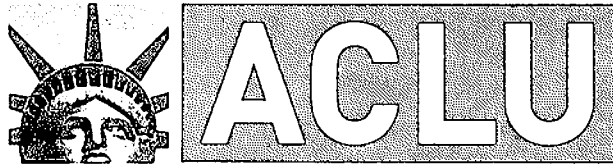


THE  
ROGER  
BALDWIN  
FOUNDATION  
OF ACLU,  
INC.



**ROGER BALDWIN FOUNDATION  
OF ACLU, INC.**

SUITE 2300  
180 NORTH MICHIGAN AVENUE  
CHICAGO, ILLINOIS 60601-1287  
(312) 201-9740  
FAX (312) 201-9760  
WWW.ACLU-IL.ORG

December 16, 2011

Superintendent Garry F. McCarthy  
Chicago Police Department  
3510 S. Michigan Avenue, 5th Floor  
Chicago, Illinois 60653  
Fax: 312-745-6963

**Re: The CPD's Crime Prevention Information Center**

Dear Superintendent McCarthy:

On behalf of the ACLU of Illinois, and its more than 10,000 members and supporters in the City of Chicago, I write to make two proposals regarding the privacy policies of the "fusion center" operated by the Chicago Police Department ("CPD"), known as the Crime Prevention Information Center ("CPIC"). We make these proposals based on information we obtained last year through FOIA requests to the CPD. We made these same proposals to your predecessor by letter of January 10, 2011.

First, the CPD should prohibit CPIC staff from collecting, maintaining, or disclosing information about individuals and groups absent "reasonable suspicion" of criminal activity. *See infra* Part I.

Second, the CPD should prohibit CPIC staff from collecting, maintaining, or disclosing information about individuals and groups based, in whole or in part, on their race, ethnicity, or other identifying characteristics, or on their political and religious beliefs, associations, and activities – unless such information directly relates to criminal conduct or activity and there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity. *See infra* Part II.

**I. A "reasonable suspicion" standard.**

Based on the information that the ACLU has obtained to date, it appears that the CPD has not adopted a "reasonable suspicion" standard for when CPIC staff may gather, maintain, and disclose information about individuals and groups. If this is not correct, please promptly advise me. The ACLU recommends that the CPD adopt such a standard.

**A. The current CPD/CPIC standard.**

The CPD/CPIC “ISE-SAR<sup>1</sup> Privacy, Civil Rights, and Civil Liberties Protection Policy” of July 2009 (hereafter “ISE-SAR Privacy Policy”) states the following rule regarding when CPIC employees may collect and maintain information about “suspicious activity”:

The CPIC will seek or retain information which a source agency (the CPIC or other agency) has determined constitutes “suspicious activity” and which:

- Is based on (a) a criminal predicate or (b) a possible threat to public safety, including potential terrorism-related conduct.
- Is relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents, the resulting justice system response, or the prevention of crime.
- The source agency assures was acquired in accordance with agency policy and in a lawful manner.

See Exh. 1 at Part E(1).

This policy defines “suspicious activity” as “[r]eported 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 (illegal) intention.” *Id.* at p. 16 (emphasis added). See also Exh. 2 (CPD Deployment Operations Center Special Order 09-10 regarding eGuardian of March 2009) at p. 1 (same). Critically, this definition uses the unqualified term “indicative,” as opposed to the qualified standard of “reasonably indicative” that is currently used by the federal government in its SAR system (discussed below).

This CPD policy also states the following rule regarding the CPIC’s disclosure of personal information: “Access and disclosure of personal information will be allowed to agencies and individual users only for legitimate law enforcement purposes and for the performance of official duties in accordance with law.” See Exh. 1 (CPD/CPIC ISE-SAR Privacy Policy) at Part I(3). See also Exh. 3 (CPD/CPIC “Privacy Policy” of July 2009) at Part III (“Information obtained from or through the CPIC can only be used for lawful purposes. A lawful purpose means the request for data can be directly linked to a law enforcement agency’s active criminal investigation or is a response to a confirmed lead that requires follow-up to prevent a criminal act.”).

**B. Why the current CPD/CPIC standard does not adequately protect privacy.**

The limits provided in the current CPD/CPIC policy – a criminal predicate, law enforcement relevance, and compliance with law – are no substitute for a “reasonable suspicion” standard. Rather, these limits do not sufficiently guide and limit officer discretion, and do not provide a meaningful basis for supervisory review. There is a substantial danger that CPIC employees applying these limits will target individuals and groups based on their political or religious

---

<sup>1</sup> “ISE” means the Information Sharing Environment, and “SAR” means Suspicious Activity Reporting.

beliefs, activities, and associations, and then collect, maintain, and disclose sensitive private information about them.

This danger is aggravated by training materials regarding suspicious activity reporting, which were created by the federal government and are used by the CPD, stating: “If it looks unusual to you – the expert – it probably is.” *See* Exh. 4 at p. 11. This training invites officers to target individuals and groups based on subjective hunches, as opposed to objective factors.

Unfortunately, in the absence of appropriate privacy safeguards, fusion centers in other states have engaged in improper political and religious targeting. For example:

- The Maryland fusion center targeted a group opposing the death penalty.<sup>2</sup>
- The Missouri fusion center targeted supporters of Congressman Ron Paul.<sup>3</sup>
- The Virginia fusion center targeted historically black colleges.<sup>4</sup>
- The Wisconsin fusion center targeted protesters on both sides of the abortion debate.<sup>5</sup>

Information collected and maintained by the CPIC in many cases is disclosed to a vast number of persons, both in government and the private sector. *See* Exh. 5 (U.S. Dept. of Justice *et al.*, “Final Report: ISE-SAR Evaluation Environment,” January 2010) at p. 103 (“CPD disseminates suspicious activity alerts, warnings, and notifications via intelligence bulletins to all law enforcement officers, as well as selected managers of critical infrastructure and other government agencies.”). Thus, it is important to ensure appropriate limits on what information is collected and maintained.

The “reasonable suspicion” standard that the ACLU herein proposes is a “best practice” used by other law enforcement agencies for intelligence databases like the CPIC:

- The Illinois State Police (“ISP”) recently adopted, for its fusion center known as the Statewide Terrorism and Intelligence Center (“STIC”), a requirement of “reasonable suspicion” for collecting, maintaining, and disseminating information about particular individuals. *See* Exh. 6 (ISP/STIC Privacy Policy of 2010) at Articles V(A), V(B), V(C)(1), V(C)(4), V(G)(1), VI(B)(1)(a).

---

<sup>2</sup> *See* <http://www.governor.maryland.gov/documents/SachsReport.pdf>; <http://www.aclu-md.org/Index%20content/NoSpying.html>.

<sup>3</sup> *See* <http://www.columbiatribune.com/news/2009/mar/14/fusion-center-data-draws-fire-over-assertions/>.

<sup>4</sup> *See* <http://www.aclu.org/technology-and-liberty/fusion-center-declares-nation-s-oldest-universities-possible-terrorist-threat>.

<sup>5</sup> *See* <http://www.cnsnews.com/news/article/61104>; <http://www.aclu.org/spy-files/more-about-fusion-centers>.

- The Office of the Director of National Intelligence (“ODNI”) recently adopted, for its nationwide Information Sharing Environment (“ISE”) comprised of SARs, a definition of “suspicious activity” as “observed behavior *reasonably indicative* of pre-operational planning related to terrorism or other criminal activity.” See Exh. 7 (ODNI-ISE memorandum of May 2009 regarding new Functional Standard for SAR) at p. 1 (emphasis added). See also Exh. 8 (ISE-SAR Criteria Guidance) (requiring “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”) (emphasis added).<sup>6</sup>
- Federal regulations have long required, for state and local criminal intelligence databases funded by the federal government, “reasonable suspicion” for collecting and maintaining information about particular individuals. See 28 C.F.R. §§ 23.3(b)(3)(i), 23.20(a), 23.20(f)(1).

In sum, the ACLU proposes that the CPD adopt a rule providing that CPIC staff cannot gather, maintain, or disclose information about an individual or a group absent reasonable suspicion that such individual or group is engaged in criminal activity. This reform might be accomplished by using the qualified term “reasonably indicative,” instead of the unqualified term “indicative,” in the aforementioned CPD/CPIC ISE-SAR Privacy Policy at Part E(1). See Exh. 1.

## **II. A ban on using race, religion, and the like as a factor giving rise to suspicion.**

Based on the information that the ACLU has obtained to date, it appears that the CPD does not prohibit CPIC staff from using race, religion, ideology, and the like as *a* factor giving rise to suspicion, provided that it is not *the only* factor. If this is not correct, please promptly advise me. The ACLU recommends that the CPD adopt a rule providing that CPIC staff cannot use such considerations, in whole or in part, as factors giving rise to suspicion – unless such information directly relates to criminal conduct or activity and there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity.

### **A. The current CPD/CPIC standard**

The CPD/CPIC ISE-SAR Privacy Policy states:

Source agencies will agree not to collect and submit SAR information, and the CPIC will not retain SAR or ISE-SAR information, about any individual that was gathered *solely* on the basis of that individual’s religious, political, or social views or activities; participation in a particular noncriminal organization or lawful event; or race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation.

---

<sup>6</sup> The current version of this federal rule (Functional Standard 1.5 adopted in May 2009) uses this “reasonably indicative” standard. The prior version of this federal rule (Functional Standard 1.0) used the mere “indicative” standard still used today by the CPD’s CPIC.

*See* Exh. 1 at Part E(2) (emphasis added). *See also* Exh. 2 (CPD Deployment Operations Center Special Order 09-10 of March 2009 regarding eGuardian) at p. 1 (“No entry into eGuardian [a federal database of suspicious activity reports] may be based *solely* on the ethnicity, race or religion of any individual or *solely* on the exercise of rights guaranteed by the First Amendment . . .”) (emphasis added).

Moreover, lists of “potential indicators of terrorist activities,” jointly issued by the CPD and the federal government, indicate that political and religious belief, activity, and association can be a factor that contributes to suspicion. *See* Exh. 9 (list regarding “mass transportation,” including “unusual comments made regarding anti-U.S., radical theology”); *id.* (list regarding “construction sites,” including “environmental and/or antigovernment slogans, banners, or signs at the site or in the nearby area that threaten or imply violence”); *id.* (list regarding “wholesale distributors,” including “comments involving radical theology” and “anti-U.S. sentiments”).

**B. Why the current CPD/CPIC standard does not adequately protect privacy.**

These policies explicitly allow CPIC employees to use race, religion, ideology, and the like as factors giving rise to suspicion – provided that suspicion is not based “solely” on these considerations. Thus, for example, if a Caucasian person and an Arab person are both engaged in identical photography on a public sidewalk (same time, place, subject, and equipment), a CPIC employee might treat the latter but not the former as suspicious, based in part (though not “solely”) on the latter’s ethnicity. Such distinctions raise First and Fourteenth Amendment concerns, unfairly burden people based on identity and belief, and chill and deter expressive and religious activity.

The rule that the ACLU herein proposes is a “best practice” used by other law enforcement agencies for intelligence databases like the CPIC. For example:

- The ISP recently adopted the following rule for its STIC fusion center: “Intelligence personnel may not collect and maintain information concerning race, ethnicity, citizenship, place of origin, age, disability, gender, sexual orientation, political, religious or social views, associations, or activities of any individual or any group unless [i] such information directly relates to criminal conduct or activity and [ii] there is reasonable suspicion that the subject of the information is or may be involved in such criminal conduct or activity.” *See* Exh. 6 (ISP/STIC Privacy Policy of 2010) at Article V(C)(10).
- The federal ODNI recently promulgated, for its nationwide SAR system, a rule providing that “factors such as race, ethnicity, national origin, or religious affiliation should not be considered as factors that create suspicion (except if used as part of a specific suspect description).” *See* Exh. 7 (ODNI-ISE memorandum regarding SAR) at p. 1. *See also* Exh. 8 (ISE-SAR Criteria Guidance) (same). This ODNI rule further provides that “those categories of activity which are generally First Amendment-protected activities should not be reported in a SAR or ISE-SAR absent articulable facts and circumstances to support the source agency’s suspicion that the behavior observed is reasonably indicative of criminal activity associated with terrorism.” *See* Exh. 7.

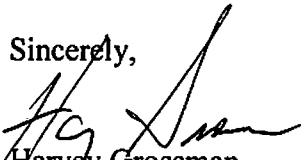
- Federal regulations have long provided, for state and local criminal intelligence databases funded by the federal government: “A project shall not collect or maintain criminal intelligence information about the political, religious or social views, associations, or activities of any individual or any group . . . unless [i] such information directly relates to criminal conduct or activity and [ii] there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity.” *See* 28 C.F.R. § 23.20(b).

In sum, the ACLU proposes that the CPD adopt a rule providing that CPIC staff cannot use race, religion, ideology, and the like, in whole or in part, as a factor giving rise to suspicion – unless such information directly relates to criminal conduct or activity and there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity. This reform might be accomplished by substituting the phrase “in whole or in part” for the word “solely” in the aforementioned CPD/CPIC ISE-SAR Privacy Policy at Part E(2). *See* Exh. 1.

\* \* \*

Thank you for your attention to this matter. By January 16, 2012, please advise me of your position regarding the ACLU’s two proposals.

Sincerely,

  
Harvey Grossman  
Legal Director  
ACLU of Illinois

# **EXHIBIT 1**

# **Chicago Police Department's Crime Prevention Information Center**

## **ISE-SAR Evaluation Environment Initiative Privacy, Civil Rights, and Civil Liberties Protection Policy**

### **A. Purpose Statement**

1. The purpose of the Information Sharing Environment-Suspicious Activity Reporting (ISE-SAR) Evaluation Environment Initiative (hereafter "EE Initiative") Privacy, Civil Rights, and Civil Liberties Protection Policy (hereafter "Privacy and CR/CL Policy") is to promote the **Chicago Police Department's Crime Prevention Information Center** (hereafter "C.P.I.C."), source agency, and user agency (hereafter collectively referred to as "participating agencies" or "participants") conduct under the EE Initiative that complies with applicable federal, state, local, and tribal laws, regulations, and policies and assists participants in:
  - Ensuring individual privacy, civil rights, civil liberties, and other protected interests.
  - Increasing public safety and improving national security.
  - Protecting the integrity of systems for the observation and reporting of terrorism-related criminal activity and information.
  - Encouraging individuals or community groups to trust and cooperate with the justice system.
  - Promoting governmental legitimacy and accountability.
  - Making the most effective use of public resources allocated to public safety agencies.

### **B. Policy Applicability and Legal Compliance**

1. All participating CPIC personnel (including personnel providing information technology services to the CPIC), private contractors, and other authorized participants will comply with applicable provisions of the CPIC's Privacy and CR/CL Policy concerning personal information, including:
  - SAR information the source agency collects and the CPIC receives.
  - The ISE-SAR information identified, submitted to the shared space, and accessed by or disclosed to CPIC personnel.
2. The CPIC will provide a printed copy of its Privacy and CR/CL Policy to all CPIC personnel, non-agency personnel who provide services to the CPIC, and to each source agency and CPIC authorized user and will require both a written acknowledgement of receipt of this policy and a written agreement to comply with applicable provisions of this policy.
3. All CPIC personnel, participating agency personnel, personnel providing information technology services to the agency, private contractors, and other authorized users shall comply with applicable laws protecting privacy, civil rights, and civil liberties, including, but not limited to, the U.S. Constitution and state, local, and federal privacy,



civil rights, civil liberties, and legal requirements applicable to the CPIC and/or other participating agencies.

**C. Governance and Oversight**

1. The **Commander** of the CPIC will have primary responsibility for operating the CPIC, ISE-SAR information system operations, and coordinating personnel involved in the EE Initiative; the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing or disclosure of SAR and ISE-SAR information; and enforcing the provisions of this policy.
2. The CPIC's participation in the EE Initiative will be guided by a trained Privacy Officer who is appointed by the CPIC Director to assist in enforcing the provisions of this policy and who, in addition to other responsibilities, will receive reports regarding alleged errors and violations of the provisions of this policy.

