Tips and Leads Processing Procedures for Suspicious Activity Reporting (SAR)
Boston Regional Intelligence Center

Abstract
Provides operating policy and procedures for the collection, coordination, analysis, retention and sharing of tips and leads regarding observed behavior that may be reasonably indicative of terrorism or other criminal activity.

BOSTON REGIONAL
INTELLIGENCE CENTER
BRIC

Contents

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 regarding observed behavior that may be reasonably indicative of terrorism or other criminal activity.

I. 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).

II. 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 analysts review Tips and Leads (TLs) from a variety of law enforcement information systems and publicly available resources. 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 that may lead to the submission of an ISE-SAR to eGuardian. Per national strategy guidance, eGuardian will serve as the NSI SAR Data Repository (SDR) for SAR for federal, state, local, tribal, and territorial (FSLTT) law enforcement agencies and state and major urban area fusion centers.[1]

III. Applicability

This plan applies to all personnel assigned to the BRIC.
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.

IV. 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.

SharePoint: A Microsoft application used by the BRIC to manage the TL vetting process. SharePoint 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. For purposes of its use in vetting tips and leads, no personal identifying information (PII) will be retained in SharePoint.

[1] NSI SAR Data Repository CONOPS, Jan 2014.

eGuardian: The FBI's unclassified threat reporting system. eGuardian will serve as the NSI SAR Data Repository (SDR) for SAR for federal, state, local, tribal, and territorial (FSLTT) law enforcement agencies and state and major urban area fusion centers.[2]

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.[3]

ISE Vision:

- National security through responsible information sharing

ISE Mission:

- Advance responsible information sharing to further counterterrorism, homeland security, and cybersecurity missions
- Improve nationwide decision making by transforming from information ownership to stewardship
- Promote partnerships across federal, state, local, and tribal governments, the private sector, and internationally

Information Sharing Environment-Suspicious Activity Reporting (ISE-SAR) Functional Standard (ISE-FS-200): Builds upon, consolidates, and standardizes nationwide aspects of those ISE-relevant activities already occurring at the federal, state, and local levels with respect to the processing, sharing, and use of suspicious activity information.[4] ***Note: This is currently operating under Version 1.5.***

Nationwide SAR Initiative (NSI): The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) is a joint collaborative effort by the U.S. Department of Homeland Security, the Federal Bureau of Investigation, and state, local, tribal, and territorial law enforcement partners. This initiative provides law enforcement with another tool to help prevent terrorism and other related criminal activity by establishing a national capacity for gathering, documenting, processing, analyzing, and sharing SAR information.[5]

---

[2] Ibid.

[3] http://www.ise.gov/.

[4] http://www.ise.gov/nationwide-sar-initiative, *ISE-SAR Functional Standard, Version 1.5 (ISE-FS-200).*

[5] *The Nationwide SAR Initiative*, http://nsi.ncirc.gov/.

The NSI is a standardized process—including stakeholder outreach, privacy protections, training, and facilitation of technology—for identifying and reporting suspicious activity in jurisdictions across the country and also serves as the unified focal point for sharing SAR information.[6]

SAR Data Repository (SDR): The database where all shared Information Sharing Environment-Suspicious Activity Reports (ISE-SARs) reside. The SDR is populated and searched through a front-end user interface application (eGuardian).[7]

Suspicious Activity Report (SAR): Official documentation of observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity.[8] *NOTE: To be considered, an ISE-SAR, a report must meet the criteria set forth in the Functional Standard Version 1.5 (see definition below).*

ISE-Suspicious Activity Report (ISE-SAR): An ISE-SAR is a SAR that has been determined, pursuant to a two-part process, to have a potential terrorism nexus (i.e., to be reasonably indicative of criminal activity associated with terrorism)[9]. ISE-SAR business, privacy, and civil liberties rules will serve as a unified process to support the reporting, tracking, processing, storage, and retrieval of terrorism-related suspicious activity reports across the ISE.

Tip and Lead (TL) Information: Uncorroborated report of information that alleges or indicates some form of possible criminal activity.[10] Tip and Lead information may originate from citizen reporters, law enforcement and public safety partners, or as a result of data analysis.

V. 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.[11] The

[6] Ibid.

[7] NSI SAR Data Repository CONOPS, Jan 2014, 1.

