GEORGIA BUREAU OF INVESTIGATION
INVESTIGATIVE DIVISION

DIRECTIVE 7-6

TITLE: Criminal Intelligence Operations and Privacy Protections

---

DATE: March 1, 1998 **PAGE 1 OF 21**

REVISION DATE: May 9, 2012

REVIEW DATE: April 19, 2012

AUTHORITY: R.E. Andrews
Deputy Director for Investigations

PURPOSE: To outline operating procedures and privacy protections for criminal intelligence systems maintained by the Georgia Bureau of Investigation (GBI) and define other operational capabilities of the GBI Intelligence Unit.

General

The GBI operates an intelligence system within the Georgia Information Sharing and Analysis Center (GISAC). GISAC is managed and supervised by a GBI Special Agent in Charge (SAC). The SAC is responsible for the overall operation of the unit, its intelligence systems, operations, information collection and retention procedures, coordination of assigned personnel and adherence to the privacy policy by all unit personnel. GBI criminal intelligence analysts assigned to the GISAC collect, evaluate, analyze and disseminate criminal intelligence information regarding criminal activity. Additionally, the GISAC has criminal intelligence analysts assigned to collect, evaluate, analyze and disseminate suspicious activity reports (SAR) derived from information reasonable indicative of potential terrorist activity. While performing these crucial tasks, it is essential that all participating system users, to include GISAC personnel and support contractors, protect the privacy, civil rights and civil liberties of the citizens of Georgia and the United States by complying with the requirements of Title 28, Part 23 of the Code of Federal Regulations (28 CFR Part 23) and the policies and procedures outlined in this directive.

Definitions

Criminal Intelligence Analyst: Collects, analyzes, organizes and performs analysis of data to support the investigative efforts of law enforcement and to forecast crime trends, activities and events. A Criminal Intelligence Analyst will review, research, and disseminate requests for information pertaining to law enforcement activity for local, state and federal law enforcement agencies. A Criminal Intelligence Analyst can be assigned to any work unit within the agency and perform tasks based on the function of that work unit.

Criminal Intelligence Collection Criteria: Guidelines set forth in 28 CFR Part 23 which identify the types of information that may be collected and retained in a Criminal Intelligence System.

Criminal Intelligence Information: Data which meets criminal intelligence collection criteria and which has been evaluated and determined to be relevant to the identification of individuals who or organizations which are reasonably suspected of involvement in criminal activity.

Criminal Intelligence System: The equipment, facilities, and procedures used for the receipt, storage, dissemination, and analysis of criminal intelligence information.

General Data: Information which, after evaluation, does not meet the collection criteria for criminal intelligence or suspicious activity reporting.

Georgia Information Sharing and Analysis Center (GISAC): A multi-discipline public safety Information and Analysis Center (ISAC) or "fusion center" with membership including but not limited to fire services, local law enforcement, homeland security, emergency management and other appropriate disciplines as determined by the Director of the Georgia Office of Homeland Security in consultation with the GBI Director. It is an "all crimes" fusion center maintaining a terrorism component that operates under the direction of the GBI.

Need to Know: When information requested by any member of a participating agency will aid in the investigation of current criminal activity.

Participating Agency: Any criminal justice agency of a city, county, state, or a federal government unit which exercises law enforcement or criminal investigation authority and is authorized to receive criminal intelligence information.

Privacy Officer: Appointed by the GBI Director to be responsible for privacy, civil rights, and civil liberties issues (including accessing and sharing terrorism-related information through the Information Sharing Environment), policy development, policy compliance, the coordination of privacy training related to all GBI Intelligence operations, and the security of information systems. The Privacy Officer will receive specialized training in these areas of responsibility.

Reasonable Suspicion: "Reasonable Suspicion" or "criminal predicate" is established when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise.

Request: An inquiry for information available through the GBI Criminal Intelligence Unit. (The requester must provide a reason for the query that meets criminal intelligence collection criteria.)

