Threat Information Receipt and Triage Plan
Boston Regional Intelligence Center

Abstract
Provides BRIC staff with operating procedures that govern the required actions taken by the BRIC in response to the reception and identification of threat-related information from Federal, State, or Local partners, or other sources.

BOSTON REGIONAL
INTELLIGENCE CENTER
BRIC

Contents

I. Title

Boston Regional Intelligence Center (BRIC) Standard Operating Procedure for Threat Information Receipt and Triage; hereinafter referred to as the Boston Regional Intelligence Center (BRIC) Threat Information Receipt and Triage Plan.

II. Purpose and Background of this Plan

The Boston Regional Intelligence Center (BRIC) has a shared responsibility with the Federal government to prevent, protect, respond, and recover from threats on our homeland. The BRIC supports and participates in the National Strategy for Information Sharing, which designates fusion centers as the focal point for receiving and sharing terrorism-related information to the stakeholders within their Area of Responsibility (AOR).[1] [2]

The BRIC's mission encompasses an "All Crimes, All Hazards" approach.[3] [4] Therefore, in addition to its counterterrorism responsibilities, the BRIC is responsible for gathering, analyzing and sharing information related to criminal activity, to include firearm, gang and drug activity, violent crime and property crime offenses, as well as threats of other criminal activity and hazards that may affect public safety.[5]

The purpose of this plan is to articulate standardized procedures to govern the required actions taken by the BRIC in response to the reception and identification of threat-related information.[6]

The procedures contained herein are intended to remain at all times compliant with the BRIC's Privacy, Civil Rights/Liberties Protection Policy and other existing policies and procedures.

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.

---

[1] *National Strategy for Information Sharing,* 2007, p. A1-8, State & Local Responsibilities.

[2] The BRIC's Area of Responsibility includes the cities and towns that represent the Metro-Boston Homeland Security Region (MBHSR): Boston, Brookline, Cambridge, Chelsea, Everett, Quincy, Revere, Somerville, and Winthrop.

[3] See Definitions section of this plan.

[4] *National Strategy for Information Sharing*, Ibid.

[5] Baseline Capabilities for State and Major Urban Area Fusion Centers, 2008, p. 2.

[6] See *Critical Operational Capabilities for State and Major Urban Area Fusion Centers Gap Mitigation Guidebook*, V2.0, July 2012. This plan addresses the requirements of Critical Operating Capability (COC) One – Receive: Ability to Receive Classified and Unclassified Information from Federal Partners. All jurisdictional law enforcement and allied agencies – to include first responders and private sector partners – are encouraged to report information that may help prevent criminal activity (to include terrorism) and identify potential terrorist and criminal conspirators/perpetrators.

IV. Definitions

Area of Responsibility (AOR): The BRIC's Area of Responsibility includes the cities and towns that represent the Metro-Boston Homeland Security Region (MBHSR) or Urban Areas Security Initiative (UASI): Boston, Brookline, Cambridge, Chelsea, Everett, Quincy, Revere, Somerville, and Winthrop.

All-Crimes Approach: An approach that incorporates traditional criminal activity, terrorism and other high-risk threats into the existing fusion center framework, to ensure that regional information sharing and analysis supports a shared responsibility of public safety within the region. This approach recognizes that there may be a nexus between types of criminal activity and terrorism.[7]

All-Hazards Approach: An approach that incorporates preparedness for terrorist attacks, major disasters, and other emergencies within the United States.[8] This approach recognizes that the fusion center plays a role in the region's prevention, protection, response and recovery efforts for such events.

Federally-Generated Information: Time sensitive, threat information that is initiated at the Federal level and delivered to the BRIC. Such information may take the form of alerts, warnings, notifications, or other products that should be accessed, reviewed, and appropriately disseminated in a timely manner.

National Terrorism Advisory System (NTAS): NTAS replaces the color-coded Homeland Security Advisory System (HSAS). This system communicates information about terrorist threats by providing timely, detailed information to the public, government agencies, first responders, airports and other transportation hubs, and the private sector.

Officer in Charge (OIC): An Officer in Charge (OIC) will be a BRIC Supervisor, designated by BRIC leadership on a case-by-case basis to have the authority and responsibility for coordinating and managing the BRIC's operational support role during an incident or event. This responsibility includes the authority for the ordering and directing BRIC resources, and the development of objectives.

Threat Information: Information pertaining to a natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment and/or property. Note: This plan refers to threats occurring in

[7] Baseline Capabilities, p. 43.

