



TIPS AND LEADS PROCESSING PROCEDURES FOR SUSPICIOUS ACTIVITY REPORTING

NOVEMBER 14, 2011

Provides operating policy and procedures for the collection, coordination, analysis, retention and sharing of tips and leads [regarding behavior] that may be indicative of intelligence gathering or preoperational planning related to terrorism or other criminal activity

Law Enforcement Sensitive



Standard Operating Procedure
Tips and Leads Processing Procedures for Suspicious Activity Reporting (SAR)

Table of Contents

1. Title	2
2. Purpose	2
3. Applicability	2
4. Definitions	2
5. Background	4
6. Overview	5
7. Tips and Leads Vetting Criteria	5
8. Responsibilities	7
9. SAR Vetting Policies	8
10. SAR Vetting Detailed Process and Detailed Procedures	13
11. Training	18
12. Privacy and Civil Liberties	19
13. Date Plan Implemented and Updated	19
14. References	19
15. Appendices	20



Standard Operating Procedure Tips and Leads Processing Procedures for Suspicious Activity Reporting (SAR)

Disclaimer: This document was prepared as a guide to help BRIC staff members understand the general operational policy and procedures for processing Tips and Leads that may be indicative of intelligence gathering or preoperational planning related to terrorism or other criminal activity. There may be situations where the circumstances surrounding an individual Tip and Lead may require deviation from the stated policies and procedures. In these situations, BRIC staff members should seek advice from the BRIC HLS Sworn Supervisor."

- 1. Title** Tips and Leads Processing Procedures for Suspicious Activity Reporting (SAR); hereinafter referred to as the *Boston Regional Intelligence Center (BRIC) SAR Standard Operating Procedure (SOP)*.
- 2. Purpose** The Boston Regional Intelligence Center (BRIC) has been a participant in the Nationwide SAR Initiative (NSI) since its inception on September 1, 2008. On a daily basis, BRIC Homeland Security analysts collect Tips and Leads (TLs) from a variety of systems and data bases; this SOP provides specific policy and procedures for the *collection, coordination, analysis, retention and sharing of TLs* [regarding behavior] that are indicative of intelligence gathering or preoperational planning related to terrorism or other criminal activity and may lead to the submission of a SAR to the NSI.
- 3. Applicability** This plan applies to all personnel working within the BRIC and is available for review by way of written manual and electronic copy.

This plan is incorporated into the BRIC's standard operating procedures, and it shall be the Commander's and Director's responsibility to ensure compliance with this plan.
- 4. Definitions**
 - CaseInfo:** The software technology used by the BRIC to manage investigative cases.
 - CrimeNtel:** The software technology used by the BRIC to manage criminal intelligence information as defined by 28 Code of Federal Regulations (CFR) Part 23, Criminal Intelligence Systems Operating Policies.
 - Fusion Core Solution (FCS):** A Microsoft SharePoint application used to manage the TL vetting process. FCS will be used to enhance information-sharing and security by automating collection, intake, workflow management, collaborative analysis, data visualization, dissemination, auditing, and capture of business-performance metrics.



Standard Operating Procedure

Tips and Leads Processing Procedures for Suspicious Activity Reporting (SAR)

Information Sharing Environment (ISE): Established by the United States Intelligence Reform and Terrorism Prevention Act of 2004, the ISE provides analysts, operators and investigators with information needed to enhance national security.

These analysts, operators and investigators come from a variety of communities - law enforcement, public safety, homeland security (HLS), intelligence, defense, and foreign affairs – and may work for federal, state, local, tribal, or territorial governments. They also have mission needs to collaborate and share information with each other and with private sector partners and our foreign allies.

ISE Shared Space: The ISE Shared Space is a software and hardware technology solution that facilitates the sharing of terrorism related SAR information among federal, state, local and tribal partners.

Information uploaded and shared by HLS partners in the ISE Shared Space is governed by the Intelligence Reform and Terrorism Prevention Act (IRTPA) Section 1016 (a) (4), and refers to all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to:

- The existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism;
- Threats posed by groups or individuals to the United States (U.S.), U.S. persons or interests, or to those of other nations;
- Communications of or by such groups or individuals; or
- Groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

Suspicious Activity Report (SAR): report of directly observed or conveyed activity and/or behavior that, based on an officer's training and experience, is believed to be indicative of intelligence gathering or preoperational planning related to terrorism, criminal, or other illicit intention.

Tip and Lead (TL) Information: Uncorroborated report of information that alleges or indicates some form of possible criminal activity. TL information does not include records management system (RMS) incident reports, open or closed case files), other criminal history records, or Computer Aided Dispatch (CAD) data.

One exception to this is when an officer determines that an incident report reveals behavior indicative of intelligence gathering or



Standard Operating Procedure Tips and Leads Processing Procedures for Suspicious Activity Reporting (SAR)

preoperational planning related to terrorism, criminal, or other illicit intention, and thus requires the attention of the BRIC as a precursor for opening a terrorism or criminal investigation”.¹

5. Background

The Nationwide Suspicious Activity Reporting Initiative (NSI) is a collaborative effort among federal, state, local, and tribal government agencies with Counterterrorism (CT) responsibilities. Developed pursuant to Presidential direction, it establishes a nationwide capability to gather, document, process, analyze, and share information about suspicious incidents to enable rapid identification and mitigation of potential terrorist threats.