**D. Terms and Definitions**

1. The primary terms and definitions used in this privacy policy are set forth in Appendix A, Terms and Definitions.

**E. Information**

1. The CPIC will seek or retain information which a source agency (the CPIC or other agency) has determined constitutes "suspicious activity" and which:
  - Is based on (a) a criminal predicate or (b) a possible threat to public safety, including potential terrorism-related conduct.
  - Is relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents, the resulting justice system response, or the prevention of crime.
  - The source agency assures was acquired in accordance with agency policy and in a lawful manner.
2. Source agencies will agree not to collect and submit SAR information, and the CPIC will not retain SAR or ISE-SAR information about any individual that was gathered solely on the basis of that individual's religious, political, or social views or activities; participation in a particular noncriminal organization or lawful event; or race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation.
3. Upon receipt of SAR information from a source agency that has processed the information in accordance with CPIC criteria (business processes), designated CPIC personnel will:

**Chicago Police Department's CPIC ISE-SAR Evaluation Environment Initiative Privacy, Civil Rights, and Civil Liberties Protection Policy**

---

- Personally review and vet the SAR information and provide the two-step assessment set forth in the ISE-SAR Functional Standard to determine whether the information qualifies as an ISE-SAR (alternatively, CPIC personnel will confirm that such an assessment has been conducted by an authorized source agency).
  - Enter the information following Information Exchange Package Documentation (IEPD) standards and code conventions to the extent feasible.
  - Provide appropriate labels as required under E.5 and E.6 below.
  - Submit (post) the ISE-SAR to the CPIC's shared space.
  - Notify the source agency that the SAR has been identified as an ISE SAR and submitted to the shared space.
4. The CPIC will ensure that certain basic and special descriptive information is entered and electronically associated with ISE-SAR information, including:
- The name of the source agency.
  - The date the information was submitted.
  - The point-of-contact information for SAR-related data.
  - Information that reflects any special laws, rules, or policies regarding access, use, and disclosure.
5. Information provided in the ISE-SAR shall indicate, to the maximum extent feasible and consistent with the Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) Version 1.0 (ISE-FS-200):
- The nature of the source: anonymous tip, confidential source, trained interviewer or investigator, written statement (victim, witness, other), private sector, or other source.
  - Confidence, including:
    - The reliability of the source:
      - Reliable—the source has been determined to be reliable.
      - Unreliable—the reliability of the source is doubtful or has been determined to be unreliable.
      - Unknown—the reliability of the source cannot be judged or has not as yet been assessed.
    - The validity of the content:
      - Confirmed—information has been corroborated by an investigator or other reliable source.
      - Doubtful—the information is of questionable credibility but cannot be discounted.
      - Cannot be judged—the information cannot be confirmed.
  - Due diligence will be exercised in determining source reliability and content validity. Information determined to be unfounded will be purged from the shared space.
  - Unless otherwise indicated by the source or submitting agency, source reliability is deemed to be “unknown” and content validity “cannot be judged.” In such case,

**Chicago Police Department's CPIC ISE-SAR Evaluation Environment Initiative Privacy, Civil Rights, and Civil Liberties Protection Policy**

---

users must independently confirm source reliability and content validity with the source or submitting agency or validate it through their own investigation.

6. At the time a decision is made to post ISE-SAR information to the shared space, CPIC personnel will ensure that the ISE-SAR information is labeled, to the maximum extent feasible and consistent with the ISE-SAR FS, to reflect any limitations on disclosure based on sensitivity of disclosure (dissemination description code), in order to:
  - Protect an individual's right to privacy, civil rights, and civil liberties.
  - Protect confidential sources and police undercover techniques and methods.
  - Not interfere with or compromise pending criminal investigations.
  - Provide any legally required protection based on an individual's status as a child, sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, or resident of a domestic abuse shelter.
7. The CPIC will share ISE-SAR information with authorized law enforcement agencies and individuals only in accordance with established CPIC policy and procedure.
8. The CPIC will ensure that ISE-SAR information in the shared space that is not verified (confirmed) will be subject to continuing assessment for confidence by subjecting it to an evaluation or screening process to confirm its credibility and value or categorize the information as unfounded or uncorroborated. If subsequent attempts to validate the information confirm its validity or are unsuccessful, the information in the shared space will be updated (replaced) to so indicate. Information determined to be unfounded will be purged from the shared space.
9. The CPIC will incorporate the gathering, processing, reporting, analyzing, and sharing of SAR and ISE-SAR information (SAR process) into existing processes and systems used to manage other crime-related information and criminal intelligence, thus leveraging existing policies and protocols utilized to protect the information, as well as the privacy, civil rights, and civil liberties of individuals.
10. Notice will be provided through data field labels or narrative information to enable authorized users to determine the nature of the protected information in the shared space and how to handle the information in accordance with applicable legal requirements, including any restrictions based on information security or classification.

**F. Acquiring and Receiving Information**

1. Information acquisition and investigative techniques used by source agencies must comply with and adhere to applicable law, regulations and guidelines, including, where applicable, U.S. and state constitutional provisions, applicable federal and state law provisions, and local ordinances and regulations.

2. Law enforcement officers and other personnel at source agencies who acquire SAR information that may be shared with the CPIC will be trained to recognize behavior that is indicative of criminal activity related to terrorism.
3. When a choice of investigative techniques is available, information documented as a SAR or ISE-SAR should be acquired or investigated using the least intrusive feasible means, taking into account such factors as the effect on individuals' privacy and potential damage to reputation.
4. Access to and use of ISE-SAR information is governed by the U.S. Constitution, the Illinois state constitution, applicable federal and state laws and local ordinances, and Office of the Program Manager for the Information Sharing Environment (PM-ISE) policy guidance applicable to the ISE-SAR EE initiative.

#### **G. Information Quality Assurance**

1. The CPIC will ensure that source agencies assume primary responsibility for the quality and accuracy of the SAR data collected by the CPIC. The CPIC will advise the appropriate contact person in the source agency in writing (this would include electronic notification) if SAR information received from the source agency is alleged, suspected, or found to be erroneous or deficient.
2. The CPIC will make every reasonable effort to ensure that SAR information collected and ISE-SAR information retained and posted to the shared space is derived from dependable and trustworthy source agencies and is as accurate, current, and complete as possible.
3. At the time of posting to the shared space, ISE-SAR information will be labeled according to the level of confidence in the information (source reliability and content validity) to the maximum extent feasible.
4. The labeling of ISE-SAR information will be periodically evaluated and updated in the shared space when new information is acquired that has an impact on confidence in the information.
5. Alleged errors or deficiencies (misleading, obsolete, or otherwise unreliable) in ISE-SAR information will be investigated in a timely manner and any needed corrections to or deletions made to such information in the shared space.
6. ISE-SAR information will be removed from the shared space if it is determined the source agency did not have authority to acquire the original SAR information, used prohibited means to acquire it, or did not have authority to provide it to the CPIC or if the information is subject to an expungement order in a state or federal court that is enforceable under state law or policy.

7. The CPIC will provide written notice (this would include electronic notification) to the source agency that provided the SAR and to any user agency that has accessed the ISE-SAR information posted to the shared space when ISE-SAR information posted to the shared space by the CPIC is corrected or removed from the shared space by the CPIC because it is erroneous or deficient such that the rights of an individual may be affected.

#### **H. Analysis**

1. ISE-SAR information posted by the CPIC to the shared space or accessed from the shared spaces under the EE Initiative will be analyzed for intelligence purposes only by qualified CPIC personnel who have successfully completed a background check and any applicable security clearance and have been selected, approved, and trained accordingly (including training on the implementation of this policy). These personnel shall share ISE-SAR information only through authorized analytical products.
2. ISE-SAR information is analyzed according to priorities and needs, including analysis, to:
  - Further terrorism prevention, investigation, force deployment, or prosecution objectives and priorities established by the CPIC.
  - Provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in or engaging in terrorism-related activities.

#### **I. Sharing and Disclosure**

1. Credentialed, role-based access criteria will be used, as appropriate, to determine which system users will be authorized to view privacy fields in ISE-SAR information in response to queries made through a federated ISE-SAR search.
2. Unless an exception is expressly approved by the PM-ISE, the CPIC will adhere to the Functional Standard for the ISE-SAR process, including the use of the ISE-SAR IEPD reporting format, EE Initiative-approved data collection codes, and ISE-SAR information sharing and disclosure business rules.
3. ISE-SAR information retained by the CPIC and entered into the CPIC's shared space will be accessed by or disseminated only to persons within the CPIC or, as expressly approved by the PM-ISE, users who are authorized to have access and need the information for specific purposes authorized by law. Access and disclosure of personal information will be allowed to agencies and individual users only for legitimate law enforcement and public protection purposes and for the performance of official duties in accordance with law.

**Chicago Police Department's CPIC ISE-SAR Evaluation Environment Initiative Privacy,  
Civil Rights, and Civil Liberties Protection Policy**

---

4. ISE-SAR information will not be provided to the public if, pursuant to applicable law, it is:
  - Required to be kept confidential or exempt from disclosure under 5 ILCS 140.
  - Classified as investigatory records and exempt from disclosure under 5 ILCS 140.
  - Controlled by another agency that are not the records of the Chicago Police Department and exempt from disclosure under 5 ILCS 140.
5. The CPIC will not confirm the existence or nonexistence of ISE-SAR information to any person, organization, or other entity not otherwise entitled to receive the information under 5 ILCS 140

**J. Disclosure and Correction/Redress**

**J.1. Mandatory Disclosure and Correction:**

1. Upon satisfactory verification (fingerprints, driver's license, or other specified identifying documentation) of his or her identity and subject to the conditions specified in item 2, below, an individual who is entitled to know the existence of and to review the information about him or her that has been gathered and retained by the CPIC or a source agency participating in the EE Initiative may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information. The CPIC's response to the request for information will be made within a reasonable time and in a form that is readily intelligible to the individual. A record will be kept of all requests and of what information is disclosed to an individual.
2. The existence, content, and source of the information will not be made available to an individual when exempt from disclosure under 5 ILCS 140:
  - Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution.
  - Disclosure would endanger the health or safety of an individual, organization, or community.
  - The CPIC or user agency did not originate or does not otherwise have a right to disclose the information.
3. The individual to whom information has been disclosed will be given reasons if requests for correction(s) are denied by the CPIC or the source agency. The individual will also be informed of the procedure for appeal when the CPIC or source agency has declined to correct challenged information to the satisfaction of the individual to whom the information relates.

**J.2. Redress (complaint and correction when no right to disclosure)**

1. If an individual has complaints or objections to the accuracy or completeness of ISE-SAR information about him or her that is alleged to be held by the CPIC, the CPIC, as

appropriate, will inform the individual of the procedure for submitting complaints or requesting corrections. A record will be kept of all complaints and requests for corrections and the resulting action, if any.

2. The CPIC will acknowledge the complaint and state that it will be reviewed but will not confirm the existence of any ISE-SAR that contains information in privacy fields that identifies the individual. However, any personal information will be reviewed and corrected in or deleted from the ISE-SAR shared space if the information is determined to be erroneous, includes incorrectly merged information, or is out of date.

#### **K. Security Safeguards**

1. The CPIC's **Senior Watch Officer (SWO)** is designated and trained to serve as the CPIC's security officer for the EE Initiative.
2. The CPIC will operate in a secure facility that is protected from external intrusion. The CPIC will utilize secure internal and external safeguards against network intrusions of ISE-SAR information. Access to the CPIC's ISE-SAR shared space from outside the facility will be allowed only over secure networks.
3. The CPIC will secure ISE-SAR information in the CPIC's shared space in such a manner that it cannot be added to, modified, accessed, destroyed, or purged except by CPIC personnel authorized to take such actions.
4. Access to ISE-SAR information will be granted only to CPIC personnel whose positions and job duties require such access; who have successfully completed a background check and any applicable security clearance; and who have been selected, approved, and trained accordingly.
5. The CPIC will, in the event of a data security breach, implement a breach notification policy within 120 days as set forth in Office of Management and Budget (OMB) Memorandum M-07-16 (May 2007).

#### **L. Information Retention and Destruction**

1. The CPIC will ensure that all ISE-SAR information is entered into on a Department Information Report and reviewed for record retention (validation or purge) in accordance with the Department's Form Retention Schedule for Information Reports .
2. The CPIC will retain ISE-SAR information in the shared space for 6 months to permit the information to be validated or refuted, its credibility and value to be reassessed, and a "disposition" label (for example, undetermined or unresolved, cleared or unfounded, or under active investigation) assigned so that a subsequent authorized user knows the status and purpose for the retention and will retain the information based on any retention period associated with the disposition label.

3. When ISE-SAR information has no further value or meets the CPIC's criteria for purge according to CPIC policy, all information will be purged from the shared space.
4. The CPIC will complete a Department To-From Subject report through the Chain of Command and a Record Destruction Report as notification of appropriate parties before information is purged.

## **M. Transparency, Accountability, and Enforcement**

### **M.1. Information System Transparency**

1. The CPIC will be open with the public in regard to SAR collection and ISE-SAR information policies and practices. The CPIC will make the CPIC's EE Initiative Privacy Policy available upon request.
2. The CPIC's Privacy Officer will be responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections relating to ISE-SAR information.

### **M.2. Accountability**

1. The audit log of queries for ISE-SAR information will identify the user initiating the query.
2. The CPIC will have access to an audit trail of inquiries to and information disseminated from the shared spaces.
3. The CPIC will adopt and follow procedures and practices to evaluate the compliance of its authorized users with ISE-SAR information policy and applicable law. This will include periodic and random audits of logged access to the shared spaces in accordance with EE Initiative policy. Record of the audits will be maintained by the Bureau of Professional Standards of the Chicago Police Department.
4. CPIC personnel and source agencies shall report violations or suspected violations of the CPIC's ISE-SAR EE Initiative Privacy Policy to the CPIC's Privacy Officer.
5. The CPIC will conduct periodic audit and inspection of the information contained in its ISE-SAR shared space. The audit will be conducted by CPIC staff or an independent auditor, as provided by EE Initiative policy. This audit will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the ISE-SAR information maintained by the CPIC in the shared space and any related documentation.
6. The CPIC's appointed and trained Privacy Officer or other expert individual or group designated by the CPIC will periodically review the CPIC's EE Initiative Privacy



**Chicago Police Department's CPIC ISE-SAR Evaluation Environment Initiative Privacy, Civil Rights, and Civil Liberties Protection Policy**

---

Policy, and the CPIC will make appropriate changes in response to changes in applicable law.

**M.3. Enforcement**

1. The CPIC reserves the right to restrict the qualifications and number of user agencies and authorized user agency personnel that it certifies for access to ISE-SAR information and to suspend or withhold service to any of its user agencies or authorized user agency personnel violating this privacy policy. The CPIC further reserves the right to deny access or participation in the EE Initiative to its participating agencies (source or user) that fail to comply with the applicable restrictions and limitations of the CPIC's privacy policy.

**N. Training**

1. The following individuals will participate in training programs regarding implementation of and adherence to this privacy, civil rights, and civil liberties policy:
  - All assigned personnel of the CPIC.
  - Personnel providing information technology services to the CPIC.
  - Staff in other public agencies or private contractors, as appropriate, providing SAR and ISE-SAR information technology or related services to the CPIC.
  - Source agency personnel providing organizational processing services for SAR information submitted to the CPIC.
  - User agency personnel and individuals authorized to access ISE-SAR information who are not employed by the CPIC or a contractor.
2. The CPIC's privacy policy training program will cover:
  - Purposes of the EE Initiative Privacy Policy.
  - Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of SAR and ISE-SAR information maintained or submitted by the CPIC to the shared space.
  - How to implement the policy in the day-to-day work of a participating agency.
  - The impact of improper activities associated with violations of the policy.
  - Mechanisms for reporting violations of the policy.
  - The possible penalties for policy violations, including transfer, dismissal, and criminal liability, if any.

## **Appendix A—Terms and Definitions**

The following is a list of primary terms and definitions used throughout this template. These terms may also be useful in drafting the definitions section of the agency's/center's privacy policy.

**Access**—Data access is being able to get to (usually having permission to use) particular data on a computer. Web access means having a connection to the World Wide Web through an access provider or an online service provider. Data access is usually specified as read-only and read/write access.

With regard to the ISE, access refers to the business rules, means, and processes by and through which ISE participants obtain terrorism-related information, to include homeland security information, terrorism information, and law enforcement information acquired in the first instance by another ISE participant.

**Acquisition**—The means by which an ISE participant obtains information through the exercise of its authorities, for example, through human intelligence collection or from a foreign partner. For the purposes of this definition, acquisition does not refer either to the obtaining of information widely available to other ISE participants through, for example, news reports or to the obtaining of information shared with them by another ISE participant who originally acquired the information.

**Agency**—The [name of agency] and all agencies that access, contribute, and share information in the [name of agency]'s justice information system.

**Audit Trail**—A generic term for recording (logging) a sequence of activities. In computer and network contexts, an audit trail tracks the sequence of activities on a system, such as user log-ins and log-outs. More expansive audit trail mechanisms would record each user's activity in detail—what commands were issued to the system, what records and files were accessed or modified, etc.