Right to Know: Any member of a participating agency who has the authority to receive intelligence information when the information received will aid in the investigation of current criminal activity.

Suspicious Activity Report/Suspicious Incident Reporting: Official documentation of observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity. Suspicious activity reports (SARs) offers a standardized means for feeding information repositories or data analysis tools. Patterns identified during SAR information analysis may be investigated in coordination with the reporting agency and, if applicable, a state or regional fusion center. SAR information is not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor is it designed to support interagency calls for service.

SAR Submission: Generally an uncorroborated report or information generated from inside or outside a law enforcement agency that alleges or indicates some form of possible terrorist activity.

A SAR submission may come from a variety of sources, including, but not limited to, the public, field interview reports, and anonymous or confidential sources. This information may be based on mere suspicion or on a level of suspicion that is less than "reasonable suspicion" and, without further information or analysis, it is unknown whether the information is accurate or useful. A SAR submission falls

between being of little or no use to law enforcement and being extremely valuable depending on the availability of time and resources to determine its meaning.

SAR Vetting Tool (SVT) – The computer based program used for the receipt, storage, and analysis of Suspicious Activity Reports.

I. Criminal Intelligence System Operations

The purpose of the Criminal Intelligence System maintained by GBI is to support the law enforcement efforts of the GBI and other participating criminal justice agencies in actively combating criminal activity by collecting, evaluating, analyzing and disseminating criminal intelligence information regarding criminal activity and potential terrorist activity. Criminal Intelligence Analysts maintain criminal intelligence information in the Criminal Intelligence System. The Criminal Intelligence System will be maintained in accordance with the following directives, which are based upon 28 CFR Part 23, in order to maintain the privacy, civil rights and liberties of all citizens.

A. Collection of Criminal Intelligence Information

Intelligence information will be collected through submissions from internal sources, such as GBI agents, and external sources, such as other law enforcement agencies or private citizens. GISAC will seek or retain information that:

1. Is based upon a criminal predicate or threat to public safety; or

2. Is based upon reasonable suspicion that an identifiable individual, regardless of citizenship or U.S. residency status, or organization has committed a criminal offense or is involved in or is planning criminal conduct or activity that presents a threat to any individual, the community, or the nation and the information is relevant to the criminal conduct or activity; or

3. Is relevant to the investigation and prosecution of suspected criminal incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime; or

4. Is useful in crime analysis or in the administration of criminal justice and public safety; and

5. Is reliable and verifiable or the limitations on the quality of the information are identified; and

6. Is collected in a lawful manner.

The GBI will not seek or retain information about:

1. Individuals or organizations solely on the basis of their religious, political, social views or activities;

2. Their participation in a particular non-criminal organization or lawful event; or

3. Their race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation.

The GBI will not directly or indirectly receive, seek, accept, or retain information from:

1. An individual or nongovernmental information provider who may or may not receive a fee or benefit for providing the information if there is reason to believe that the information provider is legally prohibited from obtaining or disclosing the information; or

2. A source that used prohibited means to gather the information.

Information gathering and investigative techniques used by GBI, GISAC, and the participating agencies will comply and adhere to the following regulations and guidelines regarding criminal intelligence information including 28 CFR Part 23 and the United States Department of Justice's National Criminal Intelligence Sharing Plan (NCISP). Agencies participating in and providing information are governed by the laws and rules governing those individual agencies, as well as by applicable federal and state laws. Techniques used by GBI, GISAC, and participating agencies will be the least intrusive means necessary in the particular circumstance to gather information it is authorized to see or retain.

B. Criminal Intelligence Information Submission Documentation

In order to be considered for submission into the criminal intelligence system, each submission must contain certain mandatory information and

that information will provide an audit trail to analyze criminal activity and for inspection purposes. Relevant information will be documented on a GBI Intelligence Report (see Attachment A). The originator of the information must make an independent determination as to the value of the information and the reliability of the source. All information must be clearly and accurately reported.