The NSI builds on what law enforcement and other agencies have been doing for years – gathering information regarding behaviors and incidents associated with crime – and establishes a formal, replicable process whereby SAR information can be shared to help detect and prevent terrorism-related criminal activity in a manner that ensures that privacy, civil liberties, and other legal rights are adequately protected.

This process (often referred to as the NSI cycle), is documented in a Concept of Operations for the NSI published in December 2008 and in a revised functional standard in May 2009.

The BRIC has been a participant in the NSI since its inception on September 1, 2008, and participated in an Evaluation Environment along with other state and major urban area fusion centers to test and evaluate the policies, procedures, and technology needed to implement a unified process for the sharing of suspicious activity reports.

This Evaluation Environment resulted in the development of the ISE Functional Standard (FS), Suspicious Activity Reporting (SAR), Version 1.5, dated May 21, 2009—commonly identified as ISE-FS-200.

ISE-FS-200 provides a framework for the NSI and defines a SAR as

“Reported or observed activity and/or behavior that, based on an officer’s training and experience, is believed to be indicative of intelligence gathering or preoperational planning related to terrorism, criminal, or other illicit intention.”

6. Overview

This SOP documents the formal process for identifying and vetting TLs that

¹ Tips and Leads Issue Paper (Department of Justice, GLOBAL, 2007), 7.



Standard Operating Procedure Tips and Leads Processing Procedures for Suspicious Activity Reporting (SAR)

may or may not lead to the reporting of a SAR to the ISE Shared Space. It is important to establish that, for the BRIC, a “SAR” is the end-result of TLs that have been evaluated through the vetting process defined within this SOP and is determined to be indicative of intelligence gathering or preoperational planning related to terrorism, criminal, or other illicit intention as is set forth in the ISE-SAR Functional Standard 1.5.

TLs that have NOT been evaluated through the vetting process defined in this SOP are to be considered unevaluated information and therefore are NOT to be entered into the ISE.

7. Tips and Leads Vetting Criteria

The TL vetting process defined in Section 10 of this SOP will be executed by trained analysts and investigators using the explicit criteria listed in ISE-FS-200, Part B, ISE-SAR Criteria Guidance:

- Defined Criminal Activity And Potential Terrorism Nexus Activity:

Category	Description
Breach/Attempted Intrusion	Unauthorized personnel attempting to or actually entering a restricted area or protected site. Impersonation of authorized personnel (e.g. police/security, janitor)
Misrepresentation	Presenting false or misusing insignia, documents, and/or identification, to misrepresent one’s affiliation to cover possible illicit activity
Theft/Loss/ Diversion	Stealing or diverting something associated with a facility/infrastructure (e.g., badges, uniforms, identification, emergency vehicles, technology or documents {classified or unclassified}, which are proprietary to the facility)
Sabotage/ Tampering/ Vandalism	Damaging, manipulating, or defacing part of a facility/infrastructure or protected site
Cyber Attack	Compromising, or attempting to compromise or disrupt an organization’s information technology infrastructure
Expressed or Implied Threat	Communicating a spoken or written threat to damage or compromise a facility/infrastructure



Standard Operating Procedure Tips and Leads Processing Procedures for Suspicious Activity Reporting (SAR)

Aviation Activity	Operation of an aircraft in a manner that reasonably may be interpreted as suspicious, or posing a threat to people or property. Such operation may or may not be a violation of Federal Aviation Regulations
--------------------------	---

- Potential Criminal or Non-Criminal Activity Requiring Additional Fact Information During Investigation:

Category	Description
Eliciting Information	Questioning individuals at a level beyond mere curiosity about particular facets of a facility's or building's purpose, operations, security procedures, etc., that would arouse suspicion in a reasonable person
Testing or probing of Security	Deliberate interactions with, or challenges to, installations, personnel, or systems that reveal physical, personnel or cyber security capabilities
Photography	Taking pictures or video of facilities, buildings, or infrastructure in a manner that would arouse suspicion in a reasonable person. Examples include taking pictures or video of infrequently used access points, personnel performing security functions (patrols, badge/vehicle checking), security-related equipment (perimeter fencing, security cameras), etc.
Observation/ Surveillance	Demonstrating unusual interest in facilities, buildings, or infrastructure beyond mere casual or professional (e.g. engineers) interest such that a reasonable person would consider the activity suspicious. Examples include observation through binoculars, taking notes, attempting to measure distances, etc.
Materials Acquisition/ Storage	Acquisition and/or storage of unusual quantities of materials such as cell phones, pagers, fuel, chemicals, toxic materials, and timers, such that a reasonable person would suspect possible criminal activity



**Standard Operating Procedure
 Tips and Leads Processing Procedures for Suspicious Activity Reporting (SAR)**

Acquisition of Expertise	Attempts to obtain or conduct training in security concepts; military weapons or tactics; or other unusual capabilities that would arouse suspicion in a reasonable person
Weapons Discovery	Discovery of unusual amounts of weapons or explosives that would arouse suspicion in a reasonable person
Sector-Specific Incident	Actions associated with a characteristic of unique concern to specific sectors (such as the public health sector), with regard to their personnel, facilities, systems or functions

Note: These activities are generally First Amendment-protected activities and should not be reported in a SAR or ISE-SAR absent the BRIC’s two pronged (civilian and sworn) vetting process that will determine articulable facts and circumstances that support the source agency’s suspicion that the behavior observed is not innocent, but rather reasonably indicative of criminal activity associated with terrorism, including evidence of pre-operational planning related to terrorism. Race, ethnicity, national origin, or religious affiliation are not to be considered as factors that create suspicion (although these factors may be used as specific suspect descriptions).

