



February 8, 2007

Kevin M. Burke
Secretary of Public Safety
Executive Office of Public Safety
One Ashburton Place
Boston, MA 02108

Re: **Public Records Request: Fusion Center**

Dear Secretary Burke,

Following Governor Romney's announcement of the formal establishment of the Fusion Center in May 2005, the American Civil Liberties Union of Massachusetts wrote to Secretary Flynn to express its concerns about proposed scope of the Center's work and requested certain public records concerning the planning for, and the establishment and funding of the Center. We were provided with some basic information about the Center, and we subsequently met with senior officials of Executive Office of Public Safety to discuss our concerns. In the intervening period, information has become available suggesting that there is reason to be concerned by the extent of the intelligence gathering activities of the Center. For this reason, we are writing to request certain additional records related to the operation and oversight of the Center.

At the outset, the principal justification for state fusion centers was to facilitate the sharing of anti-terrorist information between local, state and national criminal justice agencies. Incidental to this purpose, it was explained that there would be some coordination with the private sector and that the fusion centers could also serve other law enforcement purposes. Nevertheless, the Executive Office of Public Safety has consistently emphasized that the Fusion Center is a non-threatening means of coordination between law enforcement agencies, both federal and state. In 2005, State Police Major Robert Smith promised that the Fusion Center is "not a system that we're putting into place to spy on people."¹ Rather, the Fusion Center was to be an intelligence resource which would do no more than "analyze[] criminal information already collected in the ordinary course of police business."² We were given similar assurances when we met with senior officials of EOPS in late 2005 to express our concerns about the extent of the information being collected, and we were advised that procedures would be put in place to protect individual privacy and to prevent overreaching by the Fusion Center.

1. Stephanie Ebbert, *Fusion Center Takes Aim at Terror*, BOSTON GLOBE A1 (Sep. 26, 2005).

2. Edward Flynn, Letter to the Editor, *In Defense of Mass. Fusion Center*, BOSTON GLOBE A10 (Jun. 20, 2005).

Based on the information which is now publicly available, however, it is apparent that the anticipated intelligence gathering capacity of the Center is far more substantial than we had been led to believe, and that large amounts of information about individuals, information which was previously available only in myriad unconnected records and databases, will be readily accessible through the Center. Of equal concern to us is the fact that this information will be melded into what has aptly been described as a seamless national intelligence network in which information collected in Massachusetts can easily be shared with law enforcement and intelligence agencies across the country.

Access to Government Records Systems

Our first concern is the aggregation of government information systems, records and databases. The public documents provided by your office included federal and state materials which demonstrate the sweep of information now flowing into the Fusion Center. The U.S. Department of Homeland Security [DHS]'s *Intelligence and Information Sharing Initiative* whitepaper notes that "[e]ffective intelligence/information fusion" requires, among other things, the ability to "extract information" from state databases operated by "public health entities, emergency rooms . . . transportation entities, housing inspectors, health inspectors, building code inspectors, etc."³ Similarly, the DHS *Fusion Center Guidelines* which were included in your response recommend that the Fusion Center "consider obtaining access to a variety of databases and systems, such as driver's license, motor vehicle registration" and other systems.⁴

The materials included in your response also indicate that the Fusion Center will "consider hard copy paper reports as a data source," and has apparently begun scanning paper records into its databases – in the Fusion Center budget for fiscal years 2004 and 2005, \$477,352 was allocated for the conversion of paper records to electronic form. You will appreciate our concern over paper records, given reports that Fusion Center analysts "pore over" large volumes of "field reports filed by street cops, state troopers, and federal agents."⁵

We therefore request access to the following public records:

1. Records identifying all government information systems, databases and records accessible by the Fusion Center including:
 - a. The name of any state agency providing access to information to the Fusion Center and the nature of the records or systems of records which can be accessed by the Center;

3. U.S. DEPT. OF HOMELAND SECURITY, INTELLIGENCE AND INFORMATION SHARING INITIATIVE: HOMELAND SECURITY INTELLIGENCE & INFORMATION FUSION 4, 4 n.2 (Apr. 28, 2005) (available at http://www.dhs.gov/xlibrary/assets/HSAC_HSIntelInfoFusion_Apr05.pdf).