[8] Homeland Security Presidential Directorate 8 (HSPD-8), December 17, 2003.

or directed towards the Metropolitan Boston Homeland Security Region (MBHSR), as well as general threat information that may have local implications to public safety in the region.

Procedures

The paragraphs below provide specific procedures for threat information triage within the BRIC, and subsequently, to appropriate partners and stakeholders.

V. Receipt of Threat Information

BRIC personnel may receive or identify threat information relative to criminal activity and hazardous events from a variety of sources to include citizens, local, state and federal law enforcement and intelligence agencies, homeland security and public safety agencies, and private sector entities. Threat information may be received or identified at the BRIC electronically through numerous unclassified and classified systems.

When threat information is received or identified at the BRIC, it is the responsibility of the receiving personnel to provide an initial evaluation and assessment of the information for its relevancy and local implication to the BRIC's various stakeholders[9], and assess the credibility of the source. All information received or identified should be reviewed with a BRIC Supervisor to assess appropriate options for next steps.

A. Classified and Unclassified Systems Access

Authorized personnel within the BRIC may receive or identify both classified and unclassified federally-generated threat information via systems available to the BRIC. The information may be contained in authorized Federally-administered systems or BPD-administered systems.

It is the responsibility of the BRIC Director and BRIC Security Officer to ensure all designated staff have access to appropriate and necessary systems and portals so they may assess the information for relevancy and local implications.

The BRIC Director and Security Officer will ensure that designated personnel within the BRIC are trained on the use of classified and unclassified systems that contain the federally-generated information.

B. Acknowledgement of Receipt of Threat Information

Some time-sensitive federally-generated alerts, warnings and notifications may require a formal acknowledgement by representatives from the recipient organization (BRIC) to confirm receipt of the information.

[9] Stakeholders include all federal, state, local, tribal and territorial law enforcement, intelligence, public safety, public health, and private sector organizations that benefit from threat and hazard prevention, protection, response and recovery efforts in the Metro Boston Area.

- When such information is received and acknowledged a BRIC Supervisor must be alerted and briefed on the information.
- It will be the responsibility of the BRIC Supervisor to coordinate additional notifications and handling of the information.
- A BRIC Supervisor will coordinate dissemination at an appropriate level for specific audiences requiring the information.
- A BRIC Supervisor should coordinate with Federal Agency partners as appropriate to address any inquiries or handling requirements for the information.

VI. Evaluation of Threat Information

When threat information is received and identified at the BRIC, it is the responsibility of the receiving personnel to evaluate and assess this information for its relevancy and local implications in order to support public safety decision making.

NOTE: Initial evaluation and assessment should be conducted immediately upon receipt and identification, but a more thorough evaluation and assessment should be conducted shortly thereafter under the guidance and direction of a BRIC Supervisor.

Information received and identified by BRIC personnel should be evaluated and prioritized utilizing the following considerations:

- Can the BRIC determine the circumstance under which the information was obtained?
- Does the context of the information pose an imminent threat?
- Is the information requested or needed by another agency immediately?
- Is the information associated with a current investigation known to the BRIC?
- Does the information need to be routed to an appropriate law enforcement or public safety agency, and/or critical infrastructure sector?

Information Evaluation also includes, whenever possible, determining the source's reliability and the validity, timeliness of the information, and consistency with previous reporting. As part of the evaluation process, the following questions should be considered, but are not intended to be all inclusive:

- Is the source credible, meaning the source can be considered reliable or the information is considered plausible?
- Is the information relevant?
- Is the information current?
- Does the information contribute to the historic context of an identified issue?
- Does the information corroborate, mitigate, amplify, or refute previously reported information?
- Is there a restriction on further dissemination?

- Does further disseminating the information support the overall BRIC mission and uphold the security of the MBHSR, State of Massachusetts or the Nation?

When personnel have made a full evaluation and have determined that the information is credible and relevant to the BRIC's Area of Responsibility (AOR), this information may be documented in the appropriate BRIC-administered system(s) and shared with BRIC Supervisors to determine next steps and dissemination procedures.

VII. Triage Process: Coordination, Analysis and Production Requirements

The following triage system has been designed for guidance; it presents three (3) scales of urgency to be applied to threat information received or identified at the BRIC.

		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.

- BRIC personnel should use their best judgment for appropriate Triage protocols, and be aware that information may not always fit perfectly into the matrix categories and may require using discretion.
- All information is rated in relation to the initial report received by the BRIC, or identified by BRIC personnel, and it can be escalated or reduced as a result of a change in known information.