1. Internal Submissions

   The GBI Intelligence Report will be used by GBI personnel to document criminal intelligence information. The following information is required for submissions by GBI employees:

   a. Name of originator;
   b. Work unit of originator;
   c. Date of submission;
   d. Classification of information(Section I.C.3);
   e. Subject: The report should include identifying data of the subject, when possible, even if the information has previously been submitted to the intelligence system;
   f. Organization/Business (if applicable);
   g. Source: The source of the intelligence information must be identified by name and address or confidential source number;
   h. Rating: Source and information must be rated;
   i. Criminal Activity: Short description of the suspected criminal activity; and
   j. Summary: The report must clearly and accurately identify the suspected criminal activity. Reports will not contain information concerning an individual's racial, political, ethnic or sexual background or behavior unless such information has a bearing on criminal activity. This field may also be used to indicate legal restrictions on sharing of information based on information sensitivity or classification.

   GBI Intelligence Reports will be approved by the work unit supervisor. The supervisor will ensure that the report meets collection criteria and is properly classified. Once approved, the report will be forwarded to the GISAC for validation and inclusion into the system.

2. External Submissions

The following information is required for submissions by external sources such as other law enforcement and members of the public.

a. Date of submission
b. Name of originator
c. Criminal activity
d. Classification of information
e. Originator agency name and telephone number
f. Information relevant to the identification of individuals who or organizations which are reasonably suspected of involvement in criminal activity

3. Information Submitted That is Not Criminal Intelligence Information

GISAC may collect and investigate information that is based on reasonable suspicion of criminal activity. In the event that this information does not meet the criteria for inclusion in the Criminal Intelligence System, the information will be returned to the submitting agency with an explanation as to why it will not be included in the Criminal Intelligence System and the requirements for inclusion.

C. Evaluation and Classification of Information

1. Evaluation of Information

Upon receipt of information, criminal intelligence analysts will evaluate the information to determine if it meets the criteria for inclusion in the Criminal Intelligence System. Reports/submissions which do not meet collection criteria will not be accepted into the Criminal Intelligence System. Criminal intelligence analysts will verify the classification and/or category of the information, such as:

a. Whether the information is general data, criminal intelligence, or information reasonably indicative of terrorist activity;

b. The nature of the source of information, such as anonymous tip, protected source, etc.;

c. The reliability of the source of information:

(1) Highly Reliable

(2) Usually Reliable
(3) Fairly Reliable
(4) Unreliable
(5) Cannot Be Judged

d. The validity of the content:

(1) Confirmed True
(2) Probably True
(3) Possibly True
(4) Doubtfully True
(5) Cannot Be Judged.

In the event that the evaluation determines that the information is criminal intelligence information, the information will be classified.

The Intelligence Analyst Supervisor will be responsible for ensuring that intelligence reports and submissions received by the GISAC meet collection criteria and are properly classified before entering into the intelligence system. Intelligence reports and submissions which do not meet collection criteria will be returned to the work unit supervisor for review.

Supervisors of the GISAC and other work units having assigned criminal intelligence analysts will be responsible for ensuring that all intelligence reports and submissions created and/or evaluated by criminal intelligence analysts meet collection criteria and are properly classified before entry into the criminal intelligence system.

2. Classification Criteria

At the time a decision is made to retain information, it will be labeled pursuant to applicable limitations on access and sensitivity of disclosure in order to:

a. Protect confidential sources and police undercover techniques and methods;

b. Not interfere with or compromise pending criminal investigations;

c. Protect an individual's right of privacy and civil rights and civil liberties; and

d. Provide legally required protection based on the individual's status as a child, sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, or resident of a domestic abuse shelter.

