Tips and Leads Issue Paper

Global Justice Information Sharing Initiative

♦

Intelligence Working Group

♦

Privacy Committee

October 2007

Bureau of Justice Assistance

Tips and Leads Issue Paper

Introduction and Background

The events of September 11, 2001, like no others, have made the average American aware that law enforcement, public safety, and private sector agencies should collect and share information to make our country a safer place for all its citizens and visitors. Conversely, the public is concerned about what types of information are being collected and stored by law enforcement, and when and how that information is being used and shared, raising concerns about the potential for civil liberty and privacy abuses.

Law enforcement officials require an array of information to effectively detect and investigate criminal and terrorism activity. Information comes to law enforcement agencies through a number of horizontal and vertical channels (e.g., dispatch, criminal investigations, the public, other law enforcement agencies, arrests, and incident reports), and many standards have been established for its maintenance and use. Unfortunately, not all information fits neatly into an already established category. In many cases, it is unclear whether information is useable or meaningful, requiring law enforcement officials to further investigate, analyze, and evaluate the data to determine its accuracy and potential usefulness. Currently, state, local, and tribal agencies lack the guidance and standards for this "gray area" of information.

In furtherance of the recommendations in the *National Criminal Intelligence Sharing Plan*[1] (NCISP), the Privacy Committee of the Global Intelligence Working Group (GIWG) developed this issue paper to provide guidance to state, local, and tribal law enforcement agencies regarding the handling of information received as a result of tips, leads, and suspicious incidents.

The NCISP emphasizes that credible information can result only from information that has been evaluated and used to draw conclusions. Yet it recognizes that the collection and use of such information can affect the fundamental rights of individuals. The NCISP offers an effective approach to protecting privacy and civil liberties by supporting training and policies that eliminate unnecessary discretion in the decision-making process. The GIWG Privacy Committee strongly supported this approach when developing guidance for handling tips and leads data.

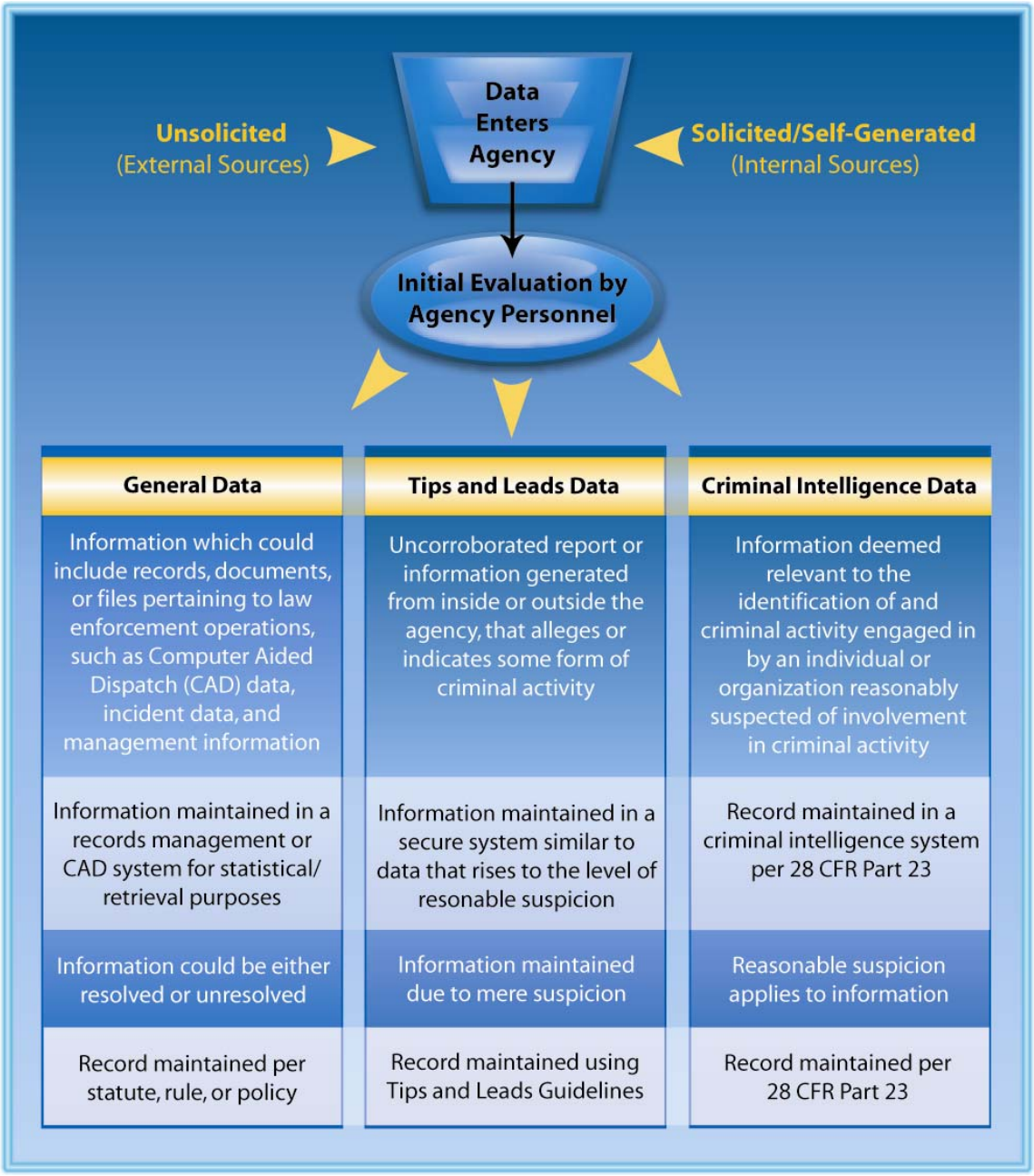
Tips and leads data are not criminal intelligence as defined by 28 Code of Federal Regulation (CFR) Part 23. However, law enforcement officials recognize the need to protect this type of information and protect individuals' privacy and civil liberties. Accordingly, this issue paper was prepared to provide guidelines on collecting, maintaining, retaining, disseminating, and purging