4. U.S. DEPT. OF JUSTICE, FUSION CENTER GUIDELINES 41 (2005) (available at http://it.ojp.gov/documents/fusion_center_guidelines.pdf).

5. Stephen Kurkjian, Kevin Kullen & Thomas Farragher, *Despite Millions Spent, Boston Is Vulnerable*, BOSTON GLOBE A1 (Sep. 10, 2006).

- b. The name of each city and town which is providing access to information to the Fusion Center and the nature of the records or systems of records which can be accessed by the Center; and
 - c. All federal government information systems which are accessible to the Center.
- 2. Records concerning the authority for disclosure to the Center of information or records held by any state agency;
- 3. Any formal agreement between the Fusion Center and/or the Department of State Police and any state or local government agency providing for access to information or records held or maintained by that agency; and
- 4. A description of all paper records which have been or will be converted to electronic form.

Access to Private Sector Records

In addition to accessing law enforcement and other government records, it appears from the information provided to us that Center will seek access to various private sector records, including hospital records and that it anticipates using consumer data aggregators such as Choicepoint and LEXIS which sell intimate personal details such as voting records, court filings, and the names of relatives and friends.⁶ Request For Proposal (RFP) SP04-I97, which solicited bids to provide the Fusion Center with its "intelligence management system" software, specifies that any winning system would need to be able to provide "a single interface" for querying "public information services" such as Choicepoint. The State Police Counter-Terrorism Unit operational budget for fiscal year 2005 confirms that \$168,000 was spent on "subscription costs for certain personal record information services."

Accordingly, we request the following records:

- 5. Records identifying each private sector entity providing the Fusion Center with access to records or information and the nature of the records or information which can be accessed by the Center;

6. For instance, ChoicePoint boasts that one of its product offerings:

provides Internet access to more than 17 billion current and historical records on individuals and businesses, and allows users to browse through those records instantly. With as little information as a name or Social Security number, users can cross-reference public and proprietary records including identity verification information, relatives and associates, corporate information, real property records, deed transfers and much more.

ChoicePoint, *AutoTrackXP*, http://choicepoint.com/industry/government/public_le_1.html (accessed Jan. 17, 2007).

6. Any formal agreement between the Fusion Center and/or the Department of State Police and any private sector entity providing for access to information or records held or maintained by that entity; and
7. Any records describing or concerning the use by the Center and/or the Department of State Police of the services of commercial data aggregators.

Other Sources of Intelligence

It also appears that the intelligence sources available to the Fusion Center are not limited to access to records and will include information about Massachusetts citizens' everyday movements. The *State Homeland Security Strategy* states that "it will be a priority for the Commonwealth to establish linkages between the Fusion Center and various Operational Control Centers operated by the Massachusetts Highway Department, MassPort, MBTA, the Massachusetts Turnpike Authority, and the Boston Transportation Department."⁷ And subsequent to the publication of the Strategy, the MBTA secured federal funding to blanket its system in surveillance cameras which have the capacity to capture and preserve high-resolution digital images of T passengers.⁸

We also note that the *Intelligence and Information Sharing Initiative* calls for the establishment and operation of a "toll-free tip line" into the Fusion Center,⁹ and that the line has been in operation at least since 2005 when Governor Romney called on meter readers, cable television technicians, and the like to use the tip line to report their observations of the people of Massachusetts.¹⁰

8. Records describing or listing the nature of the linkages between the Center and the Operational Control Centers operated by the Massachusetts Highway Department, MassPort, MBTA, the Massachusetts Turnpike Authority, the Boston Transportation Department and the Boston Police Department, and whether the information obtained from those agencies is retained in retrievable form by the Center; and

7. MASS. OFFICE OF DOMESTIC PREPAREDNESS, STATE HOMELAND SECURITY STRATEGY 6 n.5 (2004) (available at <http://www.mass.gov/Eeops/docs/programs/hs/StateHomelandSecStrategy.pdf>).