3. Types of Classification

a. **Sensitive:** The classification for intelligence reports/submissions which document criminal activity by an elected or prominent public official will be classified as Sensitive. The report is maintained in the Intelligence database with access limited to GISAC Supervisors, Intelligence Analysts, Deputy Director for Investigations, and Inspectors. Other security features built within the database provide hit notifications to GISAC supervisors if the topic of a sensitive report is queried. Dissemination must be approved by the Deputy Director for Investigations or an Inspector.

This classification also includes Confidential Informants (CI). Information on CI's may only be released after authorization from the CI's controlling agent or work unit supervisor which supervises the CI. Access to CI information is limited to the controlling agent, supervising GBI Office supervisor and administrative staff, GISAC personnel, Deputy Director for Investigations and Inspectors.

b. **Classified:** The classification for intelligence reports/submissions which document criminal activity by law enforcement officers or governmental employees will be Classified. This classification includes information which, if released, may compromise an ongoing criminal investigation or identify a protected source. Information concerning juveniles is included in this classification. Reports received with this designation may not be disseminated without the permission of the originator or the originator's work unit supervisor.

c. **GBI Only:** The classification for intelligence reports/submissions which contain information which may not be disseminated outside of the GBI without the permission of the originator or the work unit supervisor will be classified as GBI Only.

d. **Law Enforcement Only:** The classification for routine intelligence reports/submissions which contain information that may be furnished to a participating agency upon request will be classified as Law Enforcement Only.

4. Review of Classification

The classification of existing information will be reevaluated whenever:

a. New information is added that has an impact on access limitations or the sensitivity of disclosure of the information; or

b. New information is added that has an impact on the confidence (validity and reliability) in the information; or

c. There is a change in the use of the information affecting access or disclosure limitations.

D. Analysis and Merging

Criminal Intelligence Information acquired by the GBI will be analyzed only by qualified criminal intelligence analysts who have successfully completed a GBI background investigation and obtained appropriate security clearances, if applicable.

The information acquired by the GBI or accessed from other sources is analyzed according to priorities and needs and will be analyzed to:

1. Further crime prevention to include terrorism, enforcement, prosecution objectives and priorities established by the GISAC; and

2. Provide tactical and/or strategic intelligence on the existence, identification and capability of individuals and organizations suspected of having engaged in or engaging in criminal activities.

Records about an individual or organization from two or more sources will not be merged unless there is sufficient identifying information to conclude that the information is about the same individual or organization. The set of identifiers sufficient to allow merging will consist of all available attributes that can contribute to higher accuracy of match.

If the matching requirements are not fully met, but there is an identified partial match, the information may be associated if accompanied by a clear statement that it has not been adequately established that the information relates to the same individual or organization.

E. Dissemination

1. Criminal intelligence information will be disseminated to law enforcement officials, public officials, and other individuals when such persons have a need to know and a right to know the information in the performance of their duties.

2. Nothing in this directive shall limit the dissemination of an assessment of criminal intelligence information to a government official or to any other individual when necessary to avoid imminent danger to life or property.

3. Information gathered and records retained by the GISAC will not be sold, published, exchanged, or disclosed for commercial purposes or disseminated to the public.

4. Criminal intelligence information, excluding information classified as Law Enforcement Only, will not be disclosed without prior notice to the contributing agency that such information is subject to dissemination.

5. Criminal intelligence information located in the Criminal Intelligence System will be disseminated only to users authorized by GBI.

6. Dissemination of information requested or submitted to the Intelligence Unit will be based on classifications as outlined under Section I, Subsection C, Paragraph 3, of this directive.

7. Information requested or submitted through the GISAC will be disseminated to the GBI work units in the jurisdiction of the request/submission if the classification is not “Sensitive” or “Classified”.