Audit trails are a fundamental part of computer security, used to trace (usually retrospectively) unauthorized users and uses. They can also be used to assist with information recovery in the event of a system failure.

**Center**—Center refers to the [name of fusion center].

**Civil Liberties**—Fundamental individual rights, such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. They are the freedoms that are guaranteed by the Bill of Rights, the first ten Amendments to the Constitution of the United States. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference. Generally, the term "civil rights" involves positive (or affirmative) government action, while the term "civil liberties" involves restrictions on government.

**Chicago Police Department's CPIC ISE-SAR Evaluation Environment Initiative Privacy, Civil Rights, and Civil Liberties Protection Policy**

---

**Civil Rights**—The term “civil rights” refers to governments’ role in ensuring that all citizens have equal protection under the law and equal opportunity to exercise the privileges of citizenship regardless of race, religion, gender, or other characteristics unrelated to the worth of the individual. Civil rights are, therefore, obligations imposed on government to promote equality. More specifically, they are the rights to personal liberty guaranteed to all United States citizens by the Thirteenth and Fourteenth Amendments and by acts of Congress.

**Confidentiality**—Confidentiality is closely related to privacy but is not identical. It refers to the obligations of individuals and institutions to use information under their control appropriately once it has been disclosed to them. One observes rules of confidentiality out of respect for and to protect and preserve the privacy of others. See Privacy.

**Data**—Elements of information.

**Disclosure**—The release, transfer, provision of access to, sharing, publication, or divulging of personal information in any manner—electronic, verbal, or in writing—to an individual, agency, or organization outside the agency that collected it. Disclosure is an aspect of privacy, focusing on information which may be available only to certain people for certain purposes but which is not available to everyone.

**Fusion Center**—A collaborative effort of two or more agencies that provide resources, expertise, and information to a designated government agency or agency component with the goal of maximizing its ability to detect, prevent, investigate, and respond to criminal and terrorist activity.

**Homeland Security Information**—As defined in Section 892(f)(1) of the Homeland Security Act of 2002 and codified at 6 U.S.C. § 482(f)(1), homeland security information means any information possessed by a federal, state, or local agency that (a) relates to a threat of terrorist activity; (b) relates to the ability to prevent, interdict, or disrupt terrorist activity; (c) would improve the identification or investigation of a suspected terrorist or terrorist organization; or (d) would improve the response to a terrorist act.

**Information**—Information includes any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists. Information received by law enforcement agencies can be categorized into four general areas: general data, tips and leads data, suspicious activity reports, and criminal intelligence information.

**Information Quality**—Information quality refers to various aspects of the information; the accuracy and validity of the actual values of the data, data structure, and database/data repository design. Traditionally, the basic elements of information quality have been identified as accuracy, completeness, currency, reliability, and context/meaning. Today, information quality is being more fully described in multidimensional models, expanding conventional views of the topic to include considerations of accessibility, security, and privacy.

**Chicago Police Department's CPIC ISE-SAR Evaluation Environment Initiative Privacy, Civil Rights, and Civil Liberties Protection Policy**

---

**ISE-SAR**—A suspicious activity report that has been determined, pursuant to a two-part process, to have a potential terrorism nexus. ISE-SAR business rules will serve as a unifying process to support the reporting, tracking, processing, storage, and retrieval of terrorism-related suspicious activity reports across the ISE.

**ISE-SAR Information Exchange Package Documentation (IEPD)**—A schema that facilitates the posting and sharing of ISE-SAR information. The ISE-SAR IEPD is used to represent ISE information in two different data formats:

- (1) The **Detailed format** includes information contained in all data elements set forth in Section IV of the ISE-SAR FS (“ISE-SAR Exchange Data Model”), including fields denoted as privacy fields.
- (2) The **Summary format** excludes certain privacy fields as identified in the ISE-SAR FS. The ISE-SAR FS identifies the minimum privacy fields that must be excluded. Each ISE participant may exclude additional privacy fields from its Summary ISE-SARs, in accordance with applicable legal requirements.

**Law**—As used by this policy, law includes any local, state, or federal statute, ordinance, regulation, executive order, policy, or court rule, decision, or order as construed by appropriate local, state, or federal officials or agencies.

**Law Enforcement Information**—For purposes of the ISE, law enforcement information means any information obtained by or of interest to a law enforcement agency or official that is both (a) related to terrorism or the security of our homeland and (b) relevant to a law enforcement mission, including but not limited to information pertaining to an actual or potential criminal, civil, or administrative investigation or a foreign intelligence, counterintelligence, or counterterrorism investigation; assessment of or response to criminal threats and vulnerabilities; the existence, organization, capabilities, plans, intentions, vulnerabilities, means, methods, or activities of individuals or groups involved or suspected of involvement in criminal or unlawful conduct or assisting or associated with criminal or unlawful conduct; the existence, identification, detection, prevention, interdiction, or disruption of or response to criminal acts and violations of the law; identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and victim/witness assistance.

**Logs**—See Audit Trail. Logs are a necessary part of an adequate security system because they are needed to ensure that data is properly tracked and that only authorized individuals can access the system and the data.

**Participating Agencies**—Participating agencies, for purposes of the EE Initiative, include source [the agency or entity that originates SAR (and, when authorized, ISE-SAR) information], submitting (the agency or entity posting ISE-SAR information to the shared space), and user (an agency or entity authorized by the submitting agency or other authorized agency or entity to access ISE-SAR information, including information in the shared space(s),

## **Chicago Police Department's CPIC ISE-SAR Evaluation Environment Initiative Privacy, Civil Rights, and Civil Liberties Protection Policy**

---

and which may include analytical or operational component(s) of the submitting or authorizing agency or entity) agencies, in support of their responsibility to collect, document, process, access, or use SAR and ISE-SAR information.

**Personal Information**—Information that can be used, either alone or in combination with other information, to identify individual subjects suspected of engaging in an activity or incident potentially related to terrorism.

**Privacy**—Individuals' interests in preventing the inappropriate collection, use, and release of personal information. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data. Other definitions of privacy include the right to be physically left alone (solitude); to be free from physical interference, threat, or unwanted touching (assault, battery); or to avoid being seen or overheard in particular contexts.

**Privacy Fields**—Data fields in ISE-SAR IEPDs that contain personal information.

**Privacy Policy**—A written, published statement that articulates the policy position of an organization on how it handles the personal information that it gathers and uses in the normal course of business. The policy should include information relating to the processes of information collection, analysis, maintenance, disclosure, and access. The purpose of the privacy policy is to articulate that the agency/center will adhere to those legal requirements and agency/center policy determinations that enable gathering and sharing of information to occur in a manner that protects personal privacy interests. A well-developed and -implemented privacy policy uses justice entity resources wisely and effectively; protects the agency, the individual, and the public; and promotes public trust.

**Privacy Protection**—A process of maximizing the protection of privacy, civil rights, and civil liberties when collecting and sharing information in the process of protecting public safety and public health.

**Protected Information**—For the nonintelligence community, protected information is information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and laws of the United States. For state, local, and tribal governments, these protections are derived from applicable state and tribal constitutions and state, local, and tribal laws, ordinances, and codes. For the (federal) intelligence community, protected information includes information about "United States persons" as defined in Executive Order 12333. Protected information may also include other information that the U.S. government expressly determines by Executive Order, international agreement, or other similar instrument should be covered.

**Public**—Public includes:

- Any person and any for-profit or nonprofit entity, organization, or association.
- Any governmental entity for which there is no existing specific law authorizing access to the agency's/center's information.
- Media organizations.

**Chicago Police Department's CPIC ISE-SAR Evaluation Environment Initiative Privacy, Civil Rights, and Civil Liberties Protection Policy**

---

- Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit, and without distinction as to the nature or intent of those requesting information from the agency.

Public does not include:

- Employees of the agency.
- People or entities—private or governmental—who assist the agency/center in the operation of the justice information system.
- Public agencies whose authority to access information gathered and retained by the agency/center is specified in law.

**Record**—Any item, collection, or grouping of information that includes personally identifiable information and is maintained, collected, used, or disseminated by or for the collecting agency or organization.

**Retention**—Refer to Storage.

**Role-Based Access**—A type of access that uses roles to determine rights and privileges. A role is a symbolic category of users that share the same security privilege.

**Security**—The range of administrative, technical, and physical business practices and mechanisms that aim to preserve privacy and confidentiality by restricting information access to authorized users for authorized purposes. Computer and communications security efforts also have the goal of ensuring the accuracy and timely availability of data for the legitimate user set, as well as promoting failure resistance in the electronic systems overall.

**Shared Space**—A networked data and information repository which is under the control of submitting agencies and which provides terrorism-related information, applications, and services to other ISE participants.

**Sharing**—The act of one ISE participant disseminating or giving homeland security information, terrorism information, or law enforcement information to another ISE participant.

**Source Agency**—The agency or entity that originates SAR (and, when authorized, ISE-SAR) information.

**Storage**—In a computer, storage is the place where data is held in an electromagnetic or optical form for access by a computer processor. There are two general usages:

1. Storage is frequently used to mean the devices and data connected to the computer through input/output operations—that is, hard disk and tape systems and other forms of storage that do not include computer memory and other in-computer storage. This meaning is probably more common in the Information Technology industry than the second meaning.

2. In a more formal usage, storage has been divided into (1) primary storage, which holds data in memory (sometimes called random access memory or RAM) and other "built-in" devices such as the processor's L1 cache, and (2) secondary storage, which holds data on hard disks, tapes, and other devices requiring input/output operations.

Primary storage is much faster to access than secondary storage because of the proximity of the storage to the processor or because of the nature of the storage devices. On the other hand, secondary storage can hold much more data than primary storage.

With regard to the ISE, storage (or retention) refers to the storage and safeguarding of terrorism-related information, to include homeland security information, terrorism information, and law enforcement information relating to terrorism or the security of our homeland by both the originator of the information and any recipient of the information.

**Submitting Agency**—The agency or entity providing ISE-SAR information to the shared space.

**Suspicious Activity**—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 (illegal) intention. Examples of suspicious activity include surveillance, photography of facilities, site breach or physical intrusion, cyber attacks, testing of security, etc.

**Suspicious Activity Reports (SARs)**—Reports that record the observation and documentation of a suspicious activity. SARs are meant to offer a standardized means for feeding information repositories. Any patterns identified during SAR review and analysis may be investigated in coordination with the reporting agency and, if applicable, the state-designated fusion center. SARs are not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor are they designed to support interagency calls for service.

**Terrorism Information**—Consistent with Section 1016(a)(4) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), all information relating to (a) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or materials support, or activities of foreign or international terrorist groups or individuals or of domestic groups or individuals involved in transnational terrorism; (b) threats posed by such groups or individuals to the United States, United States persons, or United States interests or to those interests of other nations; (c) communications of or by such groups or individuals; or (d) other groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

**Terrorism-Related Information**—In accordance with the IRTPA, as recently amended by the 9/11 Commission Act enacted on August 3, 2007 (P.L. 110-53), the ISE facilitates the sharing of terrorism and homeland security information, as defined in the IRTPA Section 1016(a)(5) and the Homeland Security Act 892(f)(1) (6 U.S.C. § 482(f)(1)). See also *Information Sharing Environment Implementation Plan* (November 2006) and Presidential Guidelines 2 and 3 (the ISE will facilitate the sharing of "terrorism information," as defined in IRTPA, as well as the

following categories of information to the extent that they do not otherwise constitute "terrorism information": (1) homeland security information as defined in Section 892(f)(1) of the Homeland Security Act of 2002 (6 U.S.C. § 482(f)(1)) and (2) law enforcement information relating to terrorism or the security of our homeland). Such additional information includes intelligence information.

Weapons of Mass Destruction (WMD) information as a fourth (third statutory) category of ISE information is not called for in P.L. 110-53. Rather, it amends the definition of terrorism information to include WMD information and then defines that term. WMD information probably should not technically be cited or referenced as a fourth category of information in the ISE.

**Tips and Leads Information or Data**— Uncorroborated report or information generated from inside or outside the agency that alleges or indicates some form of possible criminal activity. Tips and leads can also be referred to as suspicious incident reports (SIRs), suspicious activity reports (SARs), and/or field interview reports (FIRs). Tips and leads information does not include incidents that do not have an offense attached, criminal history records, or Computer Aided Dispatch (CAD) data.

A tip or lead can come from a variety of sources, including, but not limited to, the public, field interview reports, and anonymous or confidential sources. This information has some suspicion or mere suspicion attached to it, but without further inquiry or analysis, it is unknown whether the information is accurate or useful. Tips and leads information falls between being of no use to law enforcement and being extremely valuable depending on whether time and resources are available to determine its meaning.

Tips and leads information is maintained in a secure system, similar to data that rises to the level of reasonable suspicion.

**User Agency**—The agency or entity authorized by the submitting agency or other authorized agency or entity to access ISE-SAR information in the shared space(s), which may include analytical or operational component(s) of the submitting or authorizing agency or entity.



Appendix B – Illinois Freedom of Information Act

**Chicago Police Department's CPIC ISE-SAR Evaluation Environment Initiative Privacy,  
Civil Rights, and Civil Liberties Protection Policy**

---

**Appendix C – Chicago Police Department Forms Retention Schedule**

**Chicago Police Department's CPIC ISE-SAR Evaluation Environment Initiative Privacy,  
Civil Rights, and Civil Liberties Protection Policy**

---

Appendix D – Office of Management and Budget (OMB) Memorandum M-07-16 (May 2007)

# **EXHIBIT 2**

<b>DEPLOYMENT OPERATIONS CENTER Special Order</b>	Date of Issue <b>12 March 2009</b>	Effective Date <b>17 March 2009</b>	No. <b>09-10</b>
Subject eGUARDIAN PROTOCOL	Amends		
Related Directives	Rescinds		

This directive will set forth protocol for Deployment Operations Center (DOC) personnel when entering information into the eGUARDIAN system.

eGUARDIAN is an information sharing database under the auspices of the Federal Bureau of Investigation (FBI). A member must have an active account in the FBI's Law Enforcement Online (LEO) website in order to be able to access eGUARDIAN.

eGUARDIAN is a sensitive but unclassified system for official use only. The suspicious activities contained in eGUARDIAN may be raw and unvetted data. Suspicious activity is defined by the Program Manager of the Information Sharing Environment (PM/ISE) as observed behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal or illicit intention. Suspicious activities may include, but are not limited to, surveillance, cyber attacks, probing of security and photography of key infrastructures and facilities.

No entry into eGUARDIAN may be based solely on the ethnicity, race or religion of any individual or solely on the exercise of rights guaranteed by the First Amendment or the lawful exercise of any other rights secured by the Constitution or laws of the United States.

If a member determines that information they are in receipt of meets the criteria as set forth above and in accordance with the eGUARDIAN User Agreement, the information is to be entered into eGUARDIAN. Only information that has been obtained and documented on an official Chicago Police Department (CPD) form may be entered. If a member obtains information via verbal means and the provider will not be documenting the information on an official CPD form, that information is to be documented by the member on a CPD Information Report. The source of the information must be documented on the Information Report.

If a member determines that information they have previously submitted is erroneous, the member is responsible for updating or correcting the information in eGUARDIAN. If a member discovers information that has been contributed that they know is erroneous, you are to notify a supervisor so that the person who submitted the information can be informed and a correction can be made.

Upon accessing the eGUARDIAN system, the member will click on "Incidents" and then "Add Incident" in order to enter information into the system. Most of the entry fields are self explanatory but the following will set forth protocol for some of them. In the "agency report number/ID" box, the member will input the associated RD number. If there is no RD number, the member will enter the DOC's Counter Terrorism Section (CTS) Database Tracking number associated with the report. The name of the officer who originally provided the information will be inserted into the "Reporting Officer" box. The FBI Chicago Field Office will always be selected from the drop down box for the "Local Field Office" box.

**DEPLOYMENT OPERATIONS CENTER  
Special Order**

Date of Issue  
**12 March 2009**

Effective Date  
**17 March 2009**

No.  
**09-10**

Subject  
eGUARDIAN PROTOCOL – 2<sup>nd</sup> Page

Amends

Related Directives

Rescinds

In the "Subjects" box, the member will never answer if the subject is a U.S. person. If the field requires a response, the answer will always be unknown.

Upon entering information into the system and submitting it, the member will print out a copy of the submission in addition to the CPD report(s) documentation and give it to the CTS sergeant or in his/her absence, the CTS lieutenant. The supervisor will then view the submission for completeness, accuracy and accordance with the guidelines as set forth by the FBI and re-iterated in this directive. If satisfactory, the supervisor will then approve the submission. If the submission is rejected, the supervisor will inform the member of why the submission was not satisfactory and have the member re-do the submission if it will be entered.