[1] Recommendation 9 of the *National Criminal Intelligence Sharing Plan* states that "in order to ensure that the collection/submission, access, storage, and dissemination of criminal intelligence information conforms to the privacy and constitutional rights of individuals, groups, and organizations, law enforcement agencies shall adopt, at a minimum, the standards required by the Criminal Intelligence Systems Operating Policies Federal Regulation (28 CFR Part 23), regardless of whether or not an intelligence system is federally funded."

tips, leads, and suspicious incident information. As recommended in the NCISP, agencies should develop privacy policies incorporating the guidance provided herein.

Law Enforcement Information Production

Information received by law enforcement agencies can be categorized into three general areas, as depicted in the diagram below:



Common practice involves the validation of information by agency personnel upon receipt. Data is categorized as unsubstantiated or uncorroborated after attempts to validate or

determine the reliability of the information fail (middle column above). Frequently, the agency feels the information should be kept for potential connections in the future but does not know how the data should be handled, where it should be stored, or when it should be disseminated.

> An agency's privacy policy should . . . acknowledge and address important issues that currently are not included in some criminal intelligence policies. For example, the policy should acknowledge the existence of information that is received or possessed by law enforcement agencies that does not rise to the level of "reasonable suspicion of criminal activity" and provide guidance on how to process that information. Often, this information—sometimes referred to as a "temporary" or "working" file—is received unsolicited by law enforcement agencies and cannot simply be dismissed.[2]

It is this type of temporary or working-file information—commonly known as tips and leads information—that is addressed in this issue paper.

The Importance of State, Local, and Tribal Involvement in the National Information Sharing Environment

As previously indicated, law enforcement agencies deal with tips, leads, and suspicious data on a daily basis. Although this information in and of itself may not be indicative of a potential crime, when collated and analyzed with correlating pieces of data from other sources, the information may be key in the prevention of a criminal act, including a potential act of terrorism. It is imperative that state, local, and tribal line-level officers realize the vital role they play in the preliminary receipt and investigation of this information and the potential impact it may have on an ongoing criminal or terrorism investigation.