A. Immediate and Priority Information

Based on the guidelines provided below, "Immediate" and "Priority" Information should be granted precedence over other incoming or identified information unless directed otherwise by a BRIC Supervisor.

- Imminent threat information will be brought to the attention of a BRIC Supervisor.
- BRIC Supervisors should subsequently update the BIA Bureau Chief and other BRIC leadership for situational awareness and coordination purposes.
- BRIC Supervisors, in coordination with the Bureau Chief and/or BRIC leadership, will determine if a unified BRIC response is necessary. If so, appropriate BRIC staff will be coordinated to provide analytic and/or investigative support under the direction of a designated BRIC Officer In Charge (OIC).
- The BRIC OIC will assume responsibility for coordinating BRIC actions, resources and communications while the event is being supported by the BRIC.
- If necessary, the threat information will be documented in the appropriate BRIC-administered system and communicated/coordinated to appropriate stakeholders:
    - Terrorism-related threat information will be coordinated/communicated to the FBI Joint Terrorism Task Force via the BRIC's JTTF Supervisor.
    - Threat information specific to a police District within the City of Boston, or a partner agency/jurisdiction, will be coordinated/communicated to the respective District's/agency's leadership and established points of contact.
    - Threat information indicating a risk to or impact on the private sector business community and/or critical infrastructure systems or assets will be coordinated/communicated to the appropriate private sector and/or government stakeholders.
    - Threat information indicating a risk to the general public will be coordinated/communicated through BPD Media Relations for appropriate public release.

- BRIC personnel should continue a persistent review and assessment of all available information related to the threat. This may include information related to potential suspects, targets or locations of interest.
- BRIC personnel should compile and prepare appropriate briefing materials that concisely articulate the issue, such as: Who, What, When, Where, Why, and How; and address all identified information/intelligence gaps suggesting the need for additional information.
- When appropriate, and under the direction and guidance of the BRIC OIC or a Supervisor, summary reports and/or situational awareness reports (Sit Reps) may be disseminated to alert, notify and support awareness with specific audiences and leadership.

B. Routine Information

Routine, Low Urgency Information should be assessed and shared with BRIC personnel and Supervisors, in a timely manner, to ensure situational awareness and determine:

- If the information is related to an ongoing matter being supported within the BRIC;
- If the information should be triaged to another agency's leadership or investigative

/analytic unit;
- If the information should be further disseminated to appropriate stakeholders.
- NOTE: Routine threat information may escalate to a higher urgency at any time. BRIC personnel should remain vigilant for changes in information that may support a change in urgency and thus an enhanced BRIC response.

VIII. Dissemination

As appropriate, threat information will be disseminated in a timely and efficient manner to all agencies with a mission-related right and need to know.

A. If the threat information is determined to be relevant to the BRIC's AOR, the information is then disseminated to the BRIC's stakeholders in accordance with appropriate BRIC dissemination procedures, taking into account the audience, legal restrictions, and required handling labels.

Federally-generated threat information may require coordination between a BRIC Supervisor and partner agencies (i.e. DHS I&A and the FBI Boston Field Office) prior to disseminating threat information to stakeholders. A BRIC Supervisor may also coordinate with the Commonwealth Fusion Center for deconfliction purposes and to ensure a unified message regarding the threat is disseminated to shared stakeholders.

If it is determined by a BRIC Supervisor that threat information should be disseminated to the general public, the BRIC will coordinate the release of appropriate information with the Boston Police Department's Office of Media Relations. Note: The BRIC does not disseminate information directly to the public media.

B. National Threat Advisory System Alerts (NTAS)

If the BRIC receives a NTAS alert, as defined by the U.S. Department of Homeland Security, the BRIC will coordinate the release of such information with the BPD's Office of Media Relations and each UASI jurisdiction's BRIC Point of Contact in accordance with the specific guidance accompanying the alert. Furthermore, when necessary, the BRIC will issue Situational Awareness Reports (Sit-Reps) to update all relevant public safety partners with important information related to the NTAS Alert.

IX. Dates Plan Implemented and Updated

This SOP was implemented on July 10, 2012, and **it was last updated on September 15, 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.

X. References

This plan includes references to, and should be used in conjunction with, the following documents:

- Baseline Capabilities for State and Major Urban Area Fusion Centers, September 2008
- BRIC Information Privacy, Civil Rights and Civil Liberties Protection Policy
- Critical Operational Capabilities for State and Major Urban Area Fusion Centers Gap Mitigation Guidebook, V2.0, July 2012
- National Strategy for Information Sharing, October 2007
- National Strategy for Information Sharing and Safeguarding, December 2012