The CPD report(s) documenting the information, with the eGUARDIAN tracking number noted, will then be given to the CTS member responsible for maintaining the CTS' Database Tracking system for entry and filing in accordance with the Department's retention schedule for the affected reports.

Authenticated:

SS

---

**DEPLOYMENT OPERATIONS CENTER  
Special Order**

Date of Issue  
**30 November 2009**

Effective Date  
**30 November 2009**

No.  
09-  
10A

Subject  
eGUARDIAN PROTOCOL – OUTSIDE AGENCY

Amends  
**09-10**

Related Directives

Rescinds

This directive will set forth protocol for Deployment Operations Center (DOC) personnel when approving information in the eGUARDIAN system that has been submitted by an outside agency.

eGUARDIAN is an information sharing database under the auspices of the Federal Bureau of Investigation (FBI). A member must have an active account in the FBI's Law Enforcement Online (LEO) website in order to be able to access eGUARDIAN.

Any member referring an entry in eGuardian that has been supplied from an outside agency will ensure that the following disclaimer is included in the notes section for the entry.

“This report is being submitted to your Field Office on behalf of the (insert name of outside agency) for your review and action as your Agency deems appropriate and that the Chicago Police Department has not reviewed, vetted, or investigated the entry in any manner.”

Authenticated:

SS

---

# **EXHIBIT 3**



# CHICAGO POLICE DEPARTMENT

*Crime Prevention and Information Center*



## CPIC PRIVACY POLICY



**Richard M. Daley**  
Mayor



**Jody P. Weis**  
Superintendent of Police

## **CRIME PREVENTION AND INFORMATION CENTER PRIVACY POLICY**

The **Crime Prevention and Information Center** is a Fusion Center (herein referenced to as "CPIC" as defined below:

The CPIC project was initiated in response to the increase need for timely information sharing and exchange of crime-related information among members of the law enforcement community. One component of CPIC focuses on the development and exchange of criminal intelligence. This component focuses on the intelligence process where information is collected, integrated, evaluated, analyzed and disseminated.

CPIC's intelligence products and services will be made available to law enforcement agencies and other criminal justice entities. All agencies participating in the CPIC will be subject to a Memorandum of Understanding and will be required to adhere to all CPIC's policies and security requirements. The purpose of this privacy policy is to ensure safeguards and sanctions are in place to protect personal information as information and intelligence are developed and exchanged.

### **GUIDING PRINCIPLES**

CPIC's Privacy Policy embraces the eight Privacy Design Principles which shall guide the policy and practices wherever applicable. The eight Privacy Design principles are:

1. **Purpose Specification** – Define the CPIC's purpose for information to help ensure the agency's use of information is appropriate.
2. **Collection Limitation** – Limit the collection of personal information to that required for the purposes intended.
3. **Data Quality** – Ensure data accuracy
4. **Use Limitation** – Ensure appropriate limits on Department use of personal information.
5. **Security safeguards** – Maintain effective security over personal information
6. **Openness** – Maintains a citizen access to information available through the Freedom of Information Act.
7. **Individual Participation** – Allow individual's reasonable access and opportunity to correct errors in their personal information held by the Agency.
8. **Accountability** – Identify, train and hold agency personnel accountable for adhering to agency information quality and privacy policies.

#### **I. Purpose Specification**

CPIC has developed databases by using existing data sources from federal, state and local law enforcement to integrate data with the goal of identifying, developing and analyzing intelligence related to violent crimes, terrorist activity

and other crimes for investigative leads. This capability will facilitate integration and exchange of information between participating law enforcement agencies.

## **II. Collection Limitation**

The CPIC is maintained for the purposes of developing information and intelligence by agencies who participate in the CPIC. The decision of an agency to participate in CPIC and about which databases to provide is voluntary. Information obtained and disseminated by a law enforcement agency outside of Chicago will be governed by the laws and rules governing the individual agencies respecting such data, as well as by applicable federal laws..

Because the laws, rules or policies governing information and intelligence that can be collected and released on private individuals will vary from agency to agency, limitations on the collection of data concerning individuals is the responsibility of the collector of the original source data. Therefore, each contributor of information is under different legal restraints and restrictions. Each agency has its own responsibility to abide by the collection limitations applicable to it by reasons of law. Information contributed to the center should be that which has been collected in conformance with those limitations.

## **III. Data Quality**

The agencies participating in the Crime Prevention and Information Center remain the owners of the data contributed and are, therefore, responsible for the quality and accuracy of the data accessed by the Center. Inaccurate personal information can have a damaging impact on the person concerned and on the integrity and functional value of the Center. In order to maintain the integrity of the center, any information obtained through the Center must be independently verified with the original source from which the data was extrapolated before any official action (e.g., warrant or arrest) is taken. User agencies and individual users are responsible for compliance with respect to use and further dissemination of such information and the purging and updating of the data.

## **III. Use Limitation**

Information obtained from or through the CPIC can only be used for lawful purposes. A lawful purpose means the request for data can be directly linked to a law enforcement agency's active criminal investigation or is a response to a confirmed lead that requires follow-up to prevent a criminal act.

The primary responsibility for the overall operation of the Crime Prevention and Information Center will be the Commander of the Deployment Operations Center of the Chicago Police Department. The Commander will enforce the Privacy Policy of the CPIC and take the necessary measures to make certain that access to

the CPIC's information and resources is secure and will prevent any unauthorized access or use. The Chicago Police Department reserves the right to restrict the qualifications and number of personnel who will be accessing CPIC and to suspend or withhold service to any individual violating this Privacy Policy. The Department, or persons acting on behalf of the Department, further reserves the right to conduct inspections concerning the proper use and security of the information received from the center.

Security for information derived from CPIC will be provided in accordance with all applicable federal, state and local laws, the rules and regulations of the Chicago Police Department, and CPIC policies. Furthermore, all personnel who receive, handle, or have access to CPIC data and/or sensitive information will be trained as to those requirements. All personnel having access to the CPIC's data agree to abide the following rules:

1. CPIC's data will be used only to perform official law enforcement investigative-related duties in a manner authorized by the user's employer and CPIC.
2. Individual passwords will not be disclosed to any other person except as authorized by the Department.
3. Individual passwords will be changed if authorized personnel of the Department, the CPIC or any individual password holder suspects the password has been improperly disclosed or otherwise compromised.
4. Background checks will be completed on personnel who will have direct access to CPIC.
5. Use of CPIC's data in an unauthorized or illegal manner will subject the user to denial of further use of the CPIC; discipline by the user's employing agency, and /or criminal prosecution.

Each authorized user understands that access to the CPIC can be denied or rescinded for failure to comply with the application restrictions and use limitations.

V. **Security Safeguard**

Information obtained from or through the CPIC will not be used or publicly disclosed for purposes other than those specified in the Memorandum of Understanding that each participating agency must sign. Information cannot be (1) sold, published, exchanged, or disclosed for commercial purposes; (2) disclosed or published without prior approval of the contributing agency; or (3) disseminated to unauthorized persons.

Use of CPIC's data is limited to those individuals who have been selected, approved, and trained accordingly. Access to information contained within the CPIC will be granted only to law enforcement agency personnel who have been screened with a state and national fingerprint-based background check, as well as any additional background screening process using procedures and standards established by Chicago Police Department. Each individual user must complete and Individual User Agreement in conjunction with training.

The Crime Prevention and Information Center operates in a secure facility, protecting the CPIC from external intrusion. The CPIC will utilize secure internal and external safeguards against network intrusions. Access to CPIC databases from outside the facility will only be allowed over secure networks. The CPIC will store information in a manner that cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such action.

#### VI. Openness

It is the intent of the participating agencies to be open with the public concerning data collection practices when such openness will not jeopardize ongoing criminal investigative activities. Participating agencies will refer citizens to the original collector of the data as the appropriate entity to address any concern about data accuracy and quality, when this can be done without compromising an active inquiry or investigation.

CPIC is a collection of various databases, which allows the Department and participating agencies to share information and to accelerate the dissemination of information already collected. CPIC does not change or alter a citizen's rightful access to information accorded to them under state law. The CPIC will post the Privacy Policy on the premises of the CPIC and make it available to any interested party.

#### VII. Individual Participation

The data maintained by CPIC is provided, on a voluntary basis, by the participating agencies or is information obtained by other sources. Each individual user searching against the data as described herein will be required to acknowledge that he or she remains solely responsible for the interpretations, further dissemination, and use of any information that results from the search process and is responsible for ensuring that any information relied upon is accurate, current, valid and complete, especially before any official action is taken in full or partial reliance upon the information obtained.

Members of the public cannot access individually identifiable information, on themselves or others, from the CPIC's applications. Persons wishing to access data pertaining to themselves should communicate directly with the agency or entity that is the source of the data in question.

Participating agencies agree that they will refer requests related to privacy or sunshine laws back to the originator of the information.

### VIII. Accountability

When a query is made to any of the CPIC's data applications, the original request is automatically logged by the CPIC's **Event Manager Statistical Electronic Log** system which will identify the user initiating the query. When such information is disseminated outside the agency from which the original request is made, a second dissemination log must be maintained in order to correct possible erroneous information and for audit purposes, as required by applicable law. Secondary dissemination of information can only be to a law enforcement agency for law enforcement investigative purpose or other agencies as provided by law. The agency from which the information is requested will maintain a record (log) of any secondary dissemination of information. This record will reflect as a minimum:



1. Date of release
2. To whom the information relates
3. To whom the information was released (including address and telephone number)
4. All identification numbers or other indicator that clearly identifies the data released
5. The purpose for which the information was released

The Chicago Police Department will be responsible for conducting or coordinating audits and investigating misuse of CPIC's data or information. All violations and/or exceptions shall be reported to the *Chicago Police Department Deployment Operations Center*. Individual users of the CPIC's information remain responsible for their legal and appropriate use of the information contained therein. Failure to abide by the restrictions and use of limitations for the use of CPIC's data may result in the suspension or termination of use privileges, discipline sanctions imposed by the user's employing agency, or criminal prosecution. Each user and participating agency in the CPIC is required to abide by this *Privacy Policy* in the use of information obtained by and through the Chicago Police Department's CPIC.

# **EXHIBIT 4**

Suspicious Activity Reporting

**SAR Indicators**



---

---

---

---

---

---



---

---

Suspicious Activity Reporting

**International Terrorism Indicators**

Mr. Richard A. Marquise



---

---

---

---

---

---




---

---

Suspicious Activity Reporting

**International Terrorism Threat**

- State sponsors
- Nationalist/ethnic/separatist groups
- Leftist/social revolutionary groups
- Radical Palestinians
- Religious fundamentalist groups
- Homegrown using any of the above ideologies



---

---

---

---

---

---

---



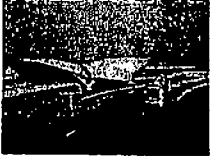
---



**Suspicious Activity Reporting**

**Recruiting**

- Building of operational teams and capabilities
  - Ressaam at mosques in Montreal
  - Abdullah Azzam in Brooklyn, 1989
  - Israel, Pakistan, India, Iraq and Afghanistan—money
  - Tabatabai murder in Bethesda in 1981
  - JFK plot in NY—tried to recruit FBI informant



---

---

---

---

---

---



---

---

**Suspicious Activity Reporting**

**Other**

- "Catch-all"
  - Criminal activity: Madrid, Abu Nidal cells in U.S., Operation Smokescreen, Canadian Hezbollah cells, and cigarette smuggling
- If it looks unusual to you—the expert—it probably is



---

---

---

---

---

---




---

---

**Suspicious Activity Reporting**

**Ahmed Ressaam— December 1999**

- Arrived in Canada in February 1994
- Arrested for theft (1995)
- CSIS monitoring telephones
- 1998—to Afghanistan
- February 1999—arrived at LAX
- Fall 1999—made bombs
- December 1999—arrested at Port Angeles, Washington



---

---

---

---

---



---

---

---

**Suspicious Activity Reporting**

**dmarquise@iir.com**  
**(703) 362-3135**



---

---

---

---

---

---

---

---

# **EXHIBIT 5**



United States  
Department of Justice

**FINAL REPORT:**  
**INFORMATION SHARING ENVIRONMENT**  
**(ISE)-SUSPICIOUS ACTIVITY REPORTING (SAR)**  
**EVALUATION**  
**ENVIRONMENT**

---

FINAL REPORT:  
INFORMATION SHARING ENVIRONMENT (ISE)-  
SUSPICIOUS ACTIVITY REPORTING (SAR)  
EVALUATION ENVIRONMENT

JANUARY 2010

---

This project was supported by Grant No. 2008-DD-BX-K480 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the SMART Office, and the Office for Victims of Crime. Points of view or opinions in this document are those of the author and do not represent the official position or policies of the United States Department of Justice.

## **CHICAGO, ILLINOIS, POLICE DEPARTMENT**

### **SAR PROCESS REPORT—POST-IMPLEMENTATION PHASE**

Following the conclusion of the Information Sharing Environment-Suspicious Activity Reporting Evaluation Environment (ISE-SAR EE), a discussion was held with the Chicago, Illinois, Police Department (CPD) to document the implementation efforts conducted during the ISE-SAR EE. The results of the discussion are detailed below.

#### **EXECUTIVE LEADERSHIP**

Prior to the ISE-SAR EE, CPD did not have a policy regarding the collection and analysis of suspicious activity information. The command staff in CPD's Deployment Operations Center had been briefed on the initiative and had attended conferences and training events in which the SAR process implementation was discussed. CPD command staff and senior management had shown their full support for this effort.

During the ISE-SAR EE, CPD command staff received the Major Cities Chiefs Association's Chief Executive Officer Briefing in May 2009, and 36 command staff personnel from approximately 31 law enforcement agencies participated. Currently, there is no separate policy for the collection and analysis of SAR information; however, there is a comprehensive policy on the handling of information reports. As the project matures, the chief of the Counterterrorism and Intelligence Division (CID) will be responsible for drafting a SAR policy. A commander from CID has been assigned to the SAR process development project; the primary responsibility of the commander is to implement a formal SAR process at CPD.

#### **SAR BUSINESS PROCESS**

Prior to the ISE-SAR EE, CPD utilized an "information report" to collect data regarding suspicious activity. CPD forwarded all of the information reports containing terrorism-related issues to CID. Based on its analysis and investigation, CID made a determination as to the disposition of these reports. The disposition included either referral for full investigation or referral to another agency for its review. A database was designated to document and track the reported terrorism-related suspicious activity information. CID is responsible for providing feedback to the officers who submit the suspicious activity.

Prior to the ISE-SAR EE, CPD had not adopted the behavior-specific codes listed in the ISE-SAR Functional Standard. All terrorism-related information reports were vetted within 24 hours and a report provided to the on-duty lieutenant in CID. After the lieutenant's review, relevant terrorism-related information reports were forwarded to the Illinois Statewide Terrorism and Intelligence Center, the U.S. Department of Homeland Security's (DHS) National Operations Center (NOC), and the Federal Bureau of Investigation's (FBI) Joint

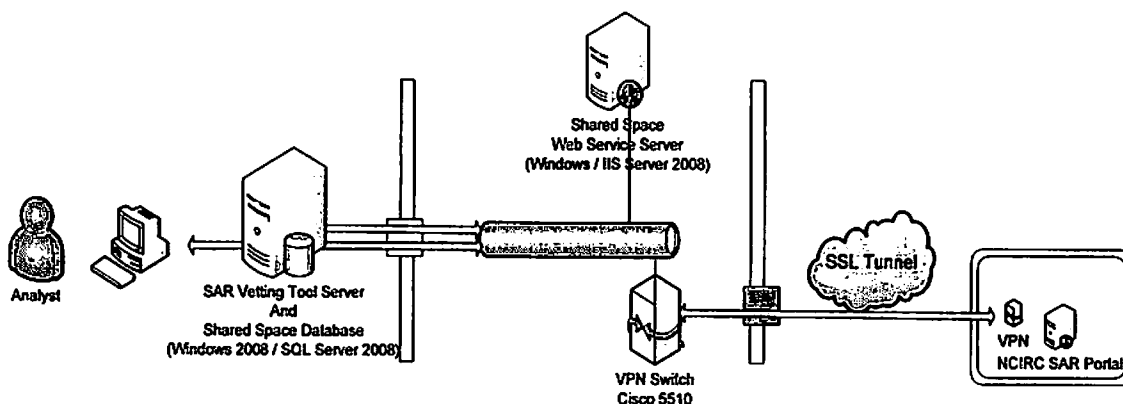
Terrorism Task Force (JTTF) for further vetting. Prior to the ISE-SAR EE, the department was using the eGuardian system to submit terrorism-related SARs to the JTTF.