[8] *ISE-SAR Functional Standard, Version 1.5 (ISE-FS-200).*

[9] Ibid. Per *ISE-SAR Functional Standard, Version 1.5,* 33*:* The determination of an ISE-SAR is a two-part process. First, at the State or major urban area fusion center or Federal agency, an analyst or law enforcement officer reviews the newly reported information against ISE-SAR behavior criteria. Second, based on available knowledge and information, the analyst or law enforcement officer determines whether the information meeting the criteria has a potential nexus to terrorism. Once this determination is made, the information becomes an "ISE-SAR" and is formatted in accordance with ISE-FS-200 (ISE-SAR Functional Standard). The ISE-SAR would then be shared with appropriate law enforcement and homeland security personnel in the State or major urban area fusion center's area of responsibility.

[10] *Tips and Leads Issue Paper* (Department of Justice, GLOBAL, 2007), 7.

[11] *The National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing*

resulting NSI business process (often referred to as the NSI cycle) was described by the Program Manager for the Information Sharing Environment (PM-ISE) in a Concept of Operations for the NSI published in December 2008 and in a revised functional standard in May 2009.[12]

The findings in *The 9/11 Commission Report* and the Markle Foundation Task Force Report (*Creating a Trusted Information Network for Homeland Security)* clearly demonstrated the need for a nationwide capacity to share information that could detect, prevent, or deter a terrorist attack. The *Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004* and the *2007 National Strategy for Information Sharing* indicate both legislative and executive intent to establish locally controlled distributed information systems wherein potential terrorism-related information could be contributed by the 18,000 state, local, tribal, and territorial (SLTT) law enforcement agencies for analysis to determine whether there are emerging patterns or trends. Following this guidance, the NSI was developed.[13]

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.[14]

The NSI established a process that rigorously protects the privacy and civil liberties of Americans. The ISE-SAR Functional Standard v. 1.5 defines suspicious activity as:

> *"Observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity."*[15]

This definition was developed after critical input from several privacy, civil rights, and civil liberties advocacy groups, including the American Civil Liberties Union (ACLU). The SAR process is critical to sharing information about suspicious activity with a potential nexus to terrorism, which can help prevent terrorist attacks and other related criminal activity from occurring. In developing the standards and processes, the NSI leveraged the guidance and expertise provided by the Global Justice Information Sharing Initiative (Global), which serves as a Federal Advisory Committee and advises the U.S. Attorney General on justice information sharing and integration initiatives.[16]

(October 2007). pp. A1-6 http://www.ise.gov.

[12] *The NSI Concept of Operations, Version 1* (December 2008) and *ISE-FS-200, Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) Version 1.5* (May 21, 2009) http://www.ise.gov.

[13] *About the NSI,* http://nsi.ncirc.gov/about_nsi.aspx.

[14] *Nationwide SAR Initiative,* http://www.ise.gov/nationwide-sar-initiative.

[15] Ibid, *About the NSI.*

[16] Ibid.

The NSI is led by the U.S. Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI), in coordination with the Program Manager for the Information Sharing Environment (PM-ISE), Global, and the Criminal Intelligence Coordinating Council (CICC). Support of the Nationwide SAR Initiative (NSI) efforts has been publicly stated by major law enforcement associations, including the International Association of Chiefs of Police (IACP), the Major Cities Chiefs Association (MCCA), the Major County Sheriffs' Association (MCSA), the National Sheriffs' Association (NSA), and the Association of State Criminal Investigative Agencies (ASCIA).[17]

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.

On December 17, 2009, DOJ was named the executive agent to establish and operate the Program Management Office (PMO) for the NSI. Then in March 2010, DOJ established the NSI PMO within the Bureau of Justice Assistance (BJA) to support nationwide implementation of the SAR process.[18] On October 1, 2013, DHS and the FBI, in coordination with BJA, directed the nationwide transition of the NSI Shared Space to a new technology platform (eGuardian) in support of the seamless sharing of SARs. Consequently, DHS and the FBI assumed responsibility for the NSI. **Training, technical assistance, and outreach are now the responsibility of DHS, while the FBI is responsible for NSI technology.** The core mission of the NSI is to assist agencies with adopting compatible processes, policies, and standards that foster broader sharing of SARs, while ensuring that privacy, civil rights, and civil liberties are protected. Primary functions of the NSI executive agent include advocating on behalf of the initiative, providing guidance to participants at all levels, and coordinating various efforts within the NSI. **Given the criticality of privacy, civil rights, and civil liberties issues, the NSI works collaboratively with and is supported by the U.S. Department of Justice (DOJ) Privacy and Civil Liberties Office.**[19]

VI. Overview

This SOP documents the formal process for identifying and vetting TLs that may or may not lead to the reporting of an ISE-SAR to eGuardian. 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

[17] Ibid.