8. The capturing of certain mandatory information regarding requests for intelligence information will provide an audit trail to analyze criminal activity and for inspection purposes. For these reasons, the GBI will maintain a record indicating who has been provided information, the reason for release of the information and the date of dissemination. The GISAC supervisors are responsible for ensuring that proper

documentation is made of each request for intelligence information by participating agencies. The request for criminal intelligence information must be documented on an Intelligence Request Form (see Attachment B) and include the following information:

a. Date of request;
b. Name of requester;
c. Requesting agency/work unit;
d. Requesting agency/work unit telephone number; and
e. Criminal activity

9. With certain exceptions, the Georgia Open Records Act makes records maintained by state and local governments available to any member of the public upon request. 28 C.F.R. Part 23 restricts the dissemination of criminal intelligence information to law enforcement authorities only, except when there is an imminent threat to the public. The disclosure of criminal intelligence information would violate the regulatory framework of 28 C.F.R. Part 23 and constitute an invasion of privacy. Accordingly, the GBI will not disclose criminal intelligence information in response to a request under the Georgia Open Records Act under O.C.G.A. § 50-18-72(a)(1). Similarly the disclosure of Suspicious Activity Reports would also constitute an invasion of privacy and will not be disclosed in response to a request under the Georgia Open Records Act. With regard to general data that does not meet the criteria for inclusion in the Criminal Intelligence System or the Suspicious Activity Report Management System; the GBI will evaluate each request in accordance with the requirements of the Georgia Open Records Act, as articulated in GBI Policy.

F. Retention

All applicable information will be reviewed for record retention (validation or purge) every five years in accordance with electronically tracked review schedules, as provided by 28 CFR Part 23. When information is misleading, obsolete or otherwise unreliable, it will be purged, destroyed, deleted or returned to the submitting source. Permission to destroy or return information or records will be presumed if the applicable information is not validated within the specified time period. Notification of proposed destruction or return of records may or may not be provided to the contributor, depending on the relevance of the information and any agreement with the providing agency.

1. Criminal intelligence information and requests for information will be deleted (purged) from the Criminal Intelligence System periodically if, after holding the information for five years, no updated criminal activity has been documented.

2. Each entry into the Criminal Intelligence System will be evaluated on its own content and may be retained if it is the opinion of the supervisor that retention of the information serves a valid law enforcement purpose and the information has been updated to comply with the retention schedule.

3. A system generated message will be sent to the originating agent or the work unit supervisor the month prior to the information being purged from the Intelligence System. If the originator has current intelligence information indicating that the subject is currently involved in criminal activity, an updated intelligence submission will authorize GISAC to maintain the information for an additional five years.

4. Copies of intelligence information classified as "Sensitive" will not be returned to the originator, but will be updated by direct contact with the originator.

G. Security Safeguards

To ensure that there is no unauthorized access or damage to criminal intelligence information stored in the GISAC, administrative, technical and physical safeguards which comply with 28 CFR Part 23 will be established.

The Privacy Officer will serve as the security officer. The Privacy Officer will be responsible for coordinating appropriate training and compliance with this policy.

1. Computer System

   a. The Intelligence databases are maintained on an in-house database server. Access to the system is based on the user's affiliation with GBI Investigative Division through the GBI secured network or by using a Secure Socket Layer (SSL) Certificate server which identifies a specific computer, specific IP address combined with a vetted user password and the user's permissions assigned at the database level. Additional participating agencies law enforcement user access is

allowed by using a vetting process to identify users and credentials and then allowing access using digital identity certificates with 2 factor authentication and data encryption.

b. Computer systems are restricted by logon names, passwords, SSL certificates, and user security code authorization assigned within the database. GBI Investigative Division computers are operated in accordance with safeguards mandated by the Georgia Crime Information Center (GCIC).

c. When remote access to the intelligence system is required, it is authorized through the use of a computer with an encrypted secure connection through a Virtual Private Network, through a SSL server or by using a vetting process to identify users assigned accessing with digital certificates using 2 factor authentication and encryption.

d. Authorization for electronic purging, destroying or modifying records is controlled by the GISAC personnel and authorized by the GISAC Supervisor(s).

