TIPS AND LEADS AND THREATS TO LIFE

REGIONAL NODES PROPOSAL

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.

Preliminary Recommendation for the Development of a Framework for Regional Criminal Intelligence Sharing Nodes

Social media companies experience difficulties when reporting online threats to law enforcement. Online threats are increasing at a rapid rate, and social media companies struggle to identify which of the 18,000 law enforcement agencies has primary jurisdiction over an incident. In addition, threats to life (TTL) often require immediate attention and must be promptly routed to the responsible state, local, tribal, or territorial (SLTT) or federal organization or foreign law enforcement agency and/or the appropriate fusion center for review and vetting.

> For purposes of the TTL Initiative, the term "threat to life" 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 threats to public safety, crisis calls, active shooters, and threats to law enforcement.

To streamline the flow of TTLs and avoid unnecessary delays caused by a fragmented system, the Northern California Regional Intelligence Center (NCRIC) and the Western States Information Network (WSIN) developed a process used by social media companies on a 24/7/365 basis for reporting online threats. With this process, vetted social media company employees use an online report form to submit TTLs identified on their platforms to the NCRIC, or WSIN after hours, for collection, triage, analysis, dissemination, and feedback.[1] The TTL reports submitted by social media companies are typically regarding platform users who are believed to be a danger to others or themselves.[2] Criminal intelligence analysts at NCRIC or WSIN attempt to identify the subject(s) making the threat(s) and/or their locations and initiate reporting to the responsible SLTT or federal organization or foreign law enforcement agency and the appropriate fusion center. Although the process has proven effective, the exponential growth of online threats has placed an extraordinary burden on the resources of NCRIC and WSIN.

The Federal Bureau of Investigation's (FBI's) National Threat Operations Center (NTOC) also processes a staggering volume of tips. The NTOC serves as the FBI's central intake point through which the public can provide tip information about potential or ongoing crimes. The NTOC assesses all tips to determine whether they require FBI action or referral to another agency, to include state and local law enforcement.[3] The FBI has enhanced the unclassified eGuardian information sharing system to dual-route TTL tips from the NTOC directly to the appropriate fusion center or other law enforcement agency for action, with a simultaneous notification to the affected FBI field office via the FBI's Guardian system. This process enables the FBI to share

[1] Feedback is limited to baseline information only (e.g., the person was contacted, assistance was provided, or an arrest was made relating to the TTL incident).
[2] This is based on a communication of a spoken or written threat to commit a crime that will result in death or serious physical injury to the individual or another person or persons.
[3] For a list of participating agencies, refer to Appendix I below.

nonfederal TTL tips with the FBI's SLTT partners to enhance the law enforcement community's ability to mitigate violent criminal activity. All tips received by the NTOC are retained in the Threat Intake Processing System (TIPS), pursuant to applicable federal laws.

The Social Media Subgroup has assessed the information sharing gaps and has developed a sustainable model for TTL reporting, triage, analysis, dissemination, and feedback. The subgroup concluded that the volume of reporting, the exigent nature of TTLs, and the absence of the equivalence of a national 9-1-1 call center underscore the need to create a streamlined process that leverages existing capabilities. Yet the simple truth is that there is no single answer to this problem. One option considered by the subgroup involved the use of a centralized system. However, a centralized mechanism may limit visibility into the threat picture if access is unduly restricted. This mechanism may also become the single point of failure and, as such, this option poses significant risks. Another option involved the creation of a submission point for each state, tribal entity, and territory, but this approach would likely be unworkable because of the need for each entity to have the operational capability to process TTL reports on a 24/7/365 basis. Social media companies would likely view this approach as unmanageable because of the sheer number of potential submission points.

I. Recommendations

The Social Media Subgroup has concluded that the model should complement the NTOC's processes and leverage the existing capabilities and resources of the National Network of Fusion Centers and the Regional Information Sharing Systems (RISS). To avoid delays and overcome gaps in operational capabilities, the Social Media Subgroup offers the following recommendations to the Global Justice Information Sharing Initiative (Global) and the Criminal Intelligence Coordinating Council (CICC):

A. A distributive regional model should be adopted and implemented to ensure that TTLs are appropriately collected, triaged, analyzed, and disseminated to the appropriate local law enforcement agencies at the right time and that feedback is provided as appropriate. To support this model, formal guidance should be developed to address how, where, and when social media companies report threat information that is detected on their platforms or reported by users of their various services. In addition, standard operating procedures should be developed, adopted, and implemented. For further information about a distributive regional model, refer to Section II.

B. As feasible, the FBI should adopt a standard requirement that all FBI field offices participate in the dual routing of TTLs.

II. Overview of Distributive Regional Model

A. Six regional criminal intelligence sharing nodes would serve as the focal point for social media companies to submit TTL reports for a particular region. Serving as the regional node provides visibility into the online threat.