As acknowledged in the *Information Sharing Environment (ISE) Implementation Plan*, the needs of state, local, and tribal governments continue to mount as these governments incorporate counterterrorism and homeland security activities into their day-to-day missions. Specifically, they need to ensure that personnel protecting local communities from a terrorist attack—or responding to an attack—have access to timely, credible, and actionable information and intelligence regarding individuals and groups intending to carry out attacks within the United States (including homegrown terrorists), their organization and financing, at-risk potential targets, preattack indicators, and other major events or circumstances requiring action by state, local, and tribal governments.[3]

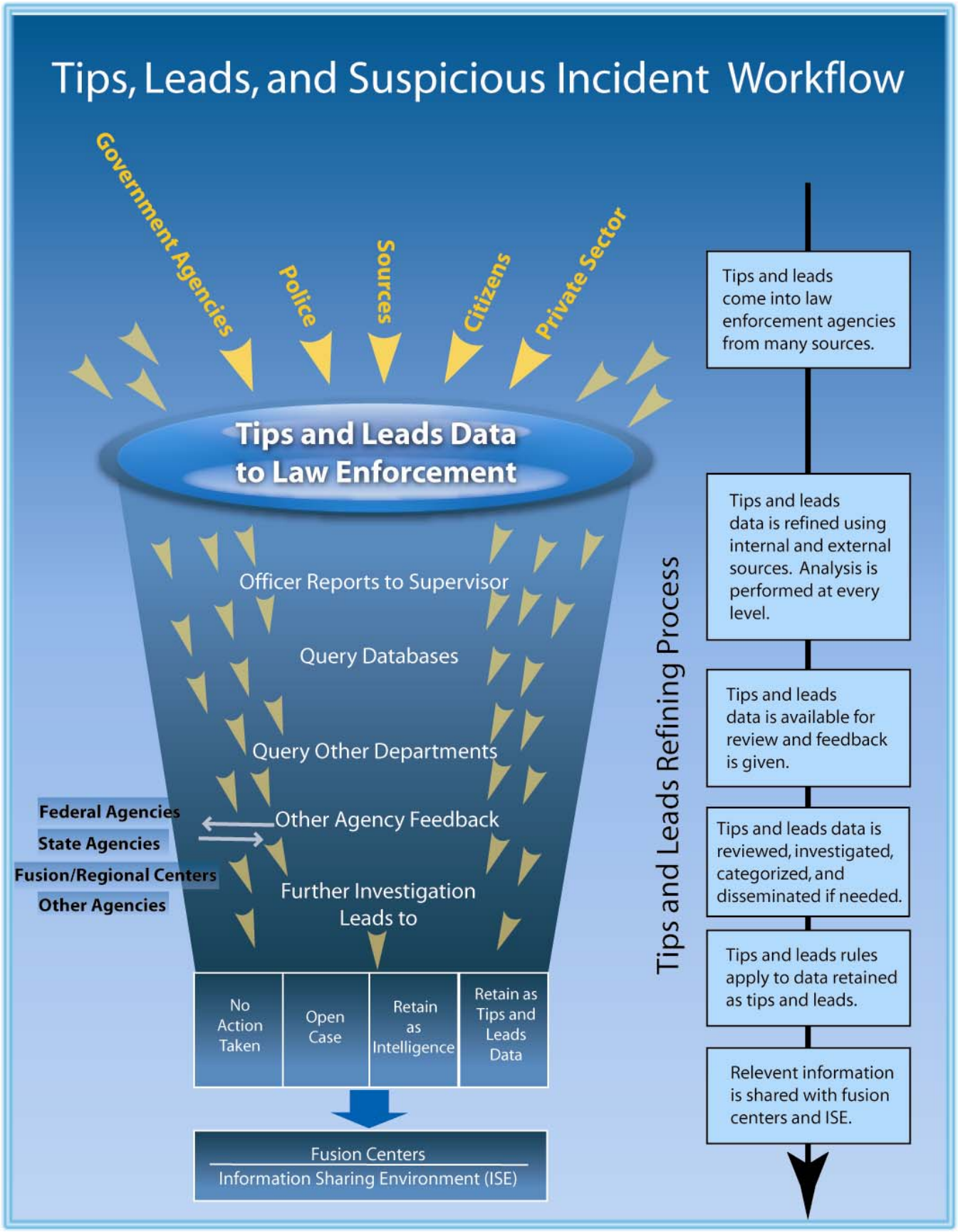
The federal government is promoting the establishment of a nationwide integrated network of state and major urban area fusion centers to facilitate effective terrorism information sharing with state, local, and tribal law enforcement agencies, and as of August 2007, more than 40 states have created fusion centers. The principal role of the fusion center is to compile, analyze, and disseminate criminal and terrorist information and intelligence, as well as other

[2] NCISP, page 6.
[3] Information Sharing Environment Implementation Plan, November 2006, page 18.