2. Facilities

a. Access to facilities and operating environments are controlled by building security to include a cardkey system.

b. Access to the GISAC file room is limited to GISAC personnel only. No other personnel are allowed access to the file room without specific authorization from the GISAC Supervisor(s).

3. Files

a. Only criminal intelligence files will be stored in the GISAC file room. All files will be filed by the user in the file room at the end of each working day.

b. No intelligence file will be removed from the GISAC area without specific authorization from the Analyst Supervisor. If a file is removed, a sign out card will be completed and placed in the file's original location.

c. All ongoing work will be secured at the workstation in a manner which does not allow unauthorized access.

In the event of a data security breach, the information will be reviewed by the Privacy Officer. If providing notice to the individual whose information has been violated will compromise the underlying law enforcement purpose of the system and put pending investigations at risk, the individual will not be notified of the breach. Otherwise, the GBI will be obligated to notify individuals whose personally identifiable information has been compromised or accessed by an unauthorized user.

II. SUSPICIOUS ACTIVITY REPORT MANAGEMENT SYSTEM

GISAC maintains Suspicious Activity Reports (SARs) in the SAR Vetting Tool (SVT). A SAR is official documentation of observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity. A SAR is not criminal intelligence and will not be maintained within the GBI Criminal Intelligence System.

GISAC personnel are trained to provide human review and vetting by investigating and recognizing behaviors and indicators that are indicative of preoperational or criminal activity related to terrorism. Information regarding observed behaviors that may be classified as a SAR is submitted to GISAC by law enforcement, private security or the public. All SAR Submissions are reviewed by a GISAC supervisor. This review ensures the information is legally collected and investigated.

Upon review by a GISAC supervisor, information meeting the established SAR Indicators and Behaviors list from NSI (http://ise.gov/sites/default/files/ISE-FS-200_ISE-SAR_Functional_Standard_V1_5_Issued_2009.pdf) will be classified as a Suspicious Activity Report (SAR). Only SARs reviewed, approved and classified by a GISAC supervisor will be maintained in the GISAC SAR Vetting Tool (SVT) and shared in the Homeland Security Information Network Georgia Portal (HSIN-GA). SARs Information that meet the standards established by NSI for submission to the National SAR Initiative (NSI) Shared Space will be submitted to the NSI system for access by DHS and other DHS recognized Fusion Centers.

GISAC personnel are required to adhere to the following practices and procedures for the receipt, collection, assessment, storage, access, dissemination, retention and security of information contained within the SVT system. These practices and procedures safeguard the information and ensure the protection of privacy, civil rights and civil liberties.

A. Upon receipt of a SAR Submission, a GISAC supervisor will review the report to determine if the activity reported is reasonably indicative of preoperational planning related to terrorism or other criminal activity.

1. If the SAR Submission is based on criminal activity with no nexus to terrorism, the SAR Submission is reviewed by a GISAC analyst for possible inclusion in the Criminal Intelligence System.

2. If the SAR Submission contains information reasonably indicative of terrorist activity, the SAR Submission is reviewed for indicators and behaviors established by the NSI. If these indicators are not present, the report is purged immediately.

3. If the indicators/behaviors are present, the SAR Submission is classified as a SAR and forwarded to a GISAC analyst for inclusion in the SVT.

4. In the event the SAR contains information of an urgent nature, the SAR will immediately be forwarded to the FBI for inclusion into the FBI Guardian system for follow up by the Joint Terrorism Task Force. SARs not of an urgent nature will be entered into the SVT for further investigation.

5. Only information regarding individuals involved in activities that have been determined to have a nexus to terrorism, i.e. consistent with behaviors associated with terrorism activities or preoperational planning in accordance with the standards established by the NSI will be shared through the NSI Shared Space. This safeguard is intended to ensure that information that could violate civil rights and civil liberties will not be intentionally or inadvertently gathered, documented, processed and shared.