8. Responsibilities The HLS Division within the BRIC will have primary responsibility for facilitating the TL vetting process defined in this SOP. Additional responsibilities are described below.

HLS Supervisor Responsibilities The BRIC will assign a team of trained Supervisors (Analytic and Investigative) from within the HLS division to oversee the entire TL processing procedures for suspicious activity reporting.

HLS Supervisors will be responsible for facilitating information review meetings; tasking and managing analysis and investigative follow-up; and ensuring information is shared, retained, and purged according to this SOP and all BRIC policies and procedures.

HLS Detective Responsibilities The BRIC will assign a team of trained Detectives from within the HLS division to perform initial vetting procedures and enter appropriately vetted information into the FCS as a TL entry. HLS Detectives shall be



Standard Operating Procedure Tips and Leads Processing Procedures for Suspicious Activity Reporting (SAR)

charged with managing the TLs assigned to them, ensuring that all information is treated in accordance with the BRIC's Information Privacy, Civil Rights/Liberties Policy.

HLS Intelligence Analyst Responsibilities

The BRIC will assign a team of trained Intelligence Analysts from within the HLS division to collect TL information, perform initial vetting procedures (such as criminal history checks), and enter appropriately vetted information into the FCS as a TL entry.

HLS Intelligence Analysts shall be charged with managing the TLs assigned to them, ensuring that all information is treated in accordance with the BRIC's Information Privacy, Civil Rights/Liberties Policy.

9. Tips and Leads Vetting Policies

BRIC staff will adhere to the below listed policies for TL collection and vetting, SAR reporting, and disposition of TLs that do not meet SAR reporting criteria; specific TL vetting procedures are detailed in Section 10.

Collection Policy

On a daily basis, HLS Analysts will collect information about law enforcement related events and activities from the following systems and sources using defined search criteria; see Appendix B, *BRIC HLS Daily Search Items* document.

- BPD Incident Tracking System
- BPD Field Interview and Observation Report System
- BPD Computer Aided Dispatch System
- Open Source
- Homeland Security Information Network (HSIN):
 - Review HSIN documents for general information and Terrorist Screening Center (TSC) hits; many of the documents on HSIN are emailed to the BRIC account from other sources.
 - For TSC Hits, review HSIN documents for TSC summary reports and other HIR documents with matches that concern Boston or the Urban Areas Security Initiative (UASI) area.
- E-Guardian (access via Law Enforcement Online (LEO)):
 - Review E-Guardian daily for new SARs posted by the FBI.



Standard Operating Procedure

Tips and Leads Processing Procedures for Suspicious Activity Reporting (SAR)

- Vet any names through BPD systems and notify BRIC supervisor and FBI analyst of any results.
 - Shared Space: Review Shared Space daily for any new SARs posted related to Boston and also when conducting SAR work ups.
 - BRIC E-mail Account: Review any e-mails received pertaining to Homeland Security issues such as Regional Fusion/ Intelligence Center bulletins, Open source reports, FBI bulletins, Media reports, NOC “Steady State” and other reports.
 - BRIC I-Watch E-mail Account.
-

Preliminary Analysis Policy

All BRIC staff assigned TL vetting responsibilities will comply with the following *preliminary analysis* policy:

- TLs received independent of BPD and/or UASI data repositories must be recorded in the BRIC FCS system and reviewed by a BRIC Supervisor.
- The HLS Supervisor will either assign each TL to a BRIC Detective for investigative follow-up and/or send to a BRIC Intelligence Analyst for further review and to assess the credibility and significance of the information.
- Once a TL is vetted by a combination of investigative and analytical methods, the BRIC HLS supervisors will make a determination on whether to classify the information as a SAR and thus enter it into the ISE shared space.
- In some instances, where the nature of the behavior immediately meets ISE SAR criteria, the information may be entered into the shared space immediately prior to the completion of further vetting by detectives and analysts. However, this decision can only be made by a BRIC HLS supervisor and the SAR will be updated in the shared space immediately upon the completion of further vetting.
- All leads received by the BRIC that are indicative of “imminent” or “known/not imminent” terrorist activity will be reported to the Boston FBI Joint Terrorism Task Force (JTTF) to aid in deconfliction, and to determine whether the leads warrant FBI/JTTF involvement (see BRIC Threat Information Triage Plan, Urgency Matrix, Immediate or Priority Factors). Reporting of the SAR to the JTTF requires review by sworn BRIC HLS Supervisors.
- BRIC HLS Analysts will review each TL considered for SAR vetting



Standard Operating Procedure Tips and Leads Processing Procedures for Suspicious Activity Reporting (SAR)

for its geospatial relationship to critical infrastructure, and to determine if the information provided fits current trends and patterns of behavior experienced locally and/or nationally.