information, to support efforts to anticipate, identify, prevent, and/or monitor criminal and terrorist activity. Consistent with their respective roles and responsibilities, the federal government will provide terrorism information to state, local, and tribal authorities primarily through these fusion centers. Conversely, the ISE Implementation Plan indicates that statewide and major area fusion centers will ensure that locally generated terrorism information is communicated to the federal government.[4]

It may be difficult to determine whether a single incident occurring within a local jurisdiction has a nexus to terrorism, but it is important to acknowledge that many outwardly unrelated tips, leads, and suspicious incidents may in fact be related and could have multijurisdictional and national implications when analyzed, shared, and combined with other seemingly unrelated information at the local, state, regional, and federal levels. Terrorist activities are being funded via local-level crimes, and state, local, and tribal law enforcement officers in our communities are best positioned not only to observe criminal and other activity that might be the first signs of a terrorist plot but also to help thwart attacks before they happen. The following graphic depicts a suggested workflow process for tips, leads, and suspicious data as it enters an agency. It outlines a refining process that includes assessment, analysis, review, categorization, and dissemination, if appropriate, to local, state, regional, and federal agencies and fusion centers in furtherance of the national information sharing environment.

[4] Ibid. Page 75, Chapter 7, Implementation Action 2.21.


Tips, Leads, and Suspicious Incident Workflow
Government Agencies
Police
Sources
Citizens
Private Sector
Tips and Leads Data to Law Enforcement
Officer Reports to Supervisor
Query Databases
Query Other Departments
Other Agency Feedback
Further Investigation Leads to
Federal Agencies
State Agencies
Fusion/Regional Centers
Other Agencies
No Action Taken
Open Case
Retain as Intelligence
Retain as Tips and Leads Data
Fusion Centers
Information Sharing Environment (ISE)
Tips and Leads Refining Process
Tips and leads come into law enforcement agencies from many sources.
Tips and leads data is refined using internal and external sources. Analysis is performed at every level.
Tips and leads data is available for review and feedback is given.
Tips and leads data is reviewed, investigated, categorized, and disseminated if needed.
Tips and leads rules apply to data retained as tips and leads.
Relevent information is shared with fusion centers and ISE.

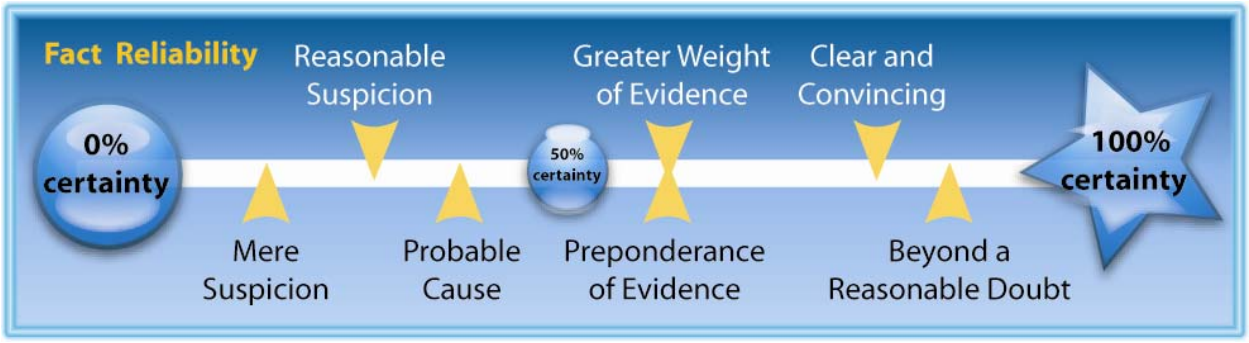
The GIWG Privacy Committee recommends that every state, local, and tribal law enforcement agency should incorporate a tips, leads, and suspicious incident refining process into its daily operations and provide appropriate training for personnel involved in the process.

Definition of Tips and Leads

The GIWG Privacy Committee defines tips and leads information as an uncorroborated report or information that alleges or indicates some form of possible criminal activity. Tips and leads can also be referred to as suspicious incident reports (SIRs) or suspicious activity reports (SARs). Tips and leads information does not include incidents that do not have an offense attached, criminal history records, records management data, or Computer Aided Dispatch (CAD) data.