8. See, e.g. Emma Fitzsimmons, *All T Stops Will Have Security Cameras*, BOSTON GLOBE B2 (Aug. 11, 2006) (noting award of \$3m grant to be spent on 200 new cameras, images of which "will be monitored from the MBTA Operations Control Center, the Transit Police Department, and the Massachusetts Emergency Management Agency's bunker in Framingham"), Mac Daniel, *Some New T Buses to Feature Cameras*, BOSTON GLOBE B2 (Aug. 18, 2006) (reporting that the new fleet of buses are wired for no fewer than "six cameras, one facing out the front of the bus, one watching the side, and four on board. The cameras, which can save 72 hours of recorded material . . . can transmit their images in real time to a portable receiver up to 400 feet away"), Bryan Bender and Mac Daniel, *T to Receive \$15m Security Grant*, BOSTON GLOBE B2 (Jan. 10, 2007) (reporting that "[t]he grant will also allow the Massachusetts Bay Transportation Authority to improve security on buses, which could include adding surveillance cameras, something the T is doing on its new buses").

9. INTELLIGENCE AND INFORMATION SHARING INITIATIVE, *supra* note 3 at 6.

10. Scott Helman, *Wiretap Mosques, Romney Suggests*, BOSTON GLOBE A1 (Sep. 15, 2005).

9. Records describing (a) the procedures used by the Center in responding to or acting on information received on the tip line, and (b) the number of calls received on the tip line in 2005 and 2006.

Disclosure of Information

We are also concerned about the security provided for the massive amounts of personal information accessible to and generated by the Center. Consistent with the purpose of the Center, it is expected to analyze and bring together – or fuse – the vast array of information available to it and to produce intelligence reports which will be available to in some measure to federal, state and local law enforcement authorities and to providers of private security. Both the materials enclosed in your preliminary response and the public comments of state officials¹¹ make it clear that the Fusion Center is supplying information about Massachusetts residents to municipal law enforcement agencies and various agencies of state government. The *State Homeland Security Strategy*, meanwhile, establishes that the Fusion Center's top priority is to "ensure the effective flow of information among federal . . . and private sector entities" in addition to municipal and state agencies.¹²

As such, we request the following records:

10. Records identifying all government agencies, whether federal, state, or municipal, which receive information from the Fusion Center, including:
 - a. The name of any federal agency accessing, or otherwise receiving, information held or generated by the Fusion Center, and the nature of the information which the Fusion Center is disseminating;
 - b. The name of any state agency accessing, or otherwise receiving, information held or generated by the Fusion Center, and the nature of the information which the Fusion Center is disseminating; and
 - c. The name of each city and town accessing, or otherwise receiving, information held or generated by the Fusion Center, and the nature of the information which the Fusion Center is disseminating.
11. Any written agreements between the Fusion Center and any federal, state, or municipal agency providing for access to, or receipt of, information from the Fusion Center in any form.

11. See, e.g. Tom Farmer, *Terrorism Intelligence Center Will Connect Local Cops to Feds*, BOSTON HERALD 16 (Sep. 23, 2004) (reporting State Police Col. Thomas G. Robbins's assertion that "[o]ur purpose is to gather information at the local level and disseminate it at the local level").

12. STATE HOMELAND SECURITY STRATEGY, *supra* note 7 at 4.

12. Records identifying any non-governmental entity accessing, or in any way receiving, any information from the Fusion Center, including the name of all private entities accessing, or in any way receiving, information held by the Fusion Center, and the nature of the information which the Fusion Center is disseminating thereto.
13. Any written agreements between the Fusion Center and any non-governmental entity providing for access to, or receipt of, information from the Fusion Center in any form.
14. Records describing or containing any policies and procedures establishing minimum standards for intelligence analysis products generated by the Center.