During the ISE-SAR EE, CPD continued to use the same SAR mechanisms that were used prior to the ISE-SAR EE. However, CPD created a multilayer review process for reviewing and vetting SARs and moving them to the ISE-SAR Shared Spaces. The department requested use of the SAR Vetting Tool (SVT) to input its SAR data for ultimate migration to the ISE-SAR Shared Spaces. CID adopted the behavior-specific codes illustrated in the ISE-SAR Functional Standard and developed and implemented a privacy policy regarding the reporting of suspicious activity that meets the applicable requirements of the ISE Privacy Guidelines. In order to protect the information within the ISE-SAR Shared Spaces, it was determined that access to the ISE-SAR Shared Spaces would be limited to personnel within CID, and by policy, all queries on the information within the ISE-SAR Shared Spaces is for law enforcement purposes only and must have a criminal nexus. It was indicated that if SAR information is identified as having an error, CID will immediately contact the source agency and rectify the error.

### SAR TECHNICAL PROCESS

Prior to the ISE-SAR EE, the center of CPD's information technology infrastructure was the Citizen Law Enforcement Analysis and Reporting (CLEAR) system. Initially deployed in April 2000, the CLEAR system is the foundation for a growing set of integrated CLEAR applications used by CPD officers and civilians in and around the Chicago area. Handling thousands of queries daily, the CLEAR system supports all law enforcement and investigative functions within CPD.

During the ISE-SAR EE, CPD requested the use of the SVT to augment existing legacy system data and act as a bridge between the legacy system and the Shared Spaces database. The SVT application and database was installed on the ISE-SAR Shared Spaces Server as an economical approach to share hardware and MS-SQL resources. The common architecture is described below.



## **TRAINING**

Prior to the ISE-SAR EE, CPD had developed a five-day terrorism training program and was in the process of training all of its officers. CID continuously monitors all incoming terrorism-related information in order to identify new trends and emerging issues. The results of this analysis are provided to the training bureau.

During the ISE-SAR EE, CPD continued its efforts to train all officers in its five-day terrorism awareness program, and SAR-related training has been provided to all Terrorism Liaison Officers (TLOs) within the department. It was indicated that CID continually monitors all incoming SARs and evaluates those for new trends and emerging issues. The results of the analysis are provided to the Training Bureau. In addition, CPD participated in the Chief Executive Officer Briefing and the SAR analyst/investigator course. During the SAR analyst/investigator course in the Chicago area in March 2009, 21 personnel were trained from three law enforcement agencies. CID plans to utilize the line officer training once it is made available nationwide.

## **INSTITUTIONALIZATION OF THE SAR PROCESS**

Prior to and during the ISE-SAR EE and continued throughout the ISE-SAR EE, CPD maintained a robust TLO program within the department. Officers are selected from 25 districts, one per watch, and include approximately 80 members. TLOs meet quarterly and have organized training programs with guest speakers. CPD disseminates suspicious activity alerts, warnings, and notifications via intelligence bulletins to all law enforcement officers, as well as selected managers of critical infrastructure and other government agencies. The audience for these reports includes the command staff, the Deployment Operations Center's Web site, roll call distribution in each district office, the Law Enforcement Online (LEO) Special Interest Group, Homeland Security State and Local Intelligence Community of Interest, and the Regional Information Sharing Systems Secure Intranet (RISSNET).

## **OUTREACH TO THE PUBLIC**

Prior to and during the ISE-SAR EE, CPD had an aggressive outreach program to the community. The Chicago Alternative Policing Strategy is used to educate the public and business community regarding activities of CPD. A weekly bulletin is distributed to the business community, and posters are provided in public areas such as mass transit utilizing the "See something—Say something" concept. Additionally, officers are assigned to the downtown business district to implement the department's homeland security strategy.

## **PARTNERING WITH OTHER AGENCIES AND CONNECTING TO INFORMATION SHARING**

Prior to and during the ISE-SAR EE, CPD had developed partnerships with other public safety agencies and utilizes the TLO program to maintain and enhance relationships with its



partners. Additionally, the mayor of Chicago and city council committees are briefed on a regular basis concerning homeland security activities.

As noted during the site visits, CPD is a member of RISSNET, LEO, and the Homeland Security Information Network and can send and receive secure e-mails via RISSNET and LEO. CPD can access the Illinois criminal justice network and operates several city and regional information systems that are accessible by CID. CPD had a working relationship with the state fusion center; however, there is no direct electronic connectivity.

### **PARTNERING TO DEVELOP GEOGRAPHIC RISK ASSESSMENTS**

Prior to and during the ISE-SAR EE, CPD indicated that it had developed threat assessments and special assessments using data from the FBI, DHS, and CPD information reports. Although it does not have a formal information needs process, CPD works closely with the FBI, DHS, and U.S. Immigration and Customs Enforcement to gain relevant information and to provide that information to relevant partners. To determine and coordinate information needs, CPD staff members noted that they regularly work with the JTTF as well as the NOC and incorporate these information needs as appropriate. They also explained that the Human Intelligence Squad is responsible for developing information needs and managing human assets. These efforts provide additional feedback to CPD for further evaluation and analysis.

### **PROJECT RECOMMENDATIONS FROM THE CHICAGO POLICE DEPARTMENT**

- There needs to be some federal-level coordination; however, the initiative is primarily a local-agency issue.
- Training on SAR should be handled at the local level.
- A national users group would be beneficial to help local agencies coordinate their activities.
- There is a need for ongoing technical support for the current technology that has been deployed for the ISE-SAR Shared Spaces.
- There is no need for a national legal office; legal issues for the Nationwide SAR Initiative are mostly a local concern.

# **EXHIBIT 6**



# STIC Privacy Policy



Statewide Terrorism  
& Intelligence Center



**Illinois State Police  
Statewide Terrorism & Intelligence Center  
Privacy Policy**

**April 2010**

Article I. Mission Statement.....	3
Article II. Compliance and Governance.....	3
Article III. Definitions .....	4
Article IV. STIC Overview.....	4
A. Intelligence personnel.....	5
B. Division of Administration Personnel .....	5
C. STIC Data Sources.....	5
Article V. General Operating Procedures.....	6
A. Criminal Intelligence File.....	6
B. Standards for Initiating a Query .....	7
C. Collection Standards/Record Entry.....	7
D. Data Quality.....	8
E. Classifications.....	9
F. Labeling .....	10
G. Dissemination.....	10
H. Review and Purge Procedures .....	11
I. Security Procedures.....	11
J. Training .....	12
Article VI. STIC Data Sources.....	13
A. Law Enforcement Data Sources .....	13
B. Criminal Intelligence Data Stores.....	16
C. Public Data Sources including Commercial Systems .....	16
D. Flow of Information.....	17
Article VII. Authorized Persons .....	18
A. Authorized persons.....	18
B. Authorized users.....	18
Article VIII. Data Quality.....	18
A. Ownership of data.....	18
B. Verifying the accuracy of STIC Law Enforcement Data Sources.....	19
C. Verifying the accuracy of STIC Criminal Intelligence Data Stores.....	19
D. Merged Data.....	19
E. Access and Review .....	20
F. Record Challenges .....	20
Article IX. Access and Dissemination of Law Enforcement Data Sources.....	20
A. Access .....	20
B. Dissemination .....	21
Article X. Accountability.....	21
A. Programmatic audit logs.....	21
B. Secondary dissemination logs.....	22
C. Monitoring system use and conducting audits.....	22
D. Violations .....	22
E. Penalties .....	22
F. ISP Statewide VITAL Coordinator.....	23
G. VITAL Quality Control.....	23

## **Article I. Mission Statement**

The mission of the Illinois State Police (ISP) Statewide Terrorism & Intelligence Center (STIC) is to collect, evaluate, analyze, and disseminate information and intelligence data regarding criminal, terrorist and all-hazards<sup>1</sup> activities.<sup>2</sup> The STIC is comprised of intelligence and public safety officials from federal, state, and local law enforcement agencies whose primary goal is to provide timely, accurate, and actionable intelligence to public safety and private-sector partners. STIC operations enhance public safety, facilitate communication between agencies, and provide support in the fight against terrorism and criminal activity.

This Privacy Policy applies to all individuals unless otherwise specified. It describes how personally identifiable information is collected, used and secured. This Policy was prepared by the ISP Privacy Office and is designed to protect the privacy rights of U.S. citizens and other specified individuals.

## **Article II. Compliance and Governance**

All intelligence personnel, participating agency personnel, private contractors, and other authorized individuals<sup>3</sup> are required to abide by this Privacy Policy and applicable laws which govern the treatment of the information the center collects, receives, maintains, archives, accesses, or discloses. All intelligence personnel are required to provide written acknowledgement of receipt of this Privacy Policy and written agreement with its compliance. Nothing in this policy is intended to create a private right of action for any member of the public or alter existing or future federal and state law requirements.

STIC has adopted standard operating procedures and policies that comply with federal and Illinois law<sup>4</sup> concerning the appropriate collection, analysis, dissemination and retention of personally identifiable information and intelligence data.

The Illinois State Police Director has the primary responsibility for the overall operation of STIC including, but not limited to, its information systems, personnel, and operations.

Reports regarding alleged violations and suggestions for amendments shall be submitted to the Illinois State Police Privacy Office.<sup>5</sup>

---

<sup>1</sup> "All-hazards" is defined as events or incidents including, but not limited to, major accidents, natural disasters, and terrorist-related activity.

<sup>2</sup> 20 ILCS 2605/2605-45(4).

<sup>3</sup> Hereinafter referred to as "intelligence personnel."

<sup>4</sup> 28 Code of Federal Regulations (CFR) Part 23; 20 ILCS 2605/2605-45(4).

<sup>5</sup> These reports will be retained subject to the Illinois State Records Act, 5 ILCS 160.

## Article III. Definitions

- (1) **Actionable intelligence** - a relatively small piece or pieces of non-obvious detail(s) that can form an initial basis point for hypothesis building.
- (2) **Authorized persons** - Terrorism Research Specialists, Criminal Intelligence Analysts, Critical Infrastructure Specialists, Watch Officers, field intelligence personnel, public safety officials, certified police officers, and other criminal justice administrative and intelligence personnel in the furtherance of their official duties.
- (3) **Authorized users** - Terrorism Research Specialists, Criminal Intelligence Analysts, Critical Infrastructure Specialists, Watch Officers, field intelligence personnel, public safety officials, certified police officers, and other criminal justice administrative and intelligence personnel who meet certain qualifications outlined in this Policy.
- (4) **Individuals** - encompasses individuals as well as any group, association, corporation, business, partnership or other organization.
- (5) **Personally identifiable information** - any data that can be used to uniquely identify, contact, or locate a single person or entity.
- (6) **Private right of action** - a term used in United States statutory and constitutional law for circumstances a court will determine that a law that creates rights also allows private parties to bring a lawsuit, even where no such remedy is expressly provided for in the law.
- (7) **Public Safety Official** - a public safety official, serving with or without compensation, working in a public agency in an official capacity, including but not limited to a law enforcement officer, intelligence analyst, firefighter, or member of emergency medical response organization
- (8) **U.S. Citizen** - individuals born in the United States, Puerto Rico, Guam, Northern Mariana Islands, Virgin Islands, American Samoa, or Swain's Island; foreign-born children, under age 18, residing in the U.S. with their birth or adoptive parents, at least one of whom is a U.S. citizen by birth or naturalization; or individuals granted citizenship status by Immigration and Naturalization Services.
- (9) **VITAL** - Violent Crime Information Tracking and Linking System is ISP's data system that stores criminal justice data collected by intelligence personnel.

## Article IV. STIC Overview

Section A.	Intelligence personnel
Section B.	Division of Administration Personnel
Section C.	STIC Data Sources

## A. Intelligence Personnel

- (1) All STIC and field intelligence personnel (hereinafter referred to as intelligence personnel) are subject to the provisions of this Privacy Policy.
- (2) Intelligence personnel include:
  - (a) **Terrorism Research Specialists** who research and analyze potential terrorism suspect and incident data;
  - (b) **Criminal Intelligence Analysts** who research and analyze potential criminal activity, suspect, and incident data;
  - (c) **Critical Infrastructure Specialists** who research and analyze potential threats to critical infrastructure; and
  - (d) **Supervisors**
    - (i) **Watch Officer** – First level of supervision within STIC; oversees the day-to-day supervision, decision-making, and quality control functions.
    - (ii) **Assistant Center Chief (ACC)** – Provides administrative and supervisory oversight to the Watch Officers.
    - (iii) **Center Chief (CC)** – Responsible for all functions and activities of STIC and its employees; provides administrative and supervisory oversight to the ACC.

## B. Division of Administration (DOA) Personnel

- (1) Select ISP DOA personnel have access to information contained in law enforcement data systems and criminal intelligence data stores for the limited purpose of providing technical assistance.
- (2) DOA personnel who have access to intelligence data are subject to the provisions of this Privacy Policy.
- (3) Notwithstanding any provisions of this policy to the contrary, DOA personnel shall not disseminate criminal intelligence information.

## C. STIC Data Sources

- (1) Intelligence personnel gather information from a variety of data sources. Specifically, personnel access information contained in law enforcement data systems, criminal intelligence data stores, and publicly available records. Depending upon the type of investigation or potential criminal conduct, Intelligence personnel query certain specified data sources and compile information about individuals or groups for appropriate dissemination in accordance with this Policy.
  - (a) **Law Enforcement Data Systems** – Intelligence personnel may access traditional sources of law enforcement data.
  - (b) **Criminal Intelligence Data Stores** – Intelligence personnel have access to intelligence information submitted by law enforcement agencies and maintained internally.
  - (c) **Publicly Available Records** - Intelligence personnel may access public records through various public and privately compiled sources.

## **Article V. General Operating Procedures**

Section A.	Criminal Intelligence File
Section B.	Standards for Initiating a Query
Section C.	Collection Standards/Record Entry
Section D.	Data Quality
Section E.	Classifications
Section F.	Labeling
Section G.	Dissemination
Section H.	Review and Purge Procedures
Section I.	Security Procedures
Section J.	Training

The U.S. Department of Justice has promulgated administrative rules at 28 Code of Federal Regulations (CFR) Part 23. These regulations were designed to bring about an equitable balance between the civil rights and liberties of citizens and the needs of law enforcement to collect and disseminate criminal intelligence on the conduct of identifiable persons and groups who may be engaged in systematic criminal activity. The following procedures are intended to implement these regulations and apply to STIC operations and personnel absent a more stringent provision adopted herein.

### **A. Criminal Intelligence File**

- (1) A criminal intelligence file consists of stored information on the activities and associations of:
  - (a) Individuals who are reasonably suspected of being involved in the actual or attempted planning, organizing, financing, or commission of criminal acts; or
  - (b) Individuals who are reasonably suspected of being involved in criminal activities with known or suspected crime figures; or
  - (c) Organizations, businesses, and groups that are reasonably suspected of being substantially and significantly involved in the actual or attempted planning, organizing, financing, or commission of criminal acts (criminal organizations); or
  - (d) Organizations, businesses, and groups that are reasonably suspected of being operated, controlled, financed, or infiltrated by known or suspected crime figures for use in an illegal manner.
- (2) Types of Crimes Resulting in the Creation of an Intelligence File
  - (a) Any suspected crime that, in the reasonable judgment of the submitting agency or officer, represents a significant and recognized threat to the population and: (1) poses a threat to the life or property of citizens; (2) involves a permanent criminal organization; or (3) is not limited to one jurisdiction.



## **B. Standards for Initiating a Query**

- (1) Intelligence personnel may provide to law enforcement officials, upon request, criminal intelligence information upon a showing of reasonable suspicion of a crime.<sup>6</sup>

## **C. Collection Standards/Record Entry**

- (1) Intelligence personnel may collect and maintain criminal intelligence information concerning an individual or a group reasonably suspected of criminal conduct or activity.
- (2) Intelligence personnel will collect and maintain a record of the source of the information.<sup>7</sup>
- (3) For purposes of this Policy, reasonable suspicion is established when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise.
- (4) Intelligence personnel are responsible for establishing the existence of reasonable suspicion of criminal activity prior to submitting information about an individual or group into any intelligence data system.
- (5) Information submitted to an intelligence system must be relevant to the suspected criminal activity and subject identification.
- (6) Criminal intelligence information that intelligence personnel submit to an intelligence system shall be labeled to indicate the level of sensitivity of the record and the level of confidence in the information in accordance with this Policy.
- (7) STIC systems may include non-criminal identifying information in a criminal intelligence information submission, provided sufficient precautions are in place to make it clear to users the two different types of data that are being accessed.<sup>8</sup>
- (8) The ISP retains the right to reject any data element that is not relevant or that could pose an unreasonable risk of harm to the public.
- (9) Investigative techniques employed by Intelligence personnel shall be lawful and only so intrusive as to gather sufficient information to prevent criminal conduct or the planning of criminal conduct.
- (10) Intelligence personnel may not collect and maintain information concerning race, ethnicity, citizenship, place of origin, age, disability, gender, sexual orientation, political, religious, or social views,

---

<sup>6</sup> The reasonable suspicion requirement represents a higher standard than required by 28 CFR Part 23.20(e); Queries will not be conducted based solely upon violation of traffic laws.