[18] *Background of the NSI Governance*, http://nsi.ncirc.gov/about_nsi.aspx.

[19] *NSI Governance,* http://nsi.ncirc.gov/about_nsi.aspx.

defined within this SOP and is determined to be reasonably indicative of terrorism or other criminal activity 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 eGuardian or the BRIC's criminal intelligence database.

VII. 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 (Currently, ISE-SAR Functional Standard Version 1.5):

- Defined Criminal Activity and/or Potential Terrorism Nexus Activity:[20]

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
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

[20] *ISE-SAR Functional Standard, Version 1.5 (ISE-FS-200).*

- Potential Criminal or Non-Criminal Activity Requiring Additional Fact Information During Investigation:[21]

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
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

[21] *ISE-SAR Functional Standard, Version 1.5 (ISE-FS-200).*

Note: Some of these activities, by themselves, may be constitutionally-protected and should not be reported as an ISE-SAR absent the BRIC's application of vetting procedures to determine articulable facts and circumstances that support the source agency's suspicion that the behavior observed is 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.

VIII. Responsibilities

Designated personnel within the BRIC will have primary responsibility for facilitating the TL vetting process defined in this SOP. Additional responsibilities are described below.

A. Supervisor Responsibilities

The BRIC will assign a team of trained Supervisors (Analytic and Investigative) to oversee the entire TL processing procedures for Suspicious Activity Reporting. 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.

B. Detective Responsibilities

The BRIC will assign a team of trained Detectives to perform preliminary investigative support outside of the scope of the analytic vetting procedures defined below. Detectives 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.

C. Analyst Responsibilities

The BRIC will assign a team of trained Intelligence Analysts to collate TL information, perform initial analytic vetting procedures, and enter appropriately vetted information into SharePoint as a TL entry, and when appropriate to do so, into eGuardian as an ISE-SAR. 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.

IX. 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 ISE-SAR reporting criteria; specific TL vetting procedures are detailed in Section X.

A. Collection and Review Policy

On a daily basis, Analysts will collect and review information from law enforcement systems and publicly available resources. This process may include the review of

information submitted to the BRIC for review from the general public, as well as other law enforcement, public safety and private sector security partners. Analysts will conduct an initial assessment of the information, based upon training and experience, to determine if the information may meet the criteria established in ISE-FS-200.

B. 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 SharePoint system and reviewed by a BRIC Supervisor. Note: Information retained in SharePoint should not include personal identifying information (PII).
- A Supervisor will assign each TL to a BRIC Detective for investigative follow-up and/or assign 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 supervisors will make a determination on whether to classify the information as an ISE-SAR and thus enter it into eGuardian.
- In some instances, where the nature of the behavior immediately meets ISE-SAR criteria, the information may be entered into eGuardian immediately prior to the completion of further vetting by detectives and analysts. However, this decision can only be made by a BRIC Supervisor, and the ISE-SAR will be updated in eGuardian 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 Receipt and Triage Plan*, Urgency Matrix, Immediate or Priority Factors). Reporting of the SAR to the JTTF requires review by sworn BRIC Supervisors.
- BRIC Analysts will review each TL considered for SAR vetting 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 ISE-SARs, can still possess criminal intelligence value. TLs that fall into this category -- where reasonable suspicion exists to support that a criminal predicate has been established -- may be entered into the BRIC's criminal intelligence system (CrimeNtel), accompanied by documented articulation of reasonable suspicion, and/or forwarded to the appropriate agencies and/or personnel.

C. 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. TLs considered for ISE-SAR must be reviewed and assessed by a group of designated personnel.
- 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 group assesses that the tip or lead being reviewed is of a criminal nature with no nexus to terrorism, the Supervisor will ensure that the information is turned over to the proper agency and/or personnel (outside of the BRIC); and BRIC SharePoint system is updated with disposition actions.
- If it is determined that investigative actions are needed to assist with the vetting process, the tip or lead is assigned a tracking number, entered into CaseInfo and assigned to a BRIC Detective for investigation.
- Upon receiving a Tip or Lead, initial vetting should occur as soon as practicable; during this time a determination should be made as to whether or not data regarding the identified behaviors and indicators can be entered into eGuardian as an ISE-SAR, or sent to the appropriate investigative authority outside of the BRIC (for Tips or Leads where non-terrorism information identified). As mentioned above, in some instances where the behaviors immediately satisfy those in ISE-FS-200, the information may be entered into eGuardian while the vetting is completed, and all additional investigative steps should be coordinated with the JTTF.