6. SARs shared through the NSI Shared Space will be retained for a period of five years complete with personally identifiable

information. These SARs are also entered into the FBI's eGuardian system for additional investigation by the FBI JTTF.

B. GISAC personnel will investigate SARs within 90 days of receipt to determine credibility of the information and develop reasonable suspicion to initiate a criminal investigation or intelligence report. Information determined to meet the criteria of a SAR will be maintained in SVT for five years. SARs that are cleared of a terrorism nexus will be maintained in the SVT but will be purged of personally identifiable information (PII) within 90 days of entry into SVT. Any SAR shared in the National Shared Space will be retained for five years. Personally identifiable information will remain in SARs shared in the National Shared Space for the full retention period.

C. GISAC personnel will store SARs in a separate, but similar method, used for criminal intelligence information and provide for an audit and inspection process, supporting documentation, and labeling of the data to delineate it from criminal intelligence information. GISAC's SVT uses a standard reporting format and commonly accepted data collection codes and a sharing process which complies with the current Information Sharing Environment – Suspicious Activity Report (ISE-SAR) Functional Standard for identifying and handling SARs determined to be potentially related to terrorism.

D. SARS will be shared with GA law enforcement personnel who have been vetted and have access to the secure HSIN-GA portal. Information stored on the HSIN-GA portal will consist of a basic description of the activity that is reported and will not contain personally identifiable information since SARs may be in the vetting process. SARs will only be posted within the HSIN-GA portal for a maximum period of six months; however, the timeframe may be decreased as determined by a GISAC supervisor based on the amount of SARs posted on the portal. GISAC will regularly provide access to or disseminate information in response to an interagency inquiry for law enforcement, homeland security, or public safety and analytical purposes or provide an assessment of the information to any agency, entity, individual, or the public when credible information indicates potential imminent danger to life or property.

III. RISK AND VULNERABILITY ASSESSMENTS

Risk and Vulnerability Assessments are a function of the Georgia Emergency Management Agency (GEMA) – Office of Homeland Security (OHS). These assessments are not considered SARs information and are classified as Protected Critical Infrastructure Information (PCII). Consequently, these assessments are not available to the public. GISAC personnel can access the assessments electronically through a server maintained by GEMA at their headquarters facility. Only personnel who have attended training on the Automated Critical Asset Management System (ACAMS) will be allowed access to the risk and vulnerability assessments.

IV. SEARCH CAPABILITIES

Upon a valid request for information, the GISAC has the capability to query all available public and private files and databases for information to support the request, such as off line searches, EPIC queries, etc. It is the responsibility of the SAC of the GISAC to ensure any commercial database contracted to provide information is in legal compliance in its information-gathering techniques.

V. ANALYTICAL SUPPORT

Analytical support involves assembling intelligence in a logical manner to form patterns and meaning. Upon request, the Intelligence Analyst may provide a variety of analytical and charting services in support of investigations and prosecutions. These services include:

A. Collating Information: Review and merge intelligence information with existing data in the intelligence system so that it may be analyzed.

B. Link Charting: Establish relationships among entities, individuals or organizations in an investigation.

C. Event Charting: Show the chronological relationships among criminal or related events.

D. Flow Charting: Depict the flow of money, narcotics, stolen goods or other commodities through the elements of a criminal network.

E. Activity Charting: Define the pattern or sequence of a criminal operation, including modus operandi.

F. Telephone Toll Analysis: Condense large volumes of data into easy to read automated reports from which the significant telephone activity may be identified.

G. Case Analysis: Summarize investigative actions taken, the main findings associated with these actions and the activities of the subjects.

H. Special Publications: Develop publications on various criminal intelligence topics. The topics are determined by interest, availability of data and need for the information.

VI. ACCOUNTABILITY

A. Information Quality Assurance

The GBI will make every reasonable effort to ensure that information will be corrected, deleted from the system, or not used when it is determined that the information is erroneous, misleading, obsolete, or otherwise unreliable. The GBI will advise all agencies to which intelligence has been provided when such intelligence has been found to be unreliable.