- TLs that do not meet the ISE-SAR functional standard 1.5 criteria, and are therefore not to be considered SARs can still possess criminal intelligence value. TLs that fall into this category, where criminal predicate has been established are to be entered into the BRIC's criminal intelligence system (CrimeNtel).

Vetting Policy

All BRIC staff assigned TL vetting responsibilities will comply with the following *vetting* policy:

- The initial vetting of TLs takes place when the Collection and Preliminary Analysis processes are completed. This is done by a committee depending on the availability of BRIC HLS staff.
- TLs considered for SAR must be reviewed and discussed with an HLS Supervisor; in addition, it is recommended that other HLS analysts, detectives, a DHS Intelligence Officer, and a FBI analyst are also present for the review (review committee).
- TLs will be reviewed to determine:
 - Source and content reliability;
 - Presence of behaviors corresponding to the ISE SAR criteria;
 - Presence of relevant information in law enforcement indices;
 - Correlation with standing warnings and bulletins; and
 - The significance and potential risk associated with the location of the event.
- If upon initial review the committee determines that the tip or lead being reviewed is of a criminal nature with no nexus to terrorism, the HLS Supervisor will ensure that:
- The information is turned over to the proper investigative unit; and BRIC FCS system is updated with disposition actions.
- If the committee determines that further review is needed, the tip or lead is assigned a case number and entered into Case Info and assigned to a BRIC HLS Detective for investigation. As the Tip or Lead proceeds through the vetting process, BRIC analysts along with the DHS Intelligence Officer and FBI analyst will provide analytical



Standard Operating Procedure

Tips and Leads Processing Procedures for Suspicious Activity Reporting (SAR)

support to the vetting process/investigation.

- Initial vetting should occur within 24 hours of receiving the Tip or Lead, pending staff availability; during this time a determination should be made as to whether or not data regarding the identified behaviors and indicators can be entered into the Shared Space.
- As mentioned above, in some instances where the behaviors immediately satisfy those in ISE-FS-200, the information may be entered into the shared space while the vetting is completed. These items must be reviewed within 24 hours of entry and adjusted based on the vetting conducted by detectives and analysts.

Disposition Categories

At the completion of the vetting procedures, all TLs will be assigned one of the following disposition categories

- **Unfounded:** No action taken. Tip or Lead determined to be a lawful act or has no nexus to a criminal or terrorist related event. These items are not entered in the ISE Shared Space or criminal intelligence system; however, may remain in the investigative case management system as an official record that shows what steps were taken to vet the item.
- **Candidate SAR:** Open case. Activity determined to be suspicious in nature, meeting the criteria set forth in the ISE-SAR functional standard 1.5, but either the source of the information or the description of the behaviors and indicators are not strong enough to allow for full vetting on behalf of the BRIC. Because the behaviors and indicators meet the SAR criteria it will be entered into the Shared Space; however, the personally identifying information (PII) will not be entered unless designated by a BRIC HLS supervisor. The BRIC takes this extra precaution to balance the importance of reporting suspicious activities and fulfilling its “due diligence”, while at the same time safeguarding privacy, civil rights and civil liberties.
- **Confirmed SAR:** Open case. All of the SAR criteria are met and the information can be considered reasonably indicative of terrorist planning activities. The behaviors and indicators are placed in the Shared Space along with PII if available, and the Boston Detectives assigned to the JTTF are notified to further the investigation.
- **Criminal Activity:** Retained as intelligence. No nexus to terrorism. The Tip or Lead appears criminal in nature and is forwarded to the appropriate investigative unit. This information will also be



Standard Operating Procedure Tips and Leads Processing Procedures for Suspicious Activity Reporting (SAR)

assessed for intelligence value and entered into the criminal intelligence system if the criteria are met.

Information Sharing Policy

All BRIC staff assigned TL vetting responsibilities will comply with the following *information sharing* policy:

- TL information should be disseminated primarily in response to an inquiry, and only for law enforcement, homeland security, and public safety purposes.
 - TL information may be included in secure information databases and disseminated to relevant law enforcement, homeland security, and public safety agencies that have the need and right to know the information in 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.
 - TL information should not be regularly disseminated in bulletins and other like products unless they have been evaluated as being potentially indicative of criminal or terrorist behavior.
-

Information Retention Policy

All BRIC staff assigned TL vetting responsibilities will comply with the following *information retention* policy:

- The retention period for TL information should be long enough for detectives and analysts to determine its credibility and value. Initial vetting should be conducted within 24 hours of receiving the TL, and should be worked according to case load/priority.
- TLs entered into FCS must have a disposition code attached.
- All Tips and Leads entered into FCS and the NSI Shared Space will be retained in a manner consistent with the BRIC's Criminal Intelligence File Guidelines and Privacy, Civil Rights and Civil Liberties policy."
- TLs with an *unfounded* disposition will be purged of all PII from the FCS system upon assignment of disposition.
- TLs with a Criminal/Non-Terrorism disposition will be purged of all PII from the FCS system upon assignment of disposition, and after relevant information has been shared with the appropriate law enforcement authority for further investigation. Aggregate data, from TLs, purged of PII, will be retained indefinitely for statistical



Standard Operating Procedure Tips and Leads Processing Procedures for Suspicious Activity Reporting (SAR)

reporting and performance measurement.