Protection of Privacy and Civil Liberties

Given the expansion of the Center's surveillance capacity and the frequency with which government data repositories suffer from unconstitutional abuse,¹³ wholesale information theft,¹⁴ and improper employee 'browsing,'¹⁵ the adoption of safeguards to protect privacy and civil liberties is of paramount importance. Indeed, such protections have been identified a critical element of intelligence fusion. The *Fusion Center Guidelines* recommend that the Fusion Center establish a privacy oversight committee or appoint a privacy officer, as "[a]ccountability is essential" to protecting constitutional and privacy rights,¹⁶ and also counsel the Center to "[d]evelop, publish, and adhere to a privacy and civil rights policy."¹⁷ Other relevant federal standards mandate background checks for employees¹⁸ and a document retention policy based upon need (rather than an open-ended quest to stockpile information).¹⁹ Moreover, the *Guidelines* dictate that the Fusion Center implement policies which permit individuals "to be able to determine if there is information about them" in the Center's databases,²⁰ and state that "all levels of law enforcement should be educated on constitutional rights, privacy issues, and

13. For example, news reports suggest that fusion centers across the country were involved in investigating information eavesdropped as part of President Bush's illegal warrantless wiretapping scheme. See Walter Pincus, *NSA Gave Other U.S. Agencies Information From Surveillance*, WASH. POST A8 (Jan. 1, 2006) (reporting that information obtained was "passed on to other government agencies, which cross-check[ed] ... with tips and information collected in other databases").
14. See, e.g. *Size of Military Data Theft Grows to Affect Millions of Troops*, N.Y. TIMES A20 (Jun. 7, 2006) (reporting that "[p]ersonal information stolen from the home of a Veterans Affairs employee included data on 2.2 million active-duty members of the military").
15. See, e.g. Sean P. Murphy, *Worker Charged with ID Theft*, BOSTON GLOBE B3 (Feb. 2, 2007) (reporting that a "subcontractor to a subcontractor to a contractor" working for the state's Department of Industrial Accidents perused the Department's records and eventually used the results of her browsing to commit identity theft), *IRS Systems and Security: Employee Browsing Not Being Addressed Effectively and Budget Requests for New Systems Development Not Justified, Hearing Before the Senate Subcomm. On Treasury and Gen. G't, Comm. On Appropriations*, 105th Cong. 1 (1997) (statement of Dr. Rona B. Stillman, IRS) (noting that the Internal Revenue Service suffers from "serious and persistent computer security and employee browsing problems").
16. FUSION CENTER GUIDELINES, *supra* note 4 at 51.
17. *Id.* at 49.
18. U.S. DEPT. OF HOMELAND SECURITY, NATIONAL CRIMINAL INTELLIGENCE SHARING PLAN 24-25 (2003) (available at http://www.it.ojp.gov/documents/National_Criminal_Intelligence_Sharing_Plan.pdf).
19. U.S. DEPT. OF JUSTICE, PRIVACY POLICY DEVELOPMENT GUIDE AND IMPLEMENTATION TEMPLATES § 7.2.4.1.5 (2006) (available at http://it.ojp.gov/documents/Privacy_Guide_Final.pdf).
20. *Id.* at § 7.2.4.1.4.

safeguards as they relate to the criminal intelligence function.”²¹ Finally, the *National Criminal Intelligence Sharing Plan* recommends that criminal intelligence systems such as the Fusion Center adopt the model case file standards published by the Law Enforcement Intelligence Unit (LEIU), which state that that law enforcement specifically avoid collecting or storing “information on an individual or group merely on the basis that such individual or group supports unpopular causes.”²²

A number of the applicable privacy and civil liberties standards are not optional. The budgetary materials included in your preliminary response indicate that the Fusion Center utilized at least \$6.3 million in federal funding during fiscal year 2005. 42 U.S.C. § 3789g(c) prohibits federally-funded criminal intelligence systems like the Fusion Center from being “utilized in violation of the privacy and constitutional rights of individuals.” As such, 28 C.F.R. § 23.20 et seq., which mandates minimum privacy standards in the use of criminal intelligence systems, requires that the official in charge of the Fusion Center certify in writing that s/he “takes full responsibility and will be accountable for insuring that the information transmitted to the interjurisdictional system or to participating agencies will be in compliance with” all of these minimum standards.²³