1. Each node would consist of a DHS-recognized fusion center ("primary entity") in partnership with another law enforcement entity ("secondary entity") and would serve as the 24/7/365 submission point for TTLs in the region.
2. To support the TTL process for the region, the primary and secondary entities must have consistent resources, capabilities (including the ability to triage, analyze, and share TTLs quickly), a standardized methodology, and a governance structure.
3. In selecting the entities that may serve as the designated regional hub, preference would be given to those fusion centers and entities with the capability to handle a high volume of TTLs on a 24/7/365 basis and to provide appropriate feedback to social media companies.

B. The location of a TTL should determine its routing.

1. Social media companies should identify the location of the TTL and report the TTL to the node with responsibility for that region.
2. For a TTL with an unknown location, social media companies should submit the TTL report directly to the FBI NTOC. Then, upon identification of the location and the subject, the NTOC would process the TTL and contact the responsible law enforcement agency directly. The local field office and the fusion center with responsibility for the area (if that fusion center is participating in the TTL program) would be cc'd by the local field office.[4]
3. For a TTL located in a foreign country, the social media companies should submit the TTL report directly to the FBI NTOC. Then, upon identification of the location and subject, the NTOC would contact the legal attaché (legat) for that jurisdiction and refer the TTL.

C. Working together, the primary and secondary entities must provide 24/7/365 support for TTL collection/receipt, triage, analysis, dissemination, and feedback. Many fusion centers, real-time crime centers, Regional Information Sharing System (RISS) Centers, and other regional or major metropolitan law enforcement agencies have the capabilities needed to support these processes, handle coordination, and follow up on imminent/immediate threats. For further information, refer to Section III.

1. The criminal intelligence analysts of these entities will attempt to identify the subject(s) making the threat(s) and initiate reporting to the appropriate federal and SLTT organization or foreign law enforcement agency and then follow up with the appropriate fusion center.[5]
2. If, however, self-harm is involved, then the regional node would not share such information with other fusion centers for information sharing or intelligence purposes; the regional node should share such information with other fusion centers

[4] It should be noted, however, that the FBI NTOC does not dual-route a TTL without a subject, victim, or witness to avoid placing an added burden on the SLTT partner (i.e., if the NTOC cannot identify a subject, victim, or witness through its vetting/assessment, it does not dual-route but rather sends the TTL directly to the appropriate field office).
[5] Further discussion, training, and coordination with social media companies is needed regarding the completeness of the TTLs they report. Training is also necessary to ensure that law enforcement gets the information needed to process the TTLs reported by social media companies and to help social media companies refine and improve their internal reporting processes.

only for purposes of emergency response and should make this determination on a case-by-case basis.

3. The secondary entities would provide backup during off-hours.

D. Upon receipt of a TTL incident, criminal intelligence analysts working at the primary or secondary entity would handle the intake, analysis, dissemination, and feedback.

1. An online submission process would be used for the intake of the TTL incident.
2. The intelligence analysts would:
   a. Review the details of the incident.
   b. Attempt to identify the subject(s) making the threat(s) and relevant location information.
   c. Conduct preliminary database checks, to include deconfliction.
   d. Evaluate whether the information received by the social media companies is sufficient or, if it is insufficient, assess whether submitting an Emergency Disclosure Request is appropriate under applicable federal or state law.[6]
   e. Evaluate whether the incident constitutes a TTL, as defined in the Standard Operating Procedures (SOPs).
      i. If so, the intelligence analysts at the regional node would identify the agency with the investigative lead and would disseminate the deconflicted TTL to that agency and to other relevant partners (including the appropriate fusion center for the AOR where the threat was located).[7]
      ii. If the incident involves federal violations of law or is of federal investigative interest, then the intelligence analysts would send it to the local FBI field office for triage and/or deconfliction.
      iii. If the incident qualifies as an Information Sharing Environment-Suspicious Activity Report (ISE-SAR), the intelligence analysts at the regional node would submit the report to the eGuardian SAR Data Repository (SDR).[8]
   f. Seek information on the disposition of the TTLs from the federal or SLTT law enforcement entity or foreign law enforcement agency and provide feedback,[9] as appropriate, to the social media corporate partner using the portal.
3. The collection, triage, analysis, dissemination, and feedback related to TTLs will comply with applicable privacy, civil rights, and civil liberties laws, regulations, and policies.

---

[6] 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 (TLO) 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 USC § 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").

[7] To identify the appropriate lead investigative agency and obtain the correct phone number, criminal intelligence analysts may use PSAPs or the internet.

[8] Only a small percentage of TTLs rise to the level of an ISE-SAR, as that term is defined in the ISE-SAR Functional Standard v. 1.5.5.

[9] Refer to footnote 1 for an explanation of the term "feedback."