D. **Disposition Policy**

The BRIC's TL vetting process is designed to ensure that appropriate steps are taken to assess whether a given TL is reasonably indicative of criminal activity associated with terrorism. Towards this end, a given TL may have a number of actions taken by the BRIC to ensure that a sound assessment is achieved. All TLs will result in one or more of the following outcomes:

- ***ISE-SAR:*** Pursuant to the review, analysis, and vetting process explained in this document, the BRIC assesses that the TL is reasonably indicative of criminal activity associated with terrorism. All ISE-SARs are shared within the FBI's

eGuardian system. TLs that meet this criteria will be noted in SharePoint using the "Submitted to eGuardian" checkbox.

- ***Candidate ISE-SAR:*** Pursuant to initial review and/or analysis processes, a given TL does not immediately meet the ISE-SAR threshold; however, investigative and analytical follow-up will allow for a more thorough and informed assessment. Such TLs are noted in SharePoint using the "BRIC Investigative Follow-Up" and / or "BRIC Analytical Follow-Up" checkboxes. If investigative actions are taken, the detective will record his or her steps in CaseInfo. At the conclusion of these steps, an assessment will be made as to whether the TL meets criteria to be considered an ISE-SAR.
    - If ISE-SAR criteria is met, the TL will be shared in the FBI's eGuardian system.
    - If ISE-SAR criteria is not met, the BRIC may determine if the information should be shared with another agency/personnel and/or stored in the BRIC's criminal intelligence database (when reasonable suspicion exists to support that a criminal predicate has been established).
- ***No BRIC Action at this Time:*** Pursuant to the initial review, analysis and/or vetting processes, it is assessed that the TL is NOT reasonably indicative of criminal activity associated with terrorism. These reports may be shared with another agency/personnel and/or stored in the BRIC's criminal intelligence database (when reasonable suspicion exists to support that a criminal predicate has been established). TLs that fall into this category will be noted in SharePoint by using any combination of the following checkboxes:
    - No BRIC Action at this Time
    - Refereed to Other Agency
    - District Investigation/Other Specialized Unit
    - CrimeNtel

E. **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.

F. **Information Retention Policy**

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

- Upon initial receipt by the BRIC, the TL information may be retained for a maximum of 30 days in order to allow adequate time for detectives and analysts to determine its credibility and value. When appropriate, and based on reasonable circumstances, a BRIC Supervisor may extend the assessment period beyond 30 days in order to effectively address the TL.
- TLs entered into SharePoint **will not include personal identifying information (PII)**. Only information pertaining to the date, time, location, disposition, the behaviors/indicators, and steps taken to vet the TL will be retained. **It is important to note that the TL module in SharePoint exists purely to track workflow, document the status of a TL, and allow for administrative reporting (i.e. statistics and performance metrics).**
- Once a TL is determined to meet ISE-SAR criteria, the incident will be entered into eGuardian – which serves as the NSI SAR Data Repository (SDR) – with all appropriate information as designated by BRIC policy.
- TLs entered into SharePoint must have a status code attached and note the appropriate outcome of the vetting process.
- All information entered into SharePoint and eGuardian will be retained in a manner consistent with the BRIC's Criminal Intelligence File Guidelines and Privacy, Civil Rights and Civil Liberties policy.[22]
    - Positive Nexus to Terrorism: 5 years
    - Inconclusive Nexus to Terrorism: 5 Years
    - No Nexus to Terrorism: 90 Days
- Aggregate data from TLs will be retained indefinitely for statistical reporting and performance measurement.

