Primary Entity] and ***[Secondary Entity]***, serving as the regional node for the ***[Name of Region]***, **WILL NOT** be taking further action on this matter. Please review the information and take any action you deem appropriate.