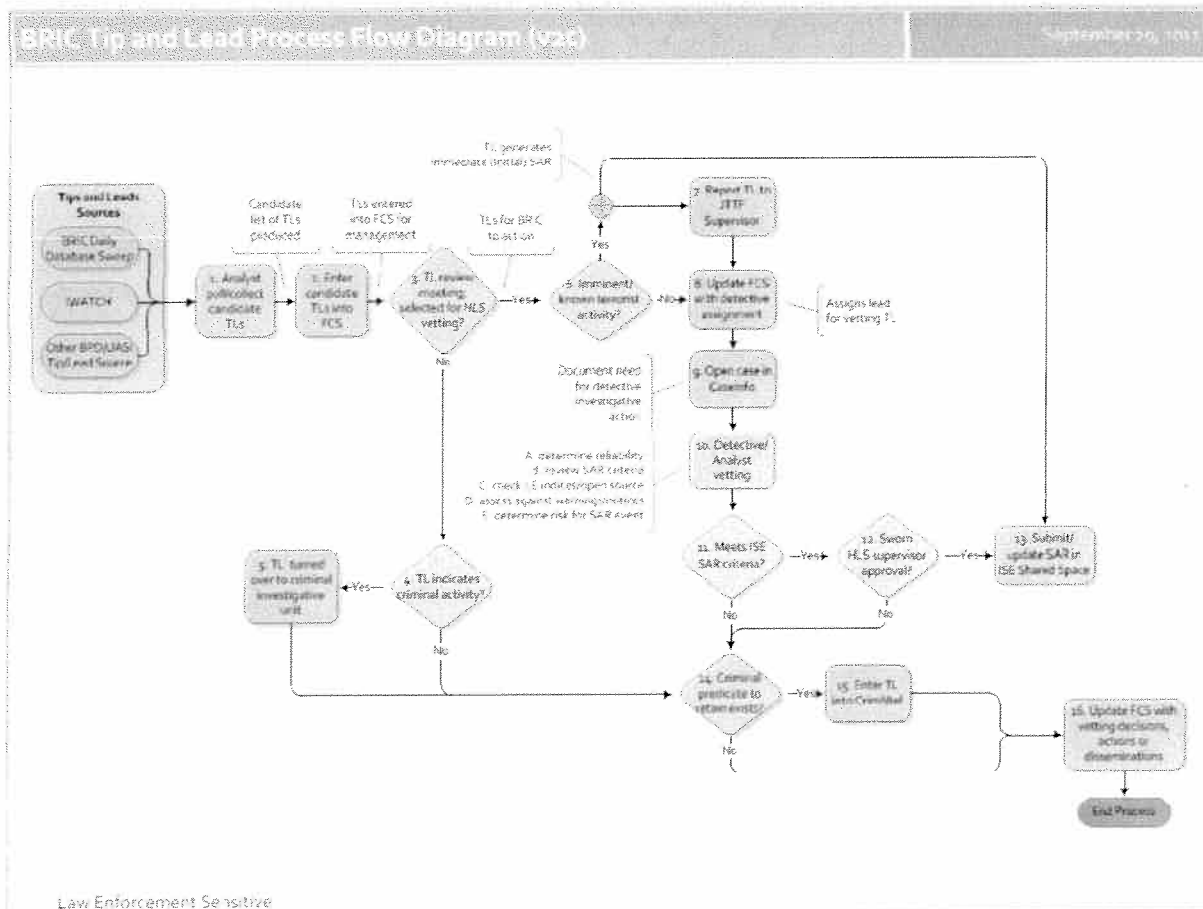
10. Tips and Leads Vetting Process and Detailed Procedures

This section provides a flow diagram for the BRIC TL vetting process and provides detailed procedures for each step of its execution. All BRIC staff members with TL vetting responsibilities, whether detective or analyst, will adhere to the steps described in this section.

The BRIC TL vetting process is executed on a daily basis and begins with the collection of information from various BPD systems, UASI partners, and the IWATCH program. The process results in one of four outcomes that correlate to the four disposition codes described in Section 9.

Tips and Leads Vetting Process Diagram

The diagram below depicts the BRIC process for vetting TLs; each of the seventeen steps in the diagram is described in detail in the next section. A larger sized version of this diagram is provided in Appendix A.