<sup>7</sup> The record of the source of the information shall contain, where relevant and appropriate: (1) the name of the originating department, component, and subcomponent; (2) the name of the agency system from which the information is disseminated; (3) the date the information was collected and the date its accuracy was last verified; and (4) the title and contact information for the person to whom questions regarding the information should be directed.

<sup>8</sup> The 1998 Policy Clarification to 28 CFR Part 23.

associations, or activities of any individual or any group unless such information directly relates to criminal conduct or activity and there is reasonable suspicion that the subject of the information is or may be involved in such criminal conduct or activity.

#### **D. Data Quality**

- (1) Prior to entering information into any intelligence system, intelligence personnel shall evaluate the reliability of each data source and assess the content validity of the data. Proper labels shall be applied to all data submitted to an intelligence system.
- (2) If intelligence personnel have cause to believe the data contains an error or deficiency, they must contact the VITAL Quality Control Crime Information Evaluator for coordination with the source of the data.
- (3) Random VITAL audits are performed on a continual basis by VITAL Quality Control.
- (4) Intelligence personnel shall use the following labels for source reliability:
  - (a) Highly Reliable - The reliability of the source is unquestioned or has been well tested in the past.
  - (b) Usually Reliable - The reliability of the source can usually be relied upon as factual. The majority of information provided in the past has proven to be reliable.
  - (c) Not Often Reliable - The reliability of the source has been sporadic in the past.
  - (d) Unknown - The reliability of the source cannot be judged. Its authenticity or trustworthiness has not yet been determined by either experience or investigation.
- (5) ISP VITAL maintains a record of the source of the information.<sup>9</sup>
- (6) Intelligence personnel shall use the following labels for content validity:
  - (a) Factual - The information has been corroborated by an investigator or another independent, reliable source.
  - (b) Possibly True - The information is consistent with past accounts.
  - (c) Hearsay - The information is inconsistent with past accounts.
  - (d) Unknown - The authenticity of the information has not yet been determined by either experience or investigation.
- (7) A data element with a source reliability of "Unknown" and a validity assessment of "Unknown" may not be entered into an intelligence system.
- (8) Intelligence personnel will respond to any requests from authorized users for validation of previously disseminated data and, when information is identified that may be inaccurate or incomplete, includes incorrectly merged information, is out of date, cannot be verified, or lacks adequate context such that the rights of an individual may be

---

<sup>9</sup> *Supra* note 8.

affected, provide notice to authorized users who are known to have received the information.<sup>10</sup>

## E. Classifications

- (1) Prior to entering information into any intelligence system, intelligence personnel shall classify the data in order to protect sources, investigations, and the data subject's right to privacy. Intelligence personnel will treat information pertaining to any individual with the exact same level of privacy protection. Classification also indicates whether internal approval must be completed prior to the release of the information to persons outside STIC.
- (2) STIC classifies data into the following categories:
  - (a) **Confidential** – Confidential information is the highest level of unclassified but sensitive information. Access to information defined as “confidential” is limited, even among law enforcement officers.
  - (b) **Law Enforcement Sensitive (LES)** – LES information is middle level unclassified but sensitive information. LES may be disseminated to law enforcement personnel only.
  - (c) **For Official Use Only (FOUO)** – FOUO is unclassified information of a sensitive nature which can be disseminated outside the scope of law enforcement personnel (i.e., participating agency personnel, private contractors, and other authorized individuals). FOUO may not be released to the general public.
  - (d) **Protected Critical Infrastructure Information (PCII)** – Protected Critical Infrastructure Information (PCII) is a subset of Critical Infrastructure Information for which protection is requested under the PCII Program by the requestor. Critical Infrastructure Information is information related to the security of critical infrastructure or protected systems that are not customarily in the public domain.
  - (e) **Open Source** – Open source information is any information that is publicly available. This information will be marked as “Unclassified” using an indicator of (U).
- (3) **Classification** - All intelligence information has its security classification marked directly on the information file.
- (4) **Re-evaluation of Classification**  
Re-evaluations can be based upon time (i.e., tied to the five-year retention/renewal); the addition of new information; or at the time of a request for the information.

---

<sup>10</sup> As required by 28 CFR Part 23.20(h).

## **F. Labeling**

- (1) All criminal intelligence information disseminated will be labeled as such so that the recipient can handle the information in accordance with applicable legal requirements.
- (2) Information labeled as non-intelligence information will be maintained and disseminated in the same manner as intelligence information.
- (3) The data contained within STIC criminal intelligence systems will be identified as intelligence or non-intelligence information and any applicable legal requirements for handling such data indicated is provided in paragraph E of this Article.

## **G. Dissemination**

- (1) Intelligence personnel may disseminate criminal intelligence information only to law enforcement or criminal investigative authorities who agree to follow procedures regarding the receipt, maintenance, security, and dissemination of information that are consistent with 28 CFR Part 23 and this Policy.
- (2) Intelligence personnel may disseminate criminal intelligence information to law enforcement or criminal investigative authorities who demonstrate a need and right to know the information in the performance of a law enforcement activity.<sup>11</sup>
- (3) Intelligence personnel may disseminate an assessment (not including personally identifiable information) of criminal intelligence information to any individual where necessary to avoid imminent danger to life or property.
- (4) An access log/audit trail or dissemination record is required when the database is accessed or information is disseminated from the intelligence system. This record can be created automatically by the database, or policies and procedures can be implemented to handle the access log/audit trail or dissemination record manually. The dissemination record shall contain the following information:
  - (a) The date of dissemination of the information;
  - (b) The name of the individual requesting the information;
  - (c) The name of the agency requesting the information;
  - (d) The reason for the release of the information (i.e., a description of the need to know and right to know);
  - (e) The information provided to the requester; and
  - (f) The name of the individual from STIC disseminating the information.
- (5) Secondary dissemination of STIC data is permissible provided the dissemination would have been allowable directly from STIC systems under the terms of this Policy.

---

<sup>11</sup> Need to know is established where the prospective recipient requires access to specific information in order to perform or assist in a lawful and authorized governmental function (i.e., access is required for the performance of official duties). Right to know is established where the prospective recipient is an authorized individual acting in furtherance of a valid law enforcement or public safety function.

## H. Review and Purge Procedures<sup>12</sup>

- (1) Intelligence personnel will make every reasonable effort to ensure that information maintained in intelligence systems about individuals is current, accurate, and relevant. To accomplish this, intelligence personnel shall annually review intelligence information. The maximum retention period is five years, unless the intelligence information is validated and updated to ensure continuing compliance with system submission criteria.
- (2) STIC intelligence databases automatically run daily checks for data that has met the five-year retention period. Data that has not been validated is purged.
- (3) The entire record including all accompanying descriptive, identifying, and non-criminal identifying data must be validated. A record must be maintained of the name of the reviewer, date, and explanation of why the information is retained. Once validated, the retention period for the information may be extended for up to five more years.
- (4) If the information has not been updated and/or validated, it must be removed from the system at the end of the retention period. Material purged from the intelligence system shall be destroyed.<sup>13</sup>
- (5) Information removal must be approved by STIC Chief or designee.
- (6) STIC will retain a record of dates when information is to be removed (purged) if not validated prior to the end of its five-year period.
- (7) Non-intelligence information will be maintained and/or destroyed in accordance with the Illinois State Records Act.<sup>14</sup>

## I. Security Procedures

- (1) STIC is committed to protecting privacy and maintaining the integrity and security of personal information. STIC shall be responsible for implementing the following security requirements for its intelligence systems.
- (2) STIC has formally adopted the Criminal Justice Information Systems (CJIS) Security Policy of the U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division<sup>15</sup> and applies these provisions to STIC operations. STIC will develop a separate security policy.
- (3) Firewalls are in place to prevent unauthorized agencies or entities from accessing STIC resources.
- (4) **Role-based user access** – The intelligence systems that intelligence personnel access utilize various levels of role-based user access.
  - (a) Each user's role shall determine the types of information accessible to the user.

---

<sup>12</sup> 28 CFR Part 23; 20 ILCS 2605/2605-45(4).

<sup>13</sup> Electronic records are permanently deleted and paper files are shredded.

<sup>14</sup> 5 ILCS 160/.

<sup>15</sup> May 2006 Version 4.3.

- (b) Each user's role contains certain permissions to modify or delete records.
- (5) **Security breaches and security breach notification** –ISP will monitor and respond to security breaches or breach attempts.<sup>16</sup>
  - (a) In the event that intelligence personnel become aware of a breach of the security of unencrypted personal information, ISP will notify an individual about whom personal information was or is reasonably believed to have been obtained by an unauthorized person and access to which threatens the physical or financial harm to the person.
  - (b) Any necessary notice will be made promptly and without unreasonable delay following discovery or notification of the access to the information, consistent with the legitimate needs of law enforcement to investigate the release or any measures necessary to determine the scope of the release of information and if necessary, to reasonably restore the integrity of any information system affected by this release.
- (6) **Physical Safeguards** – STIC systems shall be located in a physically secured area that is restricted to designated authorized personnel.
  - (a) Only designated authorized personnel will have access to information stored in the STIC data systems.
  - (b) All authorized visitors, regardless of agency, are required to register with designated authorized personnel prior to gaining admission to the facility.
  - (c) All authorized registered visitors will be escorted by designated authorized personnel for the duration of the visit.
- (7) **Disaster Recovery** – ISP has appropriate disaster recovery procedures for STIC data outlined in ISP's Disaster Recovery Plan.
- (8) **Information Security Officers** - Federal agencies housed at STIC each have a dedicated information security officer. STIC has an Information Security Officer who is trained and handles network access/security.
- (9) **Assessment Storage** - Risk and vulnerability assessments are stored separately from law enforcement and intelligence data. Risk and vulnerability assessments are not available to the public.

## J. Training

### (1) Personnel Training

- (a) STIC has adopted the Department of Homeland Security Standards as the education and training standard for its Terrorism Research Specialists, Criminal Intelligence Analysts, and Critical Infrastructure Specialists.
- (b) All intelligence personnel are provided training on this Privacy Policy.

---

<sup>16</sup> See 815 ILCS 530/.

- (c) DOA personnel who have access to STIC data are provided training on this Privacy Policy.
- (d) Training is provided on this Privacy Policy to all intelligence personnel, including Watch Officers, Statewide Zone Intelligence Officer Coordinator and Management (Center Chief and Assistant Center Chief).
- (e) STIC will provide training to personnel authorized to access and/or disseminate data, including terrorism-related data.
- (f) The ISP Privacy Officer is a licensed attorney and a Certified Information Privacy Professional.
- (g) Private sector personnel in contractual relationships with ISP STIC will receive training on this Privacy Policy.

**(2) Policy Awareness**

- (a) This Privacy Policy will be displayed for general view on the ISP website.
- (b) Individuals authorized to access or disseminate intelligence information from STIC will be provided access to and acknowledge a thorough understanding of this Privacy Policy.

**(3) Policy Updates**

- (a) The ISP Privacy Officer will update this Privacy Policy as new information sources are accessed through STIC.
- (b) The ISP Privacy Officer will monitor legislative activity and update this Privacy Policy accordingly.
- (c) The ISP Privacy Office will review this Privacy Policy annually and update it accordingly.
- (d) Updated policies will contain the policy revision date and version number.
- (e) Individuals authorized to access or disseminate intelligence information from STIC will be informed of policy updates as they become effective.

## **Article VI. STIC Data Sources**

Section A.	Law Enforcement Data Sources
Section B.	Criminal Intelligence Data Stores
Section C.	Public Data Sources
Section D.	Flow of Information

### **A. Law Enforcement Data Sources**

Data from the following systems is not aggregated into a central database or repository. Rather, an analyst accesses each system separately to acquire relevant records related to a data subject. This list is not static but may change in the future as databases are merged, new databases are added or databases that do not prove useful to the mission of STIC are removed.

- (1) The Illinois Law Enforcement Agencies Data System (LEADS) is a statewide, computerized, telecommunications system, maintained by the Illinois State Police, designed to provide the Illinois criminal justice community with access to computerized justice-related information from both the state and national level. Data within LEADS includes, but is not limited to, active warrants, federal criminal information and files from the Illinois Secretary of State (SOS).
- (2) Citizen and Law Enforcement Analysis and Reporting system (CLEAR) is an information technology system managed by the Chicago Police Department enabling Chicago police to quickly share police incident report data and crime mapping software, among other types of information.
- (3) El Paso Intelligence Center (EPIC) provides timely and expeditious information to federal, state, local, tribal, and international law enforcement agencies concerning drug interdiction and trafficking, alien and weapon smuggling, counterterrorism and other criminal activities. The systems queried include EPIC's in house computer, TECS (US Customs and Treasury), NADDIS (DEA), INS (including border crossings), FAA (Federal Aviation Association) and SENTRY-BOP.
- (4) Mid-State Organized Crime Information Center (MOCIC) is part of the overall Regional Information Sharing Systems (RISS) network. This network searches multiple databases and provides access to criminal intelligence information in the region.
- (5) Illinois Secretary of State (SOS) offers access to its data via LEADS. This access provides digital driver's license photographs & VISAGE Facial Recognition System data.
  - (a) STIC will not store SOS information; Rather STIC will contain a link to LEADS which will, in turn, provide for access to the SOS database.
  - (b) SOS data available through this link includes a subject's name, address, date of birth, gender, and digital image.
- (6) The Offender Tracking System (OTS) database is managed by the Illinois Department of Corrections. OTS provides various forms of information on individuals who have been entered into the Illinois Correctional system.
- (7) Illinois Department of Public Aid database provides access to information on wanted suspects, public aid and medicaid fraud, and sex offenders.
- (8) The Law Enforcement Online (LEO) system is maintained by the FBI and provides a secure network that LEO members – including the law enforcement community, criminal justice officials, first responders, public safety officials, and members of the Intelligence and counterintelligence communities – can use to store, process, and transmit sensitive but unclassified information.



- (9) The U.S. Department of Justice Regional Data Exchange System (RDEx) is part of the Department's Law Enforcement Information Sharing Program (LEISP). RDEx includes information to facilitate regional sharing initiatives which serves to further the LEISP's principal purpose of ensuring that criminal law enforcement information is available for users at all levels of government so that they can more effectively investigate, disrupt, and deter criminal activity, including terrorism, and protect the national security.
- (10) Illinois State Police INDICES - indexed Illinois State Police case records database.
- (11) Targeted Violence Information Sharing System (TAVISS) is a pointer system administered by the U.S. Secret Service National Threat Assessment Center and consists of a database of subjects who have threatened or inappropriately communicated with protectees from federal, state and local agencies.
- (12) Transportation Safety Administration Federal Air Marshal Service Tactical Information Sharing System (TISS) is a database system that stores information, including photos, from suspicious activity reports, incident and arrest reports, and other sources for immediate retrieval and analysis.
- (13) Financial Crimes Enforcement Network (FinCEN) is managed by the U. S. Department of Treasury and provides information to safeguard against financial crime, including terrorist financing, money laundering, and other illicit activity.
- (14) Suspicious Activity Reports – STIC does not have a tips/leads hot-line system for law enforcement or the public. However, law enforcement agencies and private sector security directors may report suspicious activity directly to STIC. If the suspicious activity reported contains personally identifying information, it must meet the Collection Standards outlined in Article V, Section C of this Policy.
- (15) SAFETNet – a database containing information on Illinois Department of Transportation numbers and safety inspections of commercial motor vehicles.
- (16) Illinois Department of Employment Security - a database containing unemployment and tax information on employers and their personnel.
- (17) Traffic Information and Planning System (TIPS) - contains information regarding prior traffic-related contacts with the ISP.
- (18) Firearm Owner's Identification Database/FTIP - database used to check an individual's record of purchasing and eligibility to purchase firearms.
- (19) Illinois State Police Internet Crimes Complaint database - a case tracking database used by the Internet Crimes Unit to initiate an investigation into purported internet crimes.