A tip or lead can result from a variety of sources including, but not limited to, the public, field interview reports, and anonymous or confidential sources. This information has some suspicion or mere suspicion attached to it, but without further inquiry or analysis it is unknown whether the information is accurate or useful. Unlike intelligence information that has undergone an evaluation process to determine the likely possibility that the information is accurate, tips and leads information hangs between being of no use to law enforcement and being extremely valuable if time and resources are available to determine its meaning.

Across a spectrum for levels of suspicion, information ranges from no suspicion to fact. Mere suspicion information (tips and leads) falls short of any established national standards used by law enforcement.



Each agency must make a determination of the types of data that will be categorized as tips and leads. The criteria for collecting and labeling information as a tip or lead should be clearly articulated in each agency's privacy policy. Following are specific areas that should be addressed when developing a privacy policy that incorporates tips and leads data:

Collection

Tips, leads, and suspicious incident data are collected in a variety of ways. They can be received or obtained through unsolicited information that the public provides; from confidential/anonymous sources; from the media and other law enforcement, public safety, or regulatory agencies; or from analysis of information. Tips and leads data can also be solicited

or self-generated information, received from the public in response to law enforcement officers' requests for information about a certain crime. However the information is received, it has not been validated for truthfulness, accuracy, or reliability of the source—determinations that aid law enforcement in deciding whether the information is credible and has value.

Controls

Similar to the intelligence process detailed in the NCISP,[5] tips and leads information should be subjected to an assessment process to determine its credibility and value. The GIWG Privacy Committee determined that appropriate controls should be recommended for each step of that process:

> Receipt/Collection—At the time of receipt or collection, tips and leads data should be assessed and reviewed, using supporting information if available, for sensitivity and confidence. An attempt should be made to validate or refute the information provided by a tip or lead. Collection of purely First Amendment activity information should be prohibited.
>
> Storage—Storage of tips and leads information should be handled similarly to data that rises to the level of reasonable suspicion. Those requirements should include an audit and inspection process, supporting documentation, and logical separation or labeling of the data from other information.
>
> Access—Because of the uncertainty about what the information says or how credible it is, it is recommended that access to tips and leads data should be handled similarly to access to data that rises to the level of reasonable suspicion. Access should be allowed only where there is a need to know and a right to know the information in the performance of a law enforcement, homeland security, or public safety activity. Law enforcement agencies may want to implement a process whereby access is role-based.
>
> Dissemination—Tips and leads information, if systematically collected and stored for interagency distribution, should be disseminated primarily in response to an inquiry, and only for law enforcement, homeland security, and public safety purposes. For example, uncorroborated tips and leads information should not be regularly disseminated in bulletins and other like products. However, it may be included in secure information databases and disseminated to relevant law enforcement, homeland security, and public safety agencies that have the need to know and right to know the information in the performance of a law enforcement activity and to such agencies and other government or nongovernment organizations or individuals when credible information indicates potential imminent danger to life or property.

[5] Intelligence Process graphic, NCISP, page 3.

Retention—The retention period for tips and leads information should be long enough for an agency to work a tip and lead to determine its credibility and value. Agencies may consider articulating the need to retain tips, leads, or suspicious incidents for longer periods of time to access and conduct analysis on the data for national security purposes. Tips and leads should have a "disposition" label so an inquirer knows the status and purpose for the retention. Disposition labels might include "undetermined/unresolved" or "cleared/unfounded." Different disposition labels may indicate different retention periods, with "cleared/unfounded" tips and leads information being retained for a shorter time than "undetermined/unresolved" tips and leads. Agencies should also consider the need for maintaining tips and leads data for purposes of statistical reporting and performance measurement when setting retention and purge procedures.

Security—It is recommended that physical and electronic security measures be similar to those used for information rising to the level of reasonable suspicion.

Current Efforts and Promising Practices

The information below describes three current efforts that address a process for handling tips and leads information:

- **U.S. Attorney General's Guidelines on General Crimes, Racketeering, and Terrorism Enterprises** (Attorney [AG] Guidelines) (U.S. Department of Justice [DOJ], 2002) offer one model for authorized information gathering in response to tips and leads information. The AG Guidelines recognize three levels of investigative activity: (1) the "prompt" and "extremely limited" (neither of which is further defined in the Guidelines) checking of initial leads, (2) preliminary inquiries, and (3) full investigations.