Standard Operating Procedure
Tips and Leads Processing Procedures for Suspicious Activity Reporting (SAR)

Tips and Leads
Vetting Detailed
TL Vetting
Procedures

Step	Description	Product/Result
1. Analyst pull/collect candidate TLs	A BRIC Homeland Security analyst(s) collects information from a variety of systems and databases and identifies events or activities that have a nexus to HLS or critical infrastructure protection.	List of TLs that are candidates for formal BRIC vetting.
2. Enter candidate TLs into FCS	New TL form is added to the FCS system for each candidate TL.	TLs records are added to FCS system.
3. TL review meeting; selected for HLS vetting?	TLs are reviewed and discussed with HLS sworn supervisor. <i>Decision: If TL is of HLS nature, it will be selected for formal vetting by the BRIC; go to step 6. If not, go to step 4.</i>	List of <i>HLS</i> TLs that will be formally vetted by the BRIC.
4. TL indicates criminal activity?	TLs are further reviewed for potential criminal activity. <i>Decision: If TL is of criminal nature with no nexus to terrorism, it is turned over to an investigative unit for further action; go to step 5. If not, go to step 14.</i>	List of criminal TLs that will <i>not</i> be vetted by BRIC.
5. TL turned over to criminal investigative unit	BRIC forwards TL to appropriate criminal investigative unit; go to step 14.	None for BRIC; criminal investigative unit takes over TL.



Standard Operating Procedure
Tips and Leads Processing Procedures for Suspicious Activity Reporting (SAR)

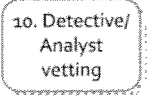

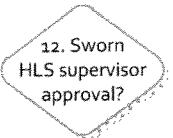
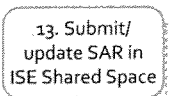
Step	Description	Product/Result
6. Imminent/ known terrorist activity?	<p>TL is reviewed to determine if it is indicative of "imminent" or "known/ not imminent" terrorist activity.</p> <p><i>Decision: If TL meets this criteria, will be reported to the JTTF supervisor immediately to aid in deconfliction, and to determine whether TL warrants FBI/JTTF involvement; go to step 7.² If not, go to step 8.</i></p>	<p>TLs meeting "imminent" or "known/ not imminent" terrorist activity are presented to the JTTF for action.</p>
7. Report TL to JTTF Supervisor	<p>TL indicating "imminent" or "known/ not imminent" terrorist activity is forwarded to the JTTF supervisor.</p>	<p>BRIC will continue its vetting process on the TL after it is forwarded to the JTTF.</p>
8. Update FCS with detective assignment	<p>For each TL selected for formal vetting, the HLS supervisor will update the FCS system with the detective assigned to lead the vetting activity.</p>	<p>TLs to be formally vetted are assigned a detective in FCS system</p>
9. Open case in CaseInfo	<p>The TL is assigned a case number and entered into CaseInfo, the BRIC case management application.</p>	<p>New CaseInfo case is opened to document investigative activities associated with the TL.</p>

Step	Description	Product/Result
------	-------------	----------------

² See BRIC Threat Information Triage Plan, Urgency Matrix, immediate or Priority Factors.



Standard Operating Procedure
Tips and Leads Processing Procedures for Suspicious Activity Reporting (SAR)

 <p>10. Detective/ Analyst vetting</p>	<p>BRIC detective reviews information in the TL to determine if it requires further investigation; support may be sought from BRIC analysts, DHS intelligence Officer, and FBI analyst, as needed.</p>	<p>Information is gathered to support decision to fully investigate the TL.</p>
 <p>11. Meets ISE SAR criteria?</p>	<p>Detective determines if TL meets/does not meet SAR reporting criteria. <i>Decision: If TL meets SAR criteria, go to step 12. If not, go to step 14.</i></p>	<p>TLS meeting SAR reporting criteria are identified.</p>
 <p>12. Sworn HLS supervisor approval?</p>	<p>Sworn HLS supervisor reviews and approves/ does not approve generation of SAR to NSI Shared Space. <i>Decision: If HLS supervisor approves SAR, go to step 13. If not, go to step 14.</i></p>	<p>TLS approved for submission as SAR to Shared Space are identified.</p>
 <p>13. Submit/ update SAR in ISE Shared Space</p>	<p>Detective creates new SAR (or updates existing SAR) using NSI Shared Space SAR Tool. <i>Note: Efforts are underway to automate SAR submission from TL entered into FCS.</i></p>	<p>New SAR is generated (or existing SAR is updated) and submitted to the NSI Shared Space.</p>

Step	Description	Product/Result
------	-------------	----------------



Standard Operating Procedure
Tips and Leads Processing Procedures for Suspicious Activity Reporting (SAR)

<p>14. Criminal predicate to retain exists?</p>	<p>Detective/Analyst determines if the information in the TL supports retention of the information as criminal intelligence, per 28 CFR Part 23.³</p> <p><i>Decision: If Detective/Analyst determines that "reasonable suspicion" or "criminal predicate" exists, go to step 15. If not, go to step 16.</i></p>	<p>TLs that can be retained as criminal intelligence are identified.</p>
<p>15. Enter TL into CrimNtel</p>	<p>Detective/Analyst enters TL information into CrimNtel, the BRIC intelligence management system.</p>	<p>New criminal intelligence record is created in CrimNtel.</p>
<p>16. Update FCS with vetting decisions, actions or disseminations</p>	<p>Detective/Analyst updates the FCS system with vetting actions taken, TL disposition code, and all external agency disseminations of TL information (JTTF, SAR, other agencies, etc.).</p>	<p>TL record in FCS system updated with vetting and dissemination actions taken.</p>

11. Training

BRIC staff will adhere to the following training requirements before engaging in the TL processing procedures defined in this SOP.