## **B. Criminal Intelligence Data Stores**

STIC has two stores of criminal intelligence information – VITAL and the STIC Network Drive. Both of these systems shall comply with 28 CFR Part 23.

- (1) VITAL is a data system that stores criminal justice data collected by intelligence personnel. VITAL is intended to enhance cross-jurisdictional information sharing and to facilitate crime prevention, crime fighting, and counter-terrorism efforts taking place throughout Illinois. Specifically, VITAL stores and disseminates intelligence data to assist crime investigators and patrol officers.
  - (a) **Entries into VITAL** – All data from any of STIC's data sources which meets the requirements of 28 CFR Part 23 may be entered into VITAL. Information that does not meet 28 CFR Part 23 collection standards is not entered into VITAL.
  - (b) **Downloads of VITAL** – Regularly scheduled downloads from the VITAL database to the FBI Regional Data Exchange database (R-DEx) warehouse will occur upon written agreement between ISP and the R-DEx Board.
- (2) The STIC Network Drive contains both intelligence and non-intelligence information. Intelligence information will only be stored in specific folders to be designated by STIC Management. The folders containing intelligence information will be easily discernible from others in the network drive to ensure proper security and review of files contained therein.

## **C. Public Data Sources including Commercial Systems**

Data from the following systems is not aggregated into a central database or repository. Rather, an analyst accesses each system separately to acquire relevant records related to a data subject. The ISP may contract with commercial providers to obtain this relevant data. The providers agree in writing to comply with all federal and state laws and provide quality data to industry standards. The ISP will only gather data with agency authority under state law.<sup>17</sup> Information will not be collected when the source agency used prohibited means to gather it.

- (1) Lexis-Nexis/Accurint provides background information to government agencies on individuals, businesses, addresses, vehicles, judgments and liens, social security numbers, media news articles, among other data.
- (2) Dun and Bradstreet database provides business information and is also a credit rating provider.
- (3) Westlaw provides access to statutes, case law materials, public records and other legal resources, as well as current news articles and business information.
- (4) National and State Sex Offender Registration Web Sites

---

<sup>17</sup> 20 ILCS 2605/2605-45(4).

- (a) Intelligence personnel will have access to links to public Sex Offender Registration Web Sites.
  - (b) Sex offender registration information available through these links includes a registrant's name, address, physical description, and digital image along with their compliancy status, crime and the county of conviction.
- (5) Federal Bureau of Prisons and State Departments of Corrections (DOC)<sup>18</sup> public websites provide inmate information on currently-incarcerated individuals.
- (a) Intelligence personnel will have access to a link to public DOC websites.
  - (b) DOC information available through these links includes parent institution, inmate status, location, physical description and digital image along with sentencing information and admission, release or discharge data.
- (6) Experian offers online credit reports and credit bureau data.
- (7) Interpol is the largest International Police Association which facilitates cross-border police co-operation, and supports and assists all organizations, authorities and services to prevent or combat international crime.
- (8) National Insurance Crime Bureau (NICB) assists law enforcement in their detection and deterrence of insurance fraud and vehicle theft.
- (9) Methamphetamine Registries

#### D. Flow of Information

- (1) **Tactical Work-Up** – This is a request for information when the requesting law enforcement officer is on an active traffic or criminal stop. The analyst conducts an abbreviated search of intelligence databases with a goal to return the relevant information to the officer within a reasonable time. Once the basic information is relayed to the officer, the analyst completes a full database work-up.
- (a) LEADS, RDEx, and VITAL will be checked during every preliminary work-up. The analysts will check other relevant data sources at their discretion.
- (2) **Full Database Work-Up** – The analyst determines the nature of the request, searches all relevant databases and sources of information, documents all information, and disseminates the information as appropriate.
- (3) **Daily Intelligence Notes** – The analyst gathers topic information, researches and verifies that information, receives authorization from the Watch Officer, and disseminates it based upon classification.
- (4) **Intelligence Alerts** – Intelligence alerts can be STIC analyst originated or pass-through products obtained by STIC from other intelligence fusion centers or sources.

---

<sup>18</sup> For purposes of this Policy, "DOC" refers to the Federal Bureau of Prisons and all state Departments of Correction.

- (5) **Threat/Event Assessments** – STIC will compile background and threat information for purposes of providing assessments of events. Examples include, but are not limited to, events with large attendance expected, venues or sites of previous threats, violence or criminal activity, and those events which may have national significance.

## **Article VII. Authorized Persons**

- Section A. Authorized persons  
Section B. Authorized users

### **A. Authorized persons**

- (1) For purposes of this Policy, authorized persons are Terrorism Research Specialists, Criminal Intelligence Analysts, Critical Infrastructure Specialists, Watch Officers, field intelligence personnel, public safety officials, certified police officers, and other criminal justice administrative personnel in the furtherance of their official duties.
- (2) Authorized users may disseminate STIC data to authorized persons as defined in this Section only in accordance with the dissemination rules of this Policy.

### **B. Authorized users**

- (1) For purposes of this Policy, authorized users are Terrorism Research Specialists, Criminal Intelligence Analysts, Critical Infrastructure Specialists, Watch Officers, field intelligence personnel, public safety officials, certified police officers, and other criminal justice administrative personnel, who:
- (a) Are approved for STIC access by the ISP; and
  - (b) Meet, at a minimum, the certification requirements for STIC access; and
  - (c) Undergo training regarding the system's capabilities as well as the appropriate use and sharing of data accessed through STIC.

## **Article VIII. Data Quality**

- Section A. Ownership of data  
Section B. Verifying the accuracy of STIC Law Enforcement Data Sources  
Section C. Verifying the accuracy of STIC Intelligence Stores  
Section D. Merged Data  
Section E. Access and Review  
Section F. Record Challenges

### **A. Ownership of data**

- (1) All data accessed through a law enforcement or public data source is considered to be the property of that source.
- (2) Because it retains ownership of the data, each source is ultimately responsible for the quality and accuracy of its data.

- (3) STIC notifies the originating agency or the originating agency's privacy officer when the center reviews the quality of the information it has received from an originating agency and identifies data that: (1) may be inaccurate or incomplete; (2) may include incorrectly merged information; (3) may be out of date; (4) cannot be verified; or (5) lacks adequate context such that the rights of the individual may be affected.
- (4) Notification pursuant to Section (A)(3) above is documented via e-mail to STIC Supervisors, consistent with Article IV (A)(2)(d), who ensure the information is not entered into VITAL.
- (5) All data entered into VITAL and the STIC Network Drive is deemed the property of the Illinois State Police.

### **B. Verifying the accuracy of STIC Law Enforcement Data Sources**

Inaccurate information can have a damaging impact upon the data subject and the integrity and functional value of STIC query responses. Any information obtained through a query to STIC from Law enforcement data sources must be independently verified with the original source from which the data was extrapolated before any official action (e.g., search warrant application or arrest) is taken. Law enforcement officers and agencies are responsible for verifying the quality and accuracy of the data.

### **C. Verifying the accuracy of STIC Criminal Intelligence Data Stores**

Any information obtained through a query to STIC from Criminal Intelligence Data Stores must be independently verified with the original source from which the data was extrapolated before any official action (e.g., search warrant application or arrest) is taken. Law enforcement officers and agencies are responsible for verifying the quality and accuracy of the data.

### **D. Merged Data**

- (1) Due to the potential harm caused by inaccurate merging of information, data about an individual from two or more sources will not be merged by a STIC Terrorism Research Specialist or Criminal Intelligence Analyst unless the identifiers or characteristics, when combined, clearly establish that the information from multiple records is about the same individual.
- (2) If the matching requirements cannot fully be met but there is an identified partial match, the information may be merged only if accompanied by a statement that it has not been adequately established that the information relates to the same individual or organization.

## **E. Access and Review**

- (1) In order to avoid interference with criminal investigations, members of the public cannot access STIC or individually identifiable information on themselves or others.<sup>19</sup>
- (2) Persons wishing to access data pertaining to themselves should communicate directly with the source of the data in question.<sup>20</sup>
- (3) Reports regarding alleged violations and suggestions for amendments shall be submitted to the Illinois State Police Privacy Office.<sup>21</sup>

## **F. Record Challenges**

Persons wishing to challenge records should communicate directly with the agency source of the data in question.

# **Article IX. Access and Dissemination of Law Enforcement Data Sources**

Section A. Access  
Section B. Dissemination

## **A. Access**

- (1) Access permissions, generally
  - (a) The information accessed through STIC is information that has been accessible to law enforcement officers for many years. STIC technology will permit authorized users to retrieve and analyze these same records in an efficient and timely manner as a law enforcement investigative tool.
  - (b) The public shall not have access to STIC data.
- (2) Use for legitimate investigative purposes
  - (a) Information obtained from or through STIC can only be used for official law enforcement investigative purposes.

---

<sup>19</sup> Requests for this information are treated as Illinois Freedom of Information Act requests and will be retained consistent with that statute. See 5 ILCS 140.

<sup>20</sup> STIC will not provide these individuals with a list of sources.

<sup>21</sup> If an individual has a complaint or objection to the accuracy or completeness of terrorism-related information that has been or may be shared through the ISE that: (a) is held by the STIC; (b) allegedly resulted in harm to the complainant; and (c) is exempt from public disclosure, the STIC will inform the individual of the procedure for submitting, if needed, and resolving complaints or objections. Complaints will be received by Lt. Kathleen deGrasse, ISP Privacy Officer, at the following address: 9511 W. Harrison St., Des Plaines, IL 60016. The STIC will acknowledge the complaint and state that it will be reviewed, but will not confirm the existence of the information that is exempt from disclosure. If the information did not originate with the STIC, STIC will notify the originating agency in writing and, upon request, assist such agency to correct or purge any identified data/record deficiencies or to verify that the record is accurate. Any personal information originating with the STIC will be reviewed and corrected in or deleted from STIC data/records if it is determined to be erroneous, include incorrectly merged information, or be out of date. The ISP Privacy Office will maintain records of complaints and correction requests and the resulting action, if any.

- (b) An official law enforcement investigative purpose means that the request for data is directly linked to a law enforcement agency's active criminal case investigation or is in response to a confirmed lead that requires additional corroboration.

## **B. Dissemination**

- (1) Prohibitions on dissemination, generally
  - (a) Except as otherwise provided in this policy, information obtained from or through STIC:
    - (i) Cannot be sold, published, exchanged, or otherwise disclosed, to the public or for commercial purposes; and
    - (ii) Can only be disseminated to authorized persons.
- (2) Confidentiality
  - (a) Intelligence personnel shall protect the confidentiality of all data entered or accessed through STIC.
- (3) Research purposes
  - (a) The Illinois State Police may use the information accessed through STIC for research purposes in the aggregate, but such aggregate or analyzed data may not be identifiable to any person without the express consent of the individual.
- (4) Secondary dissemination, generally
  - (a) Authorized users may only disseminate information accessed through STIC to other authorized persons in order to fulfill their criminal justice functions.
  - (b) All secondary disseminations must be logged in accordance with Article X of this Policy.

## **Article X. Accountability**

Section A.	Programmatic audit logs
Section B.	Secondary dissemination logs
Section C.	Monitoring system use and conducting audits
Section D.	Violations
Section E.	Penalties
Section F.	Statewide VITAL Coordinator
Section G.	VITAL Quality Control Unit

Intelligence personnel and agencies accessing STIC data must follow all applicable state and federal laws and regulations, including rules and regulations of the Illinois State Police, regarding the use and dissemination of STIC data.

### **A. Programmatic audit logs**

- (1) Queries to VITAL will be logged by the system and identify the user initiating the query. The dissemination log must contain:
  - (a) A description of the information queried (including the identity or identities to whom the information relates);
  - (b) The date the information was queried;

- (c) The individual who conducted the query (including their agency and contact information);
- (d) The authorized person to whom the information was disseminated.

## **B. Secondary dissemination logs**

- (1) When information accessed through STIC is disseminated outside the agency from which the original request is made, a secondary dissemination log must be maintained by the disseminating agency. The dissemination log must contain:
  - (a) A description of the information disseminated (including the identity or identities to whom the information relates);
  - (b) The date the information was released;
  - (c) The individual to whom the information was released (including their agency and contact information); and
  - (d) The purpose for which the information will subsequently be used.
- (2) Whenever information labeled "confidential" is disseminated outside the agency from which the original request was made, the secondary dissemination log must specify the demonstrable need to know.

## **C. Monitoring system use and conducting audits**

- (1) The Illinois State Police is responsible for monitoring the use of all STIC data sources to guard against inappropriate or unauthorized use.
- (2) The Illinois State Police will investigate misuse of STIC data and conduct or coordinate audits concerning the proper use and security of STIC data by users.
- (3) All STIC inquiries by authorized persons will be made available, upon request, to that authorized person's agency.

## **D. Violations**

- (1) When the Illinois State Police learn of a violation of policies, laws, or regulations concerning the use of STIC data, it must notify the chief executive of the offending agency in writing. Agencies must take action to correct such violations and provide an assurance in writing to the STIC Center Chief that corrective action has been taken.
- (2) Any suspected or documented misuse of STIC information discovered by or reported to a law enforcement agency must be reported by that agency to the Illinois State Police.

## **E. Penalties**

- (1) The failure of a law enforcement agency to remedy violations may result in suspension or termination of access to STIC data.



## **F. ISP Statewide VITAL Coordinator**

- (1) The ISP will appoint a Statewide VITAL Coordinator who is responsible for training intelligence personnel in the use of VITAL and 28 CFR Part 23.
- (2) The ISP Statewide VITAL Coordinator will maintain all authorized VITAL users' access forms and certification training materials at the STIC facility.

## **G. VITAL Quality Control**

- (1) The VITAL Quality Control Unit was formulated to ensure and maintain the integrity of the VITAL project database in compliance with 28 CFR Part 23.
- (2) This unit has full and complete authoritative review of all information entered into the VITAL intelligence database.
- (3) A second level of review shall be performed by VITAL Quality Control staff responsible for reviewing all entries of new VITAL users.
- (4) All entries of new users are reviewed for the first 90 days; thereafter, Quality Control staff will randomly review 25 percent of all users' entries.
- (5) Where information is found to be erroneous or deficient such that an individual's privacy rights are impacted, the VITAL Quality Control Crime Information Evaluator's responsibilities are limited to notifying the original source agency in writing for their follow-up and correction.<sup>22</sup>

---

<sup>22</sup> When data is obtained from that source agency, it once again goes through reliability checks prior to labeling. See Article V, Section D of this Policy.



Printed by the Authority of the State of Illinois  
ISP Central Printing Section  
Printed on Recycled Paper  
ISP 5-824 (9/10) M  
[www.illinois.gov](http://www.illinois.gov) [www.isp.state.il.us](http://www.isp.state.il.us)

# **EXHIBIT 7**

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE  
PROGRAM MANAGER, INFORMATION SHARING ENVIRONMENT  
WASHINGTON, DC 20511

May 21, 2009

MEMORANDUM FOR HEADS OF DEPARTMENTS AND AGENCIES

SUBJECT: Release of the Information Sharing Environment (ISE) Functional Standard for Suspicious Activity Reporting, Version 1.5 (ISE-FS-200)

REFERENCE: 1) Presidential Memorandum of December 16, 2005, subject: Guidelines and Requirement in Support of the Information Sharing Environment  
2) National Strategy for Information Sharing, October 2007

On January 25, 2008 I issued the first Common Terrorism Information Sharing Standard (CTISS) for Suspicious Activity Reporting (SAR) in accordance with Presidential Memorandum directing the development and issuance of common standards governing how terrorism information is acquired, accessed, shared, and used within the ISE. This updated version of the *ISE-SAR Functional Standard* incorporates suggestions provided by federal privacy and civil liberties attorneys and members of the privacy and civil liberties advocacy community, and:

- Refines the definition of Suspicious Activity as, “*observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity.*”
- Clarifies that the same constitutional standards that apply when conducting ordinary criminal investigations also apply to law enforcement and homeland security officers conducting SAR inquiries.
- Further emphasizes a behavior-focused approach to identify suspicious activity and requires that factors such as race, ethnicity, national origin, or religious affiliation should not be considered as factors that create suspicion (except if used as part of a specific suspect description).
- Refines the ISE-SAR Criteria Guidance to distinguish between those activities that are Defined Criminal Activity and those that are Potentially Criminal or Non-Criminal Activity requiring additional fact information during investigation.
- Clarifies those categories of activity which are generally First Amendment-protected activities should not be reported in a SAR or ISE-SAR absent articulable facts and circumstances that support the source agency’s suspicion that the behavior observed is reasonably indicative of criminal activity associated with terrorism.
- Updates the operational process descriptions to align the standard with the *Nationwide SAR Initiative Concept of Operations*, released in December 2008.