It remains unclear, however, that the ‘necessary steps have been taken to ensure compliance with these standards. To be sure, the Center’s website states that it “aspires to the principles and recommendations set forth in the National Criminal Intelligence Sharing Plan and Fusion Center Guidelines.”²⁴ However, we have been unable to confirm that a privacy policy has been adopted by the Center or that any other measures had been taken to ensure that the Center would operate lawfully and with due regard for privacy concerns. When we met with EOPS in late 2005, we were advised that privacy safeguards were still in the process of development notwithstanding the fact that the Center had then been in operation for nearly half a year and that the advisory committee on privacy had “not yet been appointed.”²⁵

Accordingly, we hereby request that you furnish records concerning:

15. Fusion Center budget information for fiscal years 2006 and 2007, including identification of any federal funds received or applied for;
16. Certification of compliance with 28 C.F.R. § 23.20;
17. Any Fusion Center policies and/or procedures governing the protection of privacy, confidentiality, or the constitutional rights of Massachusetts citizens, including procedures for the screening, training and supervision of employees and the use of

21. NATIONAL CRIMINAL INTELLIGENCE SHARING PLAN, *supra* note 18 at 15.

22. LAW ENFORCEMENT INTELLIGENCE UNIT, CRIMINAL INTELLIGENCE FILE GUIDELINES 1 (2002) (available at http://it.ojp.gov/process_links.jsp?link_id=3773).

23. 28 C.F.R. § 23.30 (d)(2).

24. Mass. Executive Office of Public Safety, *Fusion Center Overview*, http://www.mass.gov/?pageID=eopsterminal&L=3&L0=Home&L1=Homeland+Security+%26+Emergency+Response&L2=Commonwealth+Fusion+Center&sid=Eeops&b=terminalcontent&f=msp_homeland_security_terrorism_fusion_center_fusion_center_overview&csid=Eeops (accessed Jan. 10, 2007).

25. Ebbert, *supra* note 1.

any software audit trail capabilities, such as the one provided by the Fusion Center's intelligence management system, COPLINK;²⁶

18. Policies and procedures providing for a privacy oversight board or officer, including procedures for auditing and disciplining Fusion Center employees;
19. The identity of the Center's privacy officer and of all members of the privacy oversight board or committee;
20. Policies and procedures governing the establishment and maintenance of case files, including any procedures or practices to prevent the scrutiny of persons or groups solely on the basis of espousing an unpopular viewpoint;
21. Policies and procedures governing records retention and access by the public to records held by the Fusion Center, including any Fusion Center policies on permitting members of the public to view, contest, or correct information about them.

We appreciate that a request of this nature will cover a number of potentially duplicative records. As our purpose in making this request is to obtain the information contained in these records, we would be willing to discuss a narrowing of the request in the event that seems to be appropriate. If you have any questions about this request, including ways of narrowing it, please contact me at 617-482-3170, ext. 324.

Because this request involves a matter of public concern and because it is made on behalf of a nonprofit organization, we ask that you waive any copying costs pursuant to 950 CMR § 32.06(5). Alternatively, we ask that you permit us to examine the requested records and, at our election, to obtain copies of specified records.

Should you determine that some portion of the documents requested are exempt from disclosure, please release any reasonably segregable portions that are not exempt. In addition, please note the applicable statutory exemption and explain why it applies to the redacted portions. As you know, a custodian of public records shall comply with a request within ten days after receipt.

Once we have reviewed these records, we would welcome the opportunity to meet with you and your staff to discuss the issues which have prompted our concern.

Sincerely yours,

John Reinstein
Legal Director

26. According to press accounts, Raytheon Systems, the supplier of the fusion center's intelligence management system, has subcontracted with the Knowledge Computing Corporation to provide its COPLINK analytical software to the fusion center. *Business Briefs*, TELEGRAM & GAZETTE (WORCESTER, MASS.) E1 (May 25, 2005). Along with its ability to "discover hidden relationships among people," COPLINK permits Fusion Center supervisors to audit each search performed by COPLINK to ensure that Fusion Center employees are not improperly browsing records or stalking members of the public. KNOWLEDGE COMPUTING CORP., COPLINK: WHITEPAPER 1 (Oct. 2006) (available at <http://www.coplink.net/downloads/COPLINK%20Whitepaper09061.pdf>).