Analytic Training

BRIC HLS Analysts and Detectives will receive NSI SAR "Analytic Role" training. This training focuses on the evaluation of TLs to identify behaviors that may be associated with pre-incident terrorism planning and the process for sharing terrorism-related SARs nationwide.

³ "Reasonable Suspicion" or "Criminal Predicate" is established when information exists that 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, Regulation 28 CFR Part 23, Criminal Intelligence Systems Operating Policies, http://it.ojp.gov/documents/28cfr_part_23.pdf



Standard Operating Procedure Tips and Leads Processing Procedures for Suspicious Activity Reporting (SAR)

Through this curriculum, analysts and investigators are trained to recognize terrorism-related pre-incident indicators and to validate – based on a combination of knowledge, experience, and available information – whether the behavior has a potential nexus to terrorism and meets criteria for submission. The training is delivered in an eight-hour workshop format.

Law Enforcement Training

The BRIC will facilitate the training of BPD law enforcement officers, and will assist with the facilitation of training for UASI partner agencies. Frontline law enforcement personnel will be trained to recognize behavior and incidents that may indicate criminal activity associated with terrorism. The SAR Line Officer Training focuses on the critical role line officers have in the effective implementation of the SAR process by identifying and documenting suspicious activity.

Non-Law Enforcement Public Safety Training

The BRIC will utilize both custom-developed training programs and NSI training material for first responders, public safety, and private sector partners and the public to educate them on recognizing and reporting behaviors and incidents indicative of criminal activity and terrorism.

12. Privacy and Civil Liberties

The BRIC has incorporated the gathering, processing, reporting, analyzing and sharing of TLs and suspicious activities and incidents into existing processes and systems used to manage other crime-related information and criminal intelligence, so as to leverage existing policies and protocols utilized to protect the information privacy, civil liberties, and other legal rights of the general public; refer to the *BRIC Information Privacy, Civil Rights/Liberties Protection Policy* document.

13. Date Plan Implemented and Updated

This SOP was implemented as of the date of publication and will be updated, refreshed, and revised (at least) annually by the Director.

14. References

This plan includes references to, and should be used in conjunction with, the following documents; please review appendices to this document for additional detail:

- BRIC Information Privacy Policy



Standard Operating Procedure Tips and Leads Processing Procedures for Suspicious Activity Reporting (SAR)

- BRIC Analytic Training and Professional Plan
- BRIC/LEIU Criminal Intelligence File Guidelines
- BRIC Threat Information Triage Plan
- BRIC Dissemination Plan
- BRIC HLS Daily Search Items

This plan was further informed by the following documents:

- Baseline Capabilities for State and Major Urban Area Fusion Centers. September 2008.
- National Suspicious Activity Report (SAR) Initiative (NSI)
- Suspicious Activity Reporting Process Implementation Checklist
- Nationwide Suspicious Activity Reporting Initiative Concept of Operations
- Final Report: Information Sharing Environment (ISE)—Suspicious Activity Reporting (SAR) Evaluation Environment
- Findings and Recommendations of the SAR Support and Implementation Project
- Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) Version 1.5
- DOJ Tips and Leads Issue Paper
- Fusion Center Guidelines, April 2006.
- National Strategy for Information Sharing, October 2007.