III. Requirements and Capabilities of Primary and Secondary Entities

A. 24/7 support or reliable backup for the receipt, triage, and dissemination of a TTL reported by a social media company

B. Proven record of coordination and collaboration

C. Access to NCIC and relevant criminal history databases

D. Resources
   1. System requirements
      a. Fusion centers, RISS Centers, and real-time crime centers serving as the primary entities could leverage the current IT infrastructure, but they would need to build an intake system for TTLs.
   2. Staffing requirements for regional nodes
      a. At a minimum, one supervisor and approximately two to three criminal intelligence analysts dedicated to TTL per shift would be needed.
   3. Access to the resources would be needed to conduct appropriate law enforcement indices checks for criminal history, firearms registrations (where available), and calls for service.

E. Familiarity with the eGuardian system (*Recommended*)

F. Knowledge of applicable state law governing EDRs

G. Willingness to adopt and implement uniform standard operating procedures to ensure a seamless flow of TLTTLs, in a manner consistent with applicable laws, regulations, policies, and procedures. See *Threat to Life (TTL) Reporting Initiative: Template for the Standard Operating Procedures (SOP) for Criminal Intelligence Sharing Nodes*; *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*.

H. Access to appropriate training on the TTL process for criminal intelligence analysts and supervisors
   1. Analysts should receive ongoing training on topics such as open source intelligence; how to handle exigencies (including threat triage methodology); legal process relating to EDRs; privacy, civil rights, and civil liberties protections; and applicable SOPs and policies.
   2. Social media companies should receive training on the definition of TTL, the process for reporting a TTL to the regional hub and threat triage methodology.
   3. Public Safety Answering Point (PSAP) partners should receive training on the TTL process and their role in the process.

Appendix I

Currently, 26 field offices with 23 SLTT partners have successfully implemented dual routing. As of late February 2021, more than 1,000 TTLs have been dual routed from the FBI to the participating field offices and SLTT partners listed below:

FBI Field Offices (26)

1. Albany
2. Albuquerque
3. Atlanta
4. Buffalo
5. Chicago
6. Cincinnati
7. Cleveland
8. Denver
9. Detroit
10. Kansas City
11. Knoxville
12. Little Rock
13. Memphis
14. Minneapolis
15. New Orleans
16. Newark
17. Oklahoma City
18. Philadelphia
19. Pittsburgh
20. Richmond
21. Sacramento
22. Salt Lake City
23. San Antonio
24. San Diego
25. San Francisco
26. St. Louis

SLTT Agencies (23)

1. (LR) Arkansas State Fusion Center (ASFC)
2. (SC) California Highway Patrol (ENTAC)
3. (SF) Northern California Regional Intelligence Center (NCRIC)
4. (SD) San Diego Law Enforcement Coordination Center (SD-LECC)
5. (DN) Colorado Information Analysis Center (CIAC)
6. (AT) Georgia Information Sharing Analysis Center (GISAC)
7. (CG) Crime Prevention and Information Center (CPIC)
8. (NO) Louisiana State Analysis and Fusion Exchange (LA-SAFE)
9. (DE) Michigan Intelligence and Operations Center (MIOC)

10. (MP) Minnesota Fusion Center (MNFC)
11. (KC) Missouri Information Analysis Center (MIAC)
12. (NK) New Jersey Regional Intelligence and Operations Center (NJ-ROIC)
13. (AQ) New Mexico State Police (*This is not a fusion center*)
14. (AL & BF) New York State Intel Center (NYSIC)
15. (CI & CV) Ohio State Hwy Patrol (OH-STACC)
16. (OC) Oklahoma Information Fusion Center (OIFC)
17. (PH) Delaware Valley Intelligence Center (DVIC)
18. (PH & PG) Pennsylvania Criminal Intelligence Center (PACIC)
19. (KX & ME) Tennessee Fusion Center (TFC)
20. (SA) Texas Fusion Center (TXFC)
21. (SU) Statewide Information and Analysis Center (SIAC)
22. (RH) Virginia Fusion Center (VFC)
23. (PG) West Virginia State Police (WVSP) (*This is not a fusion center*)

The majority of dual-routed TTLs fall into the following general categories:

- Violent threats (to include interstate threatening communications) to murder/kill/harm
- Potential school/workplace/mass shooting or violence
- Domestic violence/kidnapping
- Crimes/threats against minors
- Human/sex trafficking
- Firearms/ammunition-related/bomb threats
- Threats directed towards faith-based organizations
- Threats directed towards law enforcement/government/public officials
- Threats directed towards prominent public figures/businesses
- Mental health/suicidal ideation
- Threats to First Amendment-protected events or mass gatherings
- Violent criminal unrest/riots
- Election/political-related threats (excluding lawful political rhetoric)
- Other