X. Tips and Leads Vetting Process and Detailed Procedures

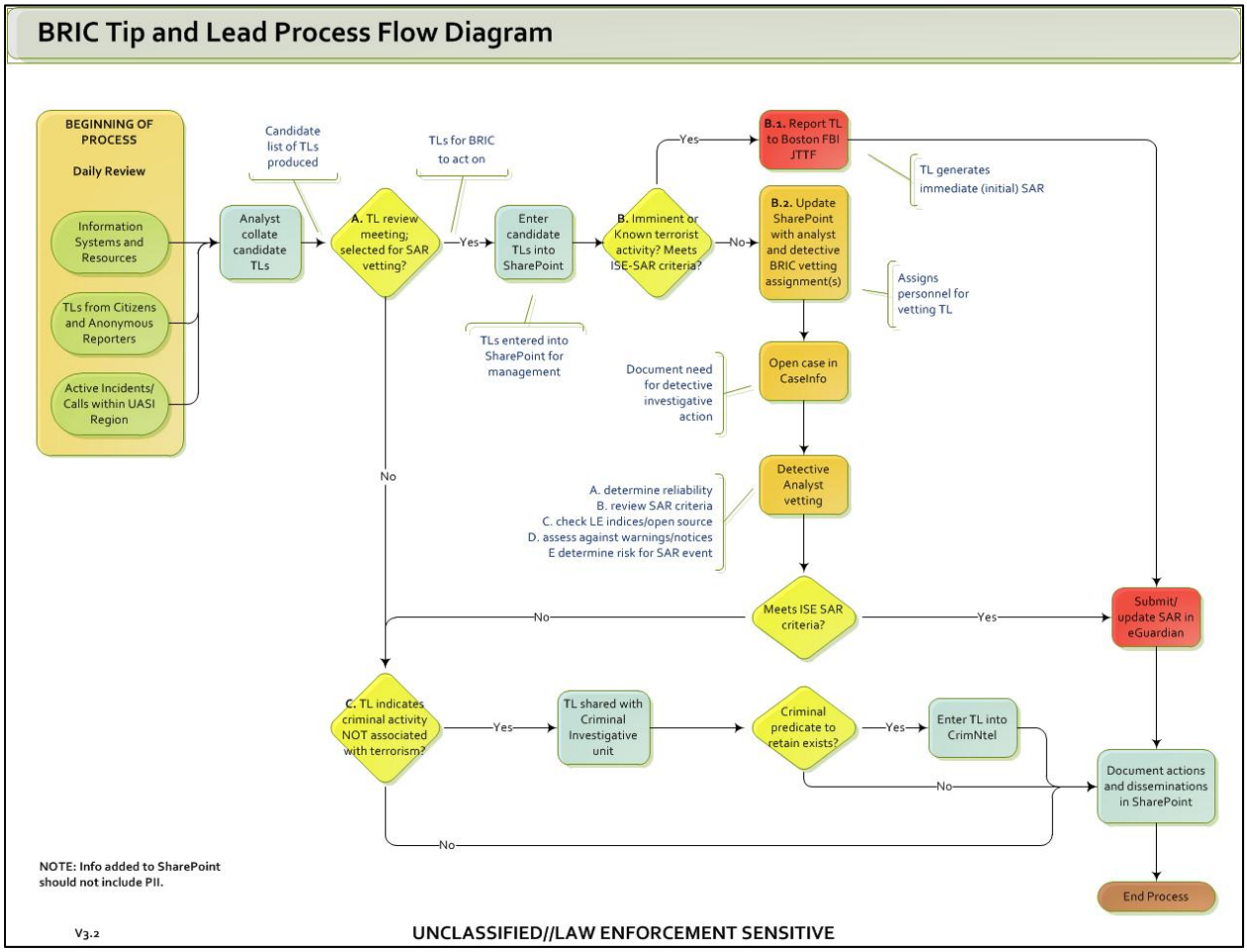
This section provides a flow diagram for the BRIC TL vetting process and provides detailed procedures for each step of its execution. All BRIC staff members with TL vetting responsibilities, whether detective or analyst, will adhere to the steps described in this

[22] The FBI's Privacy Impact Assessment (January 2014) notes that ISE-SARs shared with eGuardian will have the following default retention schedules based on the disposition given by the FBI: Positive Nexus to Terrorism – 5 years; Inconclusive Nexus to Terrorism – 5 Years; No Nexus to Terrorism – 120 Days. The BRIC has chosen to reduce the retention on records with No Nexus to Terrorism to 90 days to maintain consistency with its internal retention policies. See: eGuardian System Privacy Impact Assessment Update, dated January 8, 2014. http://www.fbi.gov/foia/privacy-impact-assessments/eguardian-threat/#update.

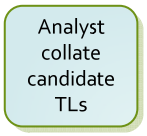
section. The BRIC TL vetting process is executed on a daily basis and begins with the collation of information from a variety of law enforcement information systems and publicly available resources. The process results in one of four outcomes that correlate to the four disposition codes described in Section IX.D.