  The **checking of initial leads** is undertaken whenever *information is received of such a nature that some follow-up as to the possibility of criminal activity is warranted.* This is a limited activity conducted with an eye toward determining whether further investigation is warranted. The next level, a **preliminary inquiry**, is undertaken when the information developed or the nature of the information received (reliable source, imminent threat) indicates *the possibility of criminal activity* and whose *responsible handling requires some further scrutiny* beyond checking initial leads. Mail opening and nonconsensual electronic surveillance are prohibited investigative techniques in the checking of initial leads or the conduct of a preliminary inquiry. They also require supervisory approval, written documentation of the allegation or other information that is deemed to warrant the approval, and completion within 180 days, with no more than two extensions of up to 90 days available with approval of the Special Agent in Charge. Any further approvals of extensions are subject to Federal Bureau of Investigation (FBI) headquarters approval. Where the checking of initial leads fails to disclose sufficient information to justify a preliminary inquiry or an investigation or a preliminary inquiry fails to disclose sufficient

information to justify an investigation, activity on the case must be immediately terminated and a record made of the closing.

Where a checking of initial leads or a preliminary inquiry produces *facts or circumstances that reasonably indicate that a federal crime has been, is being, or will be committed*, a **general crimes (full) investigation** may be initiated using the full panoply of lawful investigative techniques. Parallel standards are used to authorize criminal intelligence and racketeering enterprise investigations. All investigations must be based on a *reasonable factual predicate* and have a *valid law enforcement purpose.* In determining reasonable indication, the agent may take into account facts or circumstances that a prudent investigator would consider. There must be an objective, factual basis for initiating the investigation (more than a hunch but less than reasonable suspicion or probable cause).

Finally, the AG Guidelines permit information collected during the checking of initial leads, preliminary inquiries, and investigations to be disseminated freely within the DOJ and to state, local, and federal criminal justice agencies when the information: (1) falls within the investigative or protective jurisdiction or litigative responsibility of the agency; (2) may assist in preventing a crime or the use of violence or any other conduct dangerous to human life; or (3) is required to be furnished by Executive Order, statute, interagency agreement, or Presidential Directive. (These criteria reflect basic need-to-know and right-to-know standards). The FBI maintains a database that permits prompt retrieval of information on the status (open or closed) and subjects of all inquiries and investigations.

- **Georgia Information Sharing and Analysis Center (GISAC)** method for handling tips, leads, and suspicious incident data is a comprehensive refining process that details how multiple agencies can work together to address and properly handle this type of data.

  Receipt of Leads/Tips: GISAC receives tips from law enforcement agencies via the Georgia Terrorism Tip-Line, a joint GISAC and Federal Bureau of Investigation (FBI) call center, and through calls directly to agents assigned to GISAC. Through the Georgia Terrorism Intelligence Project (GTIP), GISAC receives and disseminates lead information through a direct link to 11 other local law enforcement agencies in the metro-Atlanta area, and throughout the state via a Web-based lead tracking system called E-Team. To aid in deconfliction between GISAC and the Atlanta FBI, GISAC provides the FBI with access to E-Team, through which the FBI monitors all GISAC leads and enters any leads from its Guardian system.

  As a matter of design, GISAC chose to educate and include other state and local law enforcement agencies in collecting threat/suspicious activity information by obtaining identifiers and other pertinent details and reporting the information to GISAC. Personnel at GISAC ensure that the information is evaluated, investigated, and forwarded where it needs to go for additional investigation or prosecution. All identified individuals are checked through state and local databases as well as through the FBI's intelligence system. In

addition, GISAC ensures that the law enforcement officers who provide the information receive follow-up calls with results of the tips or leads, even if the results are negative. GISAC takes calls from the public but does not advertise a public telephone number for reporting suspicious activity. This procedure is followed for a couple of reasons:

1) Local 911 services and police agencies will most likely receive calls first. If a call is regarding an emergency or if immediate action is required, local authorities are in a position to address the situation.

2) When citizens call 911, the local police authorities are included in the information flow. Local officers are closer to the community and know whether something is normal or unusual.

Through education, police agencies and/or 911 centers are advised to call GISAC with suspicious information, no matter how nonthreatening it may seem. GISAC collects the information and evaluates it. Citizens are able to report suspicious activity online through the Georgia Office of Homeland Security's Web site. They are clearly instructed to call 911, or the caller's local law enforcement agency, for reports requiring immediate attention.