All participating agencies are responsible for the quality and accuracy of the data accessed by or shared with the GBI. Originating agencies providing data remain the owners of the data contributed. In the event submitted data is found to be inaccurate, incomplete, out of date, or unverifiable, the GBI will advise the appropriate data owner, via electronic notification as required by the Information Sharing Environment. Additionally, in the event erroneous, inaccurate information is posted, a notification will be sent to the participating agency advising of the error.

B. Privacy Policy

This policy addresses privacy protections and will be provided to the public upon request. The Privacy Officer will be responsible for receiving and

responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information systems.

The GBI will provide a copy of this policy to all agency and non-agency personnel who provide services (i.e., MJTF agents) and will require written acknowledgement of receipt of this policy and agreement of compliance to this policy and the provisions it contains.

GISAC and the Privacy Officer will periodically review and update the provisions protecting privacy, civil rights, and civil liberties contained within this policy and make appropriate changes in response to changes in applicable law, changes in technology, changes in the purpose and use of the information systems, and changes in public expectations.

C. Audits

GISAC will conduct regular audits and inspections of the information contained in its criminal intelligence system. An inspection/audit will be conducted every year by a GBI inspection team led by the Privacy Officer. Random inspections by the work unit supervisor will be conducted and documented each year.

D. Complaints

GBI personnel will report violations or suspected violations of the privacy policy to the Privacy Officer. The Privacy Officer will assess these complaints and any such complaints from any other source, including the public and other law enforcement agencies, and if necessary, refer them to the Office of Professional Standards. All such complaints received regarding violations of the privacy policy will be documented, investigated and retained pursuant to GBI Policy 1046 (Internal Affairs Investigations).

Complaints from the public regarding information to be shared through the Information Sharing Environment will be submitted to the Privacy Officer. If an individual has complaints to the accuracy or completeness of information held by GBI Personnel and complains that such information has resulted in demonstrable harm, the individual will be informed of the procedure for submitting complaints and requesting corrections. GBI Personnel will acknowledge the complaint and advise that it will be reviewed, but will not confirm the existence of any record that contains personally identifiable information. Prior to any further dissemination, any

personally identifiable information will be reviewed and the complaint resolved. If the information is determined to be erroneous, include incorrectly merged information, or be out of date, the information will be corrected or deleted from the Criminal Intelligence System or the Suspicious Activity Report Management System, whichever applies. If the information is owned by a participating agency, GBI Personnel will inform the agency, electronically, of the complaint and provide any needed assistance in investigating and correcting or removing the information prior to any further dissemination. A record will be kept of all complaints and requests for corrections and the resulting action, if any.

E. Sanctions for Misuse

In the event any authorized user is found to be in violation of the provisions of this policy or federal law with regard to collection, use, retention, destruction, sharing, classification, or disclosure of information they will be immediately suspended from access to any systems and subject to disciplinary action, up to and including termination, and/or criminal prosecution.

F. Training

The GBI will require all personnel having access to criminal intelligence information or the Criminal Intelligence System to participate in a training program regarding this policy.

The training program will address the following:

1. Purpose of this policy;

2. Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of criminal intelligence information and suspicious activity reports;

3. Implementation of this policy in the day-to-day work of the user (either paper or systems user);

4. Impact of policy violations upon citizens and the agency; and

5. Penalties for policy violations.

GISAC will provide specialized training in recognizing behaviors and incidents that are indicative of criminal activity related to terrorism to personnel authorized to share criminal intelligence information in the Information Sharing Environment regarding the requirements and policies for collection, use and disclosure of criminal intelligence information.

VII. ANNNUAL REVIEW OF PRIVACY POLICY

The GBI Privacy Officer will review the Privacy Policy at least annually and direct the updating of the policy and procedures as necessary.

Attachments - 2
04-19-12 (chl)