A. Tips and Leads Vetting Process Diagram

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



B. Detailed TL Vetting Procedures

Step	Description	Product/Result
	BRIC analysts collate information from a variety of information systems and publicly available resources – to include recent incidents and calls for service, information reported by the public, and live, active public safety incidents – and identify activities that may have a nexus to terrorism.	List of TLs that are candidates for formal BRIC vetting.
A. 	**A.** TLs are reviewed and discussed with a supervisor. ***Decision**: If TL is of terrorism nature, it will be selected for formal vetting by the BRIC (Go to "B"). If not, review to determine if it provides indication of other criminal activity (Go to "C").*	List of SAR Candidate TLs that will be formally vetted by the BRIC.
	New TL data is added to the SharePoint system for each candidate TL.	TLs records are added to the SharePoint system.

	B. Imminent or Known terrorist activity? Meets ISE-SAR criteria? **or** **C.** TL indicates criminal activity NOT associated with terrorism?	Go to Steps B. or C. depending on whether or not TLs appear terrorism or non-terrorism related.	
B.	**B.** Imminent or Known terrorist activity? Meets ISE-SAR criteria?	TL is assessed to determine if it is indicative of "imminent" or "known (not imminent)" terrorist activity, and to determine if it meets ISE-SAR criteria based on initial assessment. ***Decision**: If TL meets these criteria, it will be reported to the JTTF supervisor immediately to aid in deconfliction, and to determine whether TL warrants FBI/JTTF involvement (Go to B.1.) If it does not meet these criteria, the TL will undergo analytic and investigative vetting (Go to B.2.)*	TLs that meet ISE-SAR criteria and are indicative of "imminent" or "known/ not imminent" terrorist activity will be presented to the JTTF for action.
B.1.	**B.1.** Report TL to Boston FBI JTTF	TL indicating "Imminent" or "Known (not imminent)" terrorist activity is forwarded to the JTTF supervisor. Behaviors meet ISE-SAR criteria.	BRIC may continue its vetting process on the TL after it is forwarded to the JTTF; however, all additional investigative activity will be coordinated with the JTTF.
	Submit/ update SAR in eGuardian	Analyst enters data from TL into eGuardian to generate an ISE-SAR and share accordingly.	New ISE-SAR is generated (or existing ISE-SAR is updated) and submitted to eGuardian.

B.2.

Document actions and disseminations in SharePoint	Analyst updates the SharePoint system with analytic and/or vetting actions taken, TL disposition code, and all external agency disseminations of TL information (JTTF, eGuardian, other agencies, etc.).	TL record in the SharePoint system updated with vetting and dissemination actions taken.
End Process	End Process	Vetting process completed.
B.2. Update SharePoint with analyst and detective BRIC vetting assignment(s)	For each TL selected for formal BRIC vetting, SharePoint will be updated with the detective and analyst assigned to lead the vetting activity.	TLs to be formally vetted are assigned a detective and/or analyst in the SharePoint system.
Open case in CaseInfo	The TL is assigned a tracking number and entered into CaseInfo, the BRIC's investigative case management application.	New CaseInfo case is opened to document investigative activities associated with the TL.
Detective Analyst vetting	BRIC detectives and analysts review information in the TL to determine if it requires further investigation.	Information is gathered to support decision to fully investigate the TL.
Meets ISE SAR criteria?	Detectives/Analysts and Supervisors determine if TL meets/does not meet ISE-SAR reporting criteria. ***Decision**: If TL meets ISE-SAR criteria, submit to eGuardian. If not, review for indication of criminal activity not associated with terrorism (Go to C.).*	TLs meeting ISE-SAR reporting criteria are identified.
Submit/ update SAR in eGuardian	Analyst creates new ISE-SAR (or updates existing ISE-SAR) in eGuardian.	New ISE-SAR is generated (or existing ISE-SAR is updated) in the NSI SAR Data Repository (SDR).