Documentation of Leads: Each tip or lead received by GISAC is recorded into E-Team and assigned for follow-up by a GISAC supervisor. Leads may be assigned to a GISAC agent, tasked out to a Georgia Bureau of Investigation (GBI) regional office, or sent to an intelligence analyst for further review and to assess the credibility and significance of the information. All leads received by GISAC are reported to the FBI/Joint Terrorism Task Force (JTTF) to aid in deconfliction and to determine whether the leads warrant FBI/JTTF involvement.

After a lead is assigned to an agent, the appropriate investigative measures are taken to proceed with the lead. If further intelligence information is needed, the agent contacts an analyst assigned to GISAC for assistance. GISAC has six criminal intelligence analysts, one analyst from the Georgia Department of Corrections, and two Georgia Emergency Management Agency representatives dedicated solely to the homeland security mission. Analysts have access to various databases including the Georgia Department of Labor, Secretary of State, Georgia Crime Information Center, and Georgia Department of Revenue. In addition, all analysts have access to public records, FBI intelligence indices, and GBI intelligence systems. Throughout this process, all activity and intelligence checks conducted by agents and analysts are recorded in E-Team for documentation. Intelligence data is not entered onto E-Team because of its wide accessibility; instead it is delivered directly to the agent assigned to the lead. The assigned agent updates the lead and passes it on to a GISAC supervisor, who decides whether the lead can be closed with no further investigation or warrants opening a full investigation. Tips and leads that are opened to investigation are recorded in FBI and/or GBI case management systems as case or intelligence investigations. Information that is compliant with 28 CFR Part 23 is also recorded in GBI's intelligence

system. All tips and leads recorded into E-Team, even closed leads, are archived within E-Team and are available for retrieval or queries for future relevance.

Dissemination of Leads: All agencies with access to E-Team are able to review updates to tips and leads as they are developed. If dissemination outside the agencies with access to E-Team is required, GISAC will determine the target audience and develop a report accordingly. GISAC and FBI work jointly on these products to ensure that all information that can be disseminated is shared.

- **Florida's Intelligence System's Operating Guidelines:** State laws and policies are likely to significantly affect how tips and leads and other investigative information are received, investigated, stored, and disseminated. Dissemination must consider the right of the public under State Sunshine Laws to obtain information in public records that pertains to them. A good example is **Florida's Public Records Statute** (Chapter 119, Sections 119.01–119.19, 2004). The statute broadly defines *criminal intelligence information* to mean "information with respect to an identifiable person or group of persons collected by a criminal justice agency in an effort to anticipate, prevent, or monitor possible criminal activity" (Sec. 119.011 (3) (a)). *Criminal investigative information* is defined to mean "information with respect to an identifiable person or group of persons compiled by a criminal justice agency in the course of conducting a criminal investigation of a specific act or omission, including, but not limited to, information derived from laboratory tests, reports of investigators or informants, or any type of surveillance" (Sec. 119.011 (3) (b)). Section 119.07 (6) (b) 1 exempts "active" criminal intelligence information and "active" criminal investigative information from the law's public inspection and copying requirements. The statute defines *criminal intelligence information* as "active as long as it is related to intelligence gathering conducted with a reasonable, good faith belief that it will lead to detection of ongoing or reasonably anticipated criminal activities" and *criminal investigative information* as "active as long as it is related to an ongoing investigation which is continuing with a reasonable, good faith anticipation of securing an arrest or prosecution in the foreseeable future" or where "directly related to pending prosecutions or appeals" (Sec. 119.011 (6) (d) 1 and 2). This statutory scheme is carefully reflected in the **Florida Intelligence System's Operating Guidelines** (Florida Guidelines) (May 2005), including the treatment of tips and leads information. The Florida Guidelines establish a dissemination protocol in Part IV.I that must be followed to disseminate system information to other members of the criminal justice community, including need to know/right to know and a detailed procedure for "third agency" dissemination under a "Third Agency Rule." One system information module, for tips and tasks, is used to capture the tips and leads received by law enforcement agencies. This information must be reviewed within 90 days after entry to make a determination of its status. Tips and leads information that is determined not to be valid must be purged from the system. Valid information, unless subsequently substantiated, must be purged from the system within two years of entry (Part XII.B and E.4).

While tips and leads information may qualify under Florida's statutory definition as "criminal intelligence information," it would not be considered "criminal intelligence information" under the definition of the term adopted by the NCISP, 28 CFR Part 23, and the academic and professional authorities cited herein. This illustrates why it is critical to consult state statutes and policies when establishing operational guidelines and policies for intelligence and information sharing.