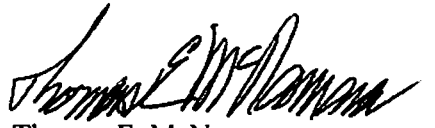
All CTISS, to include this *ISE-SAR Functional Standard*, will be implemented by ISE participants into supporting infrastructures in accordance with the *ISE Enterprise Architecture*

*Framework.* This *ISE-SAR Functional Standard* is also in alignment with the *National Strategy for Information Sharing (NSIS)*, which outlines federal, state, local, and tribal responsibilities for sharing ISE-SAR data.

This *ISE-SAR Functional Standard* documents information sharing exchanges and business requirements, and describes the structure, content, and products associated with processing, integrating, and retrieving ISE-SAR by ISE participants. Each Information Sharing Council (ISC) member and other affected agencies responsible for the collection and processing of SARs with a nexus to terrorism must apply this Functional Standard when processing, integrating, and retrieving ISE-SAR, and incorporate this Functional Standard into their business processes development and information resource planning. In particular, ISC agencies should, as appropriate, incorporate this *ISE-SAR Functional Standard* and any subsequent implementation guidance into budgetary planning activities associated with current (operational) and future development efforts associated with relevant mission-specific programs, systems, or initiatives. As appropriate, departments and agencies may consider utilizing this standard as part of the grant application process.

This updated version of the *ISE-SAR Functional Standard* will continue to be tested and evaluated by the user community. Any resulting refinements, including changes to SAR business processes and data elements, will be incorporated in future versions. Privacy assessments will also be performed as appropriate to identify privacy issues that may arise in implementing this *ISE-SAR Functional Standard* and information flow. This *ISE-SAR Functional Standard* is not intended to address all the implementation issues associated with the reporting, tracking, processing, accessing, storage, and retrieval of SAR information within the ISE; it is one component of the overall Nationwide SAR Initiative.

Please address any questions associated with this *ISE-SAR Functional Standard* to your designated ISC Representative (Attachment B) or the Office of the Program Manager.



Thomas E. McNamara

**Attachments:**

- A. Information Sharing Environment (ISE) Functional Standard (FS) for Suspicious Activity Reporting (SAR), Version 1.5 (ISE-FS-200)
- B. Information Sharing Council Members
- C. Fact Sheet: Update to Suspicious Activity Reporting Functional Standard Provides Greater Privacy and Civil Liberties Protections

cc: Information Sharing Council

# **EXHIBIT 8**

## ISE-SAR CRITERIA GUIDANCE

Category	Description
<b>DEFINED CRIMINAL ACTIVITY AND POTENTIAL TERRORISM NEXUS ACTIVITY</b>	
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.
<b>POTENTIAL CRIMINAL OR NON-CRIMINAL ACTIVITY REQUIRING ADDITIONAL FACT INFORMATION DURING INVESTIGATION</b>	
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.
Recruiting	Building of operations teams and contacts, personnel data, banking data or travel data
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
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.

**Note:** These activities are generally First Amendment-protected activities and should not be reported in a SAR or ISE-SAR absent 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 should not be considered as factors that create suspicion (although these factors may be used as specific suspect descriptions).

This list can be found in the Information Sharing Environment (ISE) Suspicious Activity Reporting (SAR) Functional Standard Version 1.5, which can be downloaded from [www.ise.gov](http://www.ise.gov).

UNCLASSIFIED

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.

**Note:** These activities are generally First Amendment-protected activities and should not be reported in a SAR or ISE-SAR absent 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 should not be considered as factors that create suspicion (although these factors may be used as specific suspect descriptions).

This list can be found in the Information Sharing Environment (ISE) Suspicious Activity Reporting (SAR) Functional Standard Version 1.5, which can be downloaded from [www.ise.gov](http://www.ise.gov).



# **EXHIBIT 9**



# Communities Against Terrorism

## Potential Indicators of Terrorist Activities

### Related to Mass Transportation

#### What Should I Consider Suspicious?

##### Related to Individual Appearance, General Behavior, and Communications:

- Significantly alters appearance from visit to visit (shaving beard, changing hair color, style of dress, etc)
- Burns on body, missing finger(s) or hand, bloody clothing, bleached body hair or bright colored stains on clothing; switch or wires concealed in hand, clothing or backpack
- Passing anonymous threats (telephone/e-mail) to facilities in conjunction with suspected surveillance incidents
- Acting nervous or suspicious, possibly mumbling to themselves, heavy sweating
- Monitoring personnel or vehicles entering/leaving facilities or parking areas
- Behaving as if using a hidden camera (panning a briefcase/bag over a particular area or constantly adjusting angle or height of an item)
- Discreetly using cameras, video recorders, binoculars, or note taking and sketching
- Unusual comments made regarding anti-U.S., radical theology, vague or cryptic warnings
- Questioning security/facility personnel through personal contact, telephone, mail, or e-mail

##### Related to Passenger Activities or Interests in Security:

- Multiple people arriving together, splitting up; may continue to communicate via cell phone
- Unusual or prolonged interest in the following:
  - Security measures or personnel
  - Security cameras
  - Entry points and access controls
  - Perimeter barriers (fences/walls)
  - Unattended train or bus
- Parking vehicles in restricted zones or purposely placing objects in sensitive or vulnerable areas to observe security responses
- Attempting to acquire official vehicles, uniforms, badges, access cards, or identification credentials for key facilities (report such losses and deactivate access cards immediately)
- Observing security reaction drills or procedures (may leave an unattended package to probe)

*It is important to remember that just because someone's speech, actions, beliefs, appearance, or way of life is different; it does not mean that he or she is suspicious.*

#### To Report a Suspicious Purchase or Activity

Email: [tripwire@chicagopolice.org](mailto:tripwire@chicagopolice.org).

In Emergency DIAL 911 and indicate

"Tripwire Program" incident

#### What Should I Do?

##### Be part of the solution.

- ✓ Require valid ID from all customers.
- ✓ Keep records of purchases.
- ✓ Talk to customers, ask questions, and listen to and observe their responses.
- ✓ Watch for people and actions that are out of place.
- ✓ Make note of suspicious statements, people, and/or vehicles.
- ✓ If something seems wrong, notify law enforcement authorities.

##### Do not jeopardize your safety or the safety of others.

Preventing terrorism is a community effort. By learning what to look for, you can make a positive contribution in the fight against terrorism. The partnership between the community and law enforcement is essential to the success of anti-terrorism efforts.

Some of the activities, taken individually, could be innocent and must be examined by law enforcement professionals in a larger context to determine whether there is a basis to investigate. The activities outlined on this handout are by no means all-inclusive but have been compiled from a review of terrorist events over several years.





# Communities Against Terrorism

## Potential Indicators of Terrorist Activities Related to Construction Sites

### What Should I Consider Suspicious?

- Removal or altering of survey stakes on a construction site.
- Anyone inquiring about security at a construction area.
- Surveillance of the site by unknown individuals.
- Environmental and/or antigovernment slogans, banners, or signs at the site or in the nearby area that threaten or imply violence.
- Group identifiers or warning signs left on the site.
- People entering a construction site after work hours.
- Warnings or threats sent to construction companies.
- Unscheduled deliveries of materials/equipment.
- Items found on-site that do not belong or are not a part of the site materials.
- Vandalism at similar sites.
- Thefts of hazardous materials.
- Evidence of intentional damage to cables, gas lines, and power lines.
- Vandalism at the site, including window breakage, slashed tires, spray-painting, sand/sugar in fuel tanks, cutting of fuel and brake lines, and/or glued locks.
- Arson at buildings under construction, work sheds, or any kind of equipment, including trucks, bulldozers, and cranes.
- Following a crime on-site, the discovery of discarded clothing, shoes/boots, tools, or spray-paint cans along roads and paths near the site.

*It is important to remember that just because someone's speech, actions, beliefs, appearance, or way of life is different, it does not mean that he or she is suspicious.*

**To Report a Suspicious Purchase or Activity**  
**Email: [tripwire@chicagopolice.org](mailto:tripwire@chicagopolice.org)**

**In Emergency DIAL 911 and indicate  
"Tripwire Program" incident**

### What Should I Do?

**Maintain your construction sites.**

- ✓ Secure potentially dangerous or hazardous products.
- ✓ Clean the site regularly.
- ✓ Watch for people and actions that are out of place.
- ✓ Know what material and equipment should be on-site.
- ✓ Know what subcontractors and workers should be on-site.
- ✓ Do not leave the site unattended for long periods.
- ✓ Require all subcontractors to be licensed and insured.

**If something seems wrong, notify law enforcement authorities.**

**Do not jeopardize your safety or the safety of others.**

Preventing terrorism is a community effort. By learning what to look for, **you** can make a positive contribution in the fight against terrorism. The **partnership between the community and law enforcement** is essential to the success of anti-terrorism efforts.

Some of the activities, taken individually, could be innocent and must be examined by law enforcement professionals in a larger context to determine whether there is a basis to investigate. The activities outlined on this handout are by no means all-inclusive but have been compiled from a review of terrorist events over several years.





# Communities Against Terrorism Potential Indicators of Terrorist Activities Related to Wholesale Distributors- Beauty/Drug

## What Should I Consider Suspicious?

## What Should I Do?

### Suspicious People Who:

- Have burn marks on customer's hands, arms, or face
- Are Missing hand / fingers, bright colored stains on clothing, strange odors
- Significantly alters appearance from visit to visit (shaving beard, changing hair color, style of dress, etc)
- Only chemicals and no other beauty supplies purchased
- Customer does not work at or own a salon
- Preoccupation with the concentration levels of Hydrogen Peroxide or Acetone
- Asks about boiling or making liquid more concentrated
- Comments involving radical theology, vague or cryptic warnings, anti-U.S. sentiments
- Travels illogical distance to store, uses lookout or is picked-up
- Nervous/suspicious behavior, evasive or vague about intended use of products

### Purchase Activities Include:

- Requests for large quantities of Hydrogen Peroxide or Acetone
- Numerous smaller purchases of Hydrogen Peroxide or Acetone (consumer-grade HP is 3-6%)
- Requests for higher concentrations or information on how to do that themselves
- Quantity desired inconsistent with use; illogical explanation for supplies
- Purchase of storage containers (glass jars or plastic buckets), mixing utensils, and/or rubber gloves, in conjunction with Hydrogen Peroxide/Acetone

*It is important to remember that just because someone's speech, actions, beliefs, appearance, or way of life is different; it does not mean that he or she is suspicious.*

**To Report a Suspicious Purchase or Activity**

**Email: [tripwire@chicagopolice.org](mailto:tripwire@chicagopolice.org)**

**In Emergency DIAL 911 and indicate  
"Tripwire Program" incident**

### Be part of the solution.

- ✓ Require valid ID from all new customers.
- ✓ Keep records of purchases.
- ✓ Talk to customers, ask questions, and listen to and observe their responses.
- ✓ Make note of suspicious statements, people, and/or vehicles.
- ✓ **If something seems wrong, notify law enforcement authorities.**

**Do not jeopardize your safety or the safety of others.**

Preventing terrorism is a community effort. By learning what to look for, you can make a positive contribution in the fight against terrorism. **The partnership between the community and law enforcement is essential to the success of anti-terrorism efforts.**

Some of the activities, taken individually, could be innocent and must be examined by law enforcement professionals in a larger context to determine whether there is a basis to investigate. The activities outlined on this handout are by no means all-inclusive but have been compiled from a review of terrorist events over several years.



# **EXHIBIT 10**

# CHICAGO POLICE DEPARTMENT

## 2008 ANNUAL REPORT

---

### A YEAR IN REVIEW

CITY OF CHICAGO  
RICHARD M. DALEY  
MAYOR

CHICAGO POLICE DEPARTMENT  
1000 N. LAKE ST.  
CHICAGO, IL 60607  
312.437.3000

## Chicago Police Crack Down on Metal Theft

Metal theft was a growing crime problem in 2008. Fueled by rising metal prices, thieves have been stealing aluminum and copper, and then selling the metal to recycling facilities for cash. In many of these crimes, thieves have targeted public utilities, costing utility companies thousands of dollars, cutting off services, and creating safety hazards. Targets have



included telecommunications cables, copper ground conductors on power transformers, switching signals on train tracks, and gas meters from outside homes.

In response to the problem, the Department participated in a multi-agency anti-metal theft task force. Participants included Alderman Danny Solis (25<sup>th</sup> Ward), the Chicago Department of Environment, the Cook County State's Attorney's Office, Crime

Stoppers, AT&T, ComEd, and Peoples Gas. By November, the task force had launched a public awareness campaign, and worked to establish Chicago Municipal Code 11-4-2625. This new ordinance restricts recycling facilities from receiving certain materials, including utility equipment. The statute also requires recycling facilities to keep records of transactions involving metal sales.

## Crime Prevention Information Center (CPIC) Continues to Advance

In April 2007, the Department's Crime Prevention Information Center (CPIC) became operational. The unique feature of the CPIC is that it addresses both violent crime prevention and homeland security issues. The CPIC serves as an intelligence hub, bringing together a large number of data sources in one location. CPIC staff work around the clock to monitor and mine these sources. Through these efforts, staff provide real time violent crime detection, continual assessment of available resources, enhanced field support, instantaneous major incident



identification, and identification of possible retaliatory gang violence. In 2008, the CPIC continued to expand its capabilities in these areas.



Information-sharing and inter-agency partnerships are keys to the success of the CPIC. Numerous law enforcement agencies commit knowledge and resources to the CPIC. CPIC staff continue to work with federal agencies to sharpen the Department's ability to address foreign threats to domestic security.

# **EXHIBIT 11**



## **CRIME PREVENTION AND INFORMATION CENTER (CPIC)**

### **ROLE OF FUSION CENTERS**

State and regional fusion centers enable local, state, and Tribal governments to gather, process, analyze, and share information and intelligence relating to all crimes and all hazards. Fusion centers communicate, cooperate, and coordinate with each other and with the federal government

#### **These centers:**

- Contribute information to ongoing federal and national-level terrorist risk assessments and complete statewide, regional, or site specific and topical risk assessments.
- Disseminate federally generated alerts, warnings, and notifications regarding time sensitive threats, situational awareness reports, and analytical products.
- Gather, process, analyze, and disseminate locally generated information, such as Suspicious Activity Reports.
- Produce or interpret intelligence products relevant to stakeholders.
- Protect civil liberties and privacy interests of American citizens throughout the intelligence process.

### **FUSION CENTERS IN ACTION**

#### **CRIME PREVENTION AND INFORMATION CENTER (CPIC)**

Located in Chicago Police Department Headquarters is the Crime Prevention and Information Center (CPIC). CPIC is a joint DHS and CPD venture that utilizes multiple federal, state, local, and county law enforcement resources and the latest technologies, primarily in violent crime reduction and terrorist threat assessment and, secondarily, serving as an Incident Intelligence Center in the event of a major crime/non-criminal incident or natural disaster. Encompassing both crime prevention and homeland security measures, the CPIC is able to engage in real-time monitoring of criminal activity and provides resources to assist in investigations. This comprehensive all-crimes approach allows for greater cooperation among agencies that engenders lasting partnerships.

## **CRIME PREVENTION AND INFORMATION CENTER (CPIC)**

### **WHAT IS A FUSION CENTER?**

A fusion center is a collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity. Intelligence processes-through which information is collected, integrated, evaluated, analyzed, and disseminates-are a primary focus.

Data fusion involves the exchange of information from different sources-including law enforcement, public safety, and the private sector. Relevant and actionable intelligence results from analysis and data fusion. The fusion process helps agencies be proactive and protect communities.

### **NATIONAL SUPPORT FOR FUSION CENTERS**

In 2006, the President approved the establishment of a national integrated network of state and major urban area information fusion centers. The U.S. Department of Homeland Security (DHS) and the FBI have begun deploying personnel to work within the fusion centers.

### **ALL 50 STATES HAVE FUSION CENTERS**

Recognizing the critical importance of information sharing, all 50 states have created fusion centers with various federal, state, and local funds (several major urban areas also have fusion centers). Currently, there are a total of 72 fusion centers in the U.S.

### **FUSION CENTER GUIDELINES**

The Fusion Center Guidelines were developed to ensure that fusion centers are established and operated consistently, resulting in enhanced coordination, strengthened partnerships, and improved crime-fighting and anti-terrorism capabilities.

(over)