	Document actions and disseminations in SharePoint	Analyst updates the SharePoint system with analytic and/or vetting actions taken, TL disposition code, and all external agency disseminations of TL information (JTTF, eGuardian, other agency).	TL record in the SharePoint system updated with vetting and dissemination actions taken.
	End Process	End Process	Vetting process completed.
C.	**C.** TL indicates criminal activity?	**C.** TLs are further reviewed for potential criminal activity (non-terrorism). ***Decision**: If TL is of criminal nature with no nexus to terrorism, it is turned over to an investigative unit for further action.*	List of criminal TLs that will *not* be vetted by BRIC.
	TL shared with Criminal Investigative unit	BRIC shares TL with appropriate criminal investigative agency/ unit/personnel.	Criminal investigative agency/unit/personnel takes over investigation of TL.
	Enter candidate TLs into SharePoint	TL data is added to or updated in the SharePoint system for each candidate TL.	TLs records are added to or updated in the SharePoint system.
	Criminal predicate to retain exists?	Detectives/Analysts determine if the information in the TL supports retention of the information as criminal intelligence, per 28 CFR Part 23.[23] ***Decision**: If "reasonable suspicion" or "criminal predicate" exists, enter into CrimNtel.*	TLs that can be retained as criminal intelligence are identified.

[23] "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

Enter TL into CrimNtel	Detective/Analyst enters TL information into CrimNtel, the BRIC intelligence management system.	New criminal intelligence record is created in CrimNtel.
Document actions and disseminations in SharePoint	Analyst updates the SharePoint system with vetting actions taken, TL disposition code, and all external agency disseminations of TL information (JTTF, SAR, other agencies).	TL record in the SharePoint system updated with vetting and dissemination actions taken.
End Process	End Process	Vetting process completed.

XI. SAR Policy Refresh

All BRIC Staff will receive an annual refresher session on matters covered within the SAR Policy. The refresher will include re-issuance of the most current SAR Policy as well as a related discussion covering the responsibilities and standards as outline within the SAR Policy to increase familiarity and reinforce compliance. Please note that in addition to this refresher, all BRIC personnel are required to participate in annual training related to Privacy, Civil Rights and Civil Liberties.

XII. Privacy, Civil Rights 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 rights, civil liberties, and other legal rights of the general public; refer to the *BRIC Information Privacy, Civil Rights and Civil Liberties Protection Policy*.

XIII. Date Plan Implemented and Updated

This SOP was implemented on November 14, 2011, and it was last updated on September 9, 2014. This SOP will be reviewed (at least) annually, and will be updated, refreshed, and revised when necessary by the Director and senior BRIC/BIA personnel.

XIV. 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 Privacy Civil Rights and Civil Liberties Protection Policy
- BRIC Threat Information Receipt and Triage Plan
- BRIC Criminal Intelligence File Guidelines

This plan was further informed by the following documents:

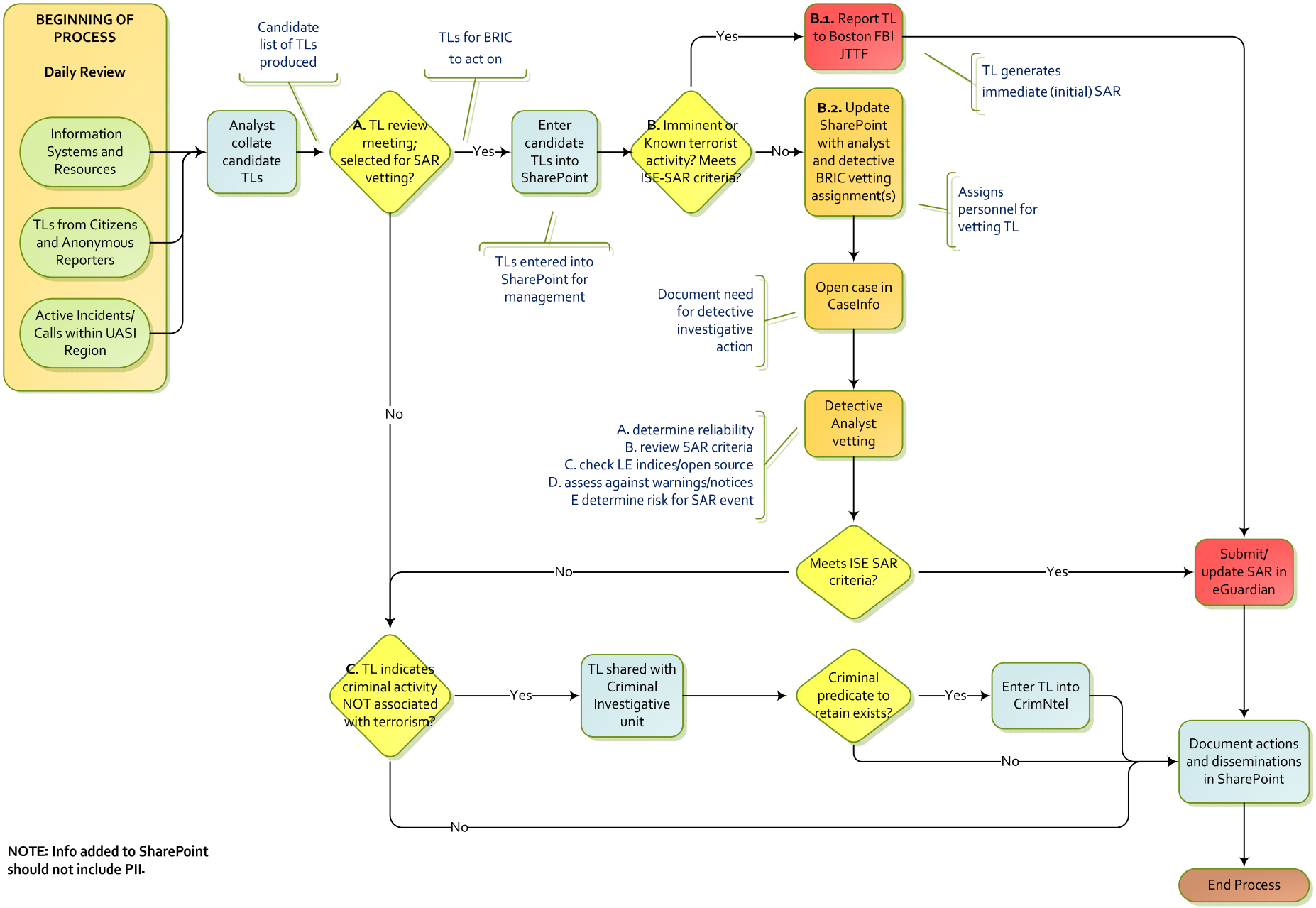
- Baseline Capabilities for State and Major Urban Area Fusion Centers, September 2008.
- National Suspicious Activity Report (SAR) Initiative (NSI)
- Suspicious Activity Reporting Process Implementation Checklist
- Nationwide Suspicious Activity Reporting Initiative Concept of Operations, December 2008
- 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) 200 (Version 1.5)
- DOJ Tips and Leads Issue Paper
- Fusion Center Guidelines, April 2006.
- National Strategy for Information Sharing, October 2007.
- National Strategy for Information Sharing and Safeguarding, December 2012.
- NSI SAR Data Repository CONOPS, January 2014.

XV. Appendices

This plan includes the following appendices:

- Appendix A – Tips and Leads Vetting Process Diagram
- Appendix B – Urgency Matrix

Appendix A: Tips and Leads Process Diagram



NOTE: Info added to SharePoint should not include PII.

Appendix B: Threat Information Triage Plan Urgency Matrix

		URGENCY		
		IMMEDIATE	**PRIORITY**	**ROUTINE**
FACTOR	**TIME**	Imminent	Known but not imminent	Not known or not relevant
	TARGET	Specific reference to a priority location or named critical infrastructure, person, group, or organization.	General, non-specific reference to a location or named critical infrastructure, person, group, or organization.	No reference to location or named critical infrastructure, person, group, or organization.
	THREAT	Clear details of a natural or man-made occurrence, individual, entity, or action that has the potential to cause harm. Occurrence, individual, entity, or action has intent and/or capability to cause harm.	Unclear details of a natural or man-made occurrence, individual, entity, or action that has the potential to cause harm. Unclear if occurrence, individual, entity, or action has intent and/or capability to cause harm.	No details of a natural or man-made occurrence, individual, entity, or action that has the potential to cause harm. No subjects identified, or occurrence, individual, entity, or action does not have intent and/or capability to cause harm.
	SOURCE	Source is reliable and credible.	Source is identified but reliability cannot be rated.	Anonymous or source is known to be unreliable.
	CONTEXT	Occurrence or individual or entity indicated, displayed or engaged in activity – lacking a plausible, legitimate explanation – that strongly suggests convergence with specific, credible threat reporting and/or risk of harm.	Occurrence or individual or entity indicated, displayed or engaged in unusual behavior that lacked a plausible, legitimate explanation and did not fit typical activity patterns.	Occurrence or individual or entity indicated, displayed or engaged in ordinary behavior that was interpreted as unusual, suspicious or harmful.