Appendices

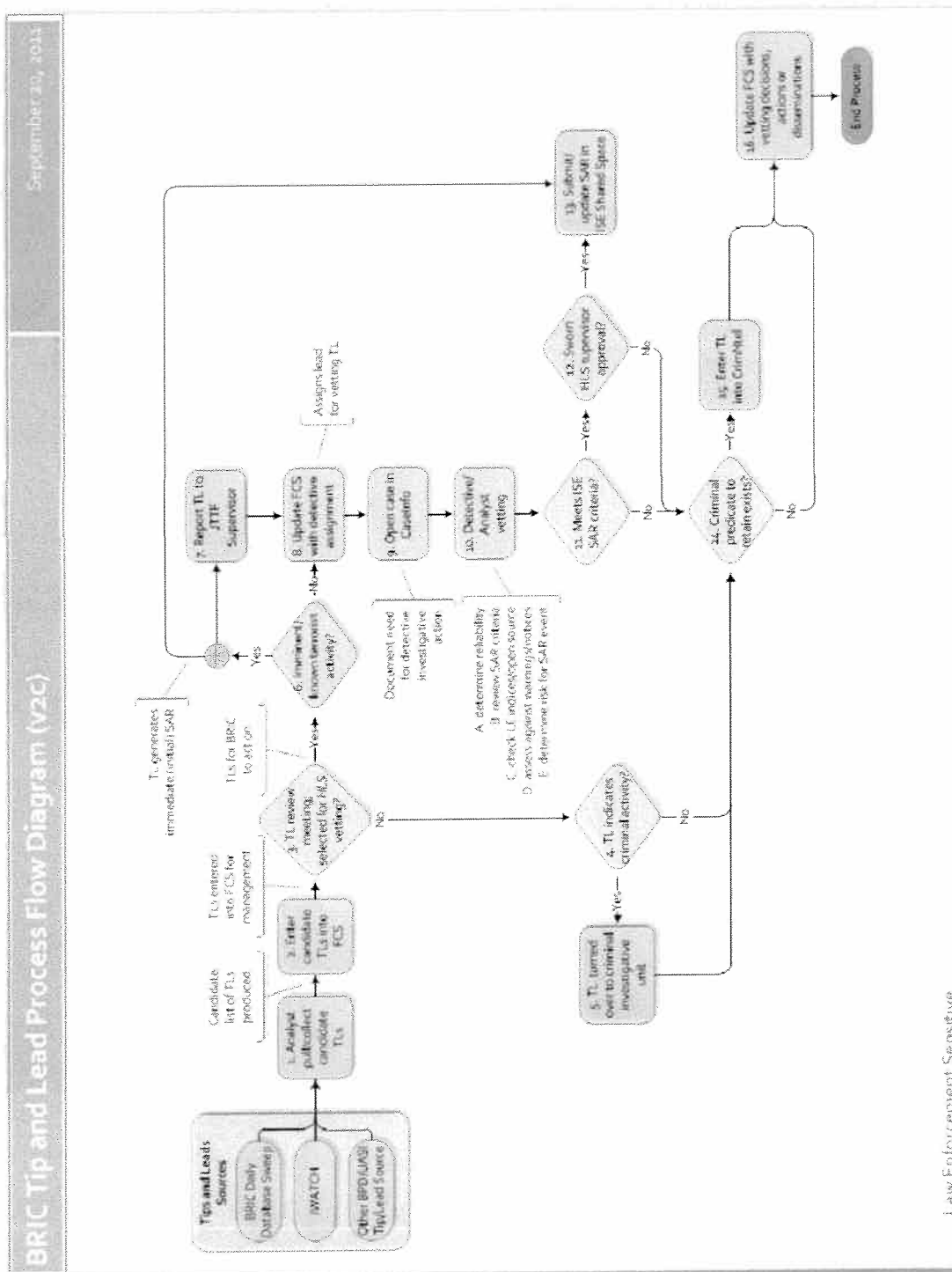
This plan includes the following appendices:

- Appendix A – Tips and Leads Vetting Process Diagram
 - Appendix B – BRIC HLS Daily Search Items
-



Standard Operating Procedure
 Tips and Leads Processing Procedures for Suspicious Activity Reporting (SAR)

Appendix A - Tips and Leads Vetting Process Diagram





Standard Operating Procedure Tips and Leads Processing Procedures for Suspicious Activity Reporting (SAR)

Appendix B - BRIC HLS Daily Search Items

Key Situation Search:

- Homeland Security
- Homeland Security UASI

Incident Description Search:

- Aircraft Incidents
- Biological Threats
- Bomb Threats
- Dangerous or Hazardous Condition
- Demonstrations/Riot
- Explosions
- Explosives – Turned in or Found
- Harbor – Viol. Reg & Statutes
- Harbor Incidents
- Investigate Person
- Investigate Property
- Investigation for Another Agency
- Racial – Religious Report
- Vandalism – Graffiti

FIO Review:

- FIO's where "Terrorism" box is checked off

Web CAD Review:

- Use the Web Cad System in Moodle
- Search since prior day for the following codes: susper; terobs; bomb; bombr; bombt; explos; suslet; and spurs

Keyword Search in BRIC Data Mining Tool

- Run keyword searches on BPD incident narratives using the keyword database to insert pre-defined keywords

Critical Infrastructure Viewer

- Pull up arrest locations and FIOs within 25 yards of a critical infrastructure building

HSIN



Standard Operating Procedure Tips and Leads Processing Procedures for Suspicious Activity Reporting (SAR)

BRIC

- Review HSIN documents for general information and TSC hits
- TSC Hits- Review HSIN documents for TSC summary reports and other HIR documents with matches that concern Boston or UASI

E-Guardian (via LEO)

- Review E-Guardian daily for any new SARs posted by the FBI

Shared Space

- Review Shared Space daily for any new SARs posted related to Boston and when conducting SAR work ups

BRIC EMAIL Account

- Review any emails received pertaining to Homeland Security such as:
 - Regional fusion/ intelligence center bulletins
 - Open source reports
 - FBI bulletins
 - Media reports
 - NOC “Steady State” and other reports
 - Keep an eye out for events and information pertaining to or applicable to Boston

Open Source Review

- Review open source reports pertaining to world events, especially the Middle East, Asia and America
- Review open source reports pertaining to worldwide terrorism
- Review FaceBook, Craigslist and other sources for events in Boston stemming from world events (e.g. Iranian protests)
- Much of this will be FYI, but keep an eye out for events and information pertaining to or applicable to Boston

Person Work Up

- BOP
- RMV Information
- RIC / CR Report
- Hackney
- ITS
- FIOs



Standard Operating Procedure Tips and Leads Processing Procedures for Suspicious Activity Reporting (SAR)

- Clear
- Crimentel
- Shared Space
- Open Source (facebook, MySpace, LinkedIn)
- FBI Search through George
- DHS Search through Quinn