



# The Information Society Project

December 15, 2010

Mary Ellen Callahan  
Chief Privacy Officer  
Privacy Office  
Department of Homeland Security  
Washington, DC 20528

Dear Ms. Callahan:

The Media Freedom and Information Access Practicum (MFIA), a joint initiative of the Knight Law & Media Program and the Information Society Project at Yale Law School, writes to you today to comment on the Department of Homeland Security Office of Operations Coordination and Planning—003 Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion System of Records, docket number DHS-2010-0052, FR Doc 2010-28566, published in the *Federal Register* on November 15, 2010 at 75 FR 69689-93. We greatly appreciate your willingness to listen and your commitment to collaboration.

Our comments make two points. First, we argue that there is insufficient public information available on fusion centers for the public to adequately evaluate the effect of the proposed information collection system, 003 Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion System of Records (hereinafter Fusion System). Second, we express concerns about the expense, mission creep, and privacy effects of the proposed database.

**I) It Is Difficult for the Public To Comment on the Merits of the Request for Notice and Comment Because So Little Information is Available on Fusion Centers**

The public lacks sufficient information on the existing operation of fusion centers. Without more details on fusion center operations – including mechanisms for data collection – citizens simply cannot assess how the proposed Fusion System will affect their privacy. Furthermore, the government has thwarted efforts to obtain such information through the channels provided by the Freedom of Information Act. Government operations consistent with the Privacy Act would enable “meaningful” transparency – allowing individuals to be aware of what personal information is gathered in fusion center databases, and thus to meaningfully determine how the proposed new system will affect their privacy.

***A) Publicly Available Information on Fusion Centers is Insufficient for the Public To Adequately Comment on the Proposed Rule***

State and local fusion centers are designed “to share information and intelligence within their jurisdictions as well as with the federal government.”<sup>1</sup> However, the public lacks sufficient information on the data collection procedures to determine how the proposed database on which the agency seeks comment will affect their privacy.

*Available Information*

Public information currently available on fusion centers lacks the specificity to enable the public to evaluate its rights under the Privacy Act. The government has made available general information about fusion centers, including through its website, press releases, speeches, and Congressional testimony.<sup>2</sup> This information is outdated; the website has not been updated nor have press releases been added since September 2009.

Further, in Congressional testimony the government has referenced other important Fusion Center documents, such as the internal Fusion Center Implementation Plan of 2006, and a capability appendix to the U.S. Department of Justice’s Global Justice Information Sharing Initiative’s (Global) Baseline Capabilities for State and Major Urban Area Fusion Centers (Baseline Capabilities Document), do not appear to be publicly available.<sup>3</sup> Other documents available online about Fusion Centers, including Fusion Center Guidelines,<sup>4</sup> a Privacy Impact Assessment (PIA),<sup>5</sup> a Civil Liberties Impact Assessment (CLIA),<sup>6</sup> and the Baseline Capabilities Document,<sup>7</sup> are not clearly linked

---

<sup>1</sup> Department of Justice, State and Local Fusion Centers, [http://www.dhs.gov/files/programs/gc\\_1156877184684.shtm](http://www.dhs.gov/files/programs/gc_1156877184684.shtm).

<sup>2</sup> See, e.g., Department of Justice, State and Local Fusion Centers, [http://www.dhs.gov/files/programs/gc\\_1156877184684.shtm](http://www.dhs.gov/files/programs/gc_1156877184684.shtm); Office of the Press Secretary, Department of Homeland Security, Press Release, DHS Announces New Information-Sharing Tool to Help Fusion Centers Combat Terrorism, Sept. 14, 2009, [http://www.dhs.gov/ynews/releases/pr\\_1252955298184.shtm](http://www.dhs.gov/ynews/releases/pr_1252955298184.shtm); Department of Homeland Security, Remarks by Homeland Security Secretary Janet Napolitano to the National Fusion Center Conference in Kansas City, Mo. on March 11, 2009, Mar. 13, 2009, [http://www.dhs.gov/ynews/speeches/sp\\_1236975404263.shtm](http://www.dhs.gov/ynews/speeches/sp_1236975404263.shtm).

<sup>3</sup> The Future of Fusion Centers: Potential Promise and Dangers: Hearing Before the Com. on Homeland Sec’y, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, Apr. 1, 2009 (statement of Director Robert Rieggle, State and Local Program Office, Office of Intelligence and Analysis) [hereinafter Rieggle statement].

<sup>4</sup> Department of Justice, Bureau of Justice Assistance, Office of Justice Programs, Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era, available at [http://it.ojp.gov/documents/fusion\\_center\\_guidelines\\_law\\_enforcement.pdf](http://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf) [hereinafter Fusion Center Guidelines].

<sup>5</sup> Department of Homeland Security, Privacy Impact Assessment for the Department of Homeland Security State, Local, and Regional Fusion Center Initiative, Dec. 11, 2008, available at [http://www.dhs.gov/xlibrary/assets/privacy/privacy\\_pia\\_ia\\_slrfci.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ia_slrfci.pdf) [hereinafter Privacy Impact Statement].

<sup>6</sup> Department of Homeland Security, Civil Liberties Impact Assessment for the State, Local, and Regional Fusion Center Initiative, available at [http://www.dhs.gov/xlibrary/assets/crcl\\_civil\\_liberties\\_impact\\_assessment\\_12\\_11\\_08.pdf](http://www.dhs.gov/xlibrary/assets/crcl_civil_liberties_impact_assessment_12_11_08.pdf).

<sup>7</sup> Department of Justice, Global Justice Information Sharing Initiative, Baseline Capabilities for

from the Fusion Center website, making it difficult for the public to recognize that such information is available.

A review of this information suggests it is insufficient in at least two ways:

- (a) It fails to allow the public to evaluate the degree to which its privacy is currently protected; and
- (b) It fails to allow the public to compare the proposed Fusion System with existing mechanisms for collecting information.

### *Relationship to Privacy*

There is limited information available about fusion centers' approaches to privacy. While the federal government has provided guidance to state and local centers on how to secure information, provide privacy outreach, and to develop more detailed privacy policies,<sup>8</sup> the information available on individual fusion center approaches – and the degree to which states have successfully implemented these privacy guidelines – remains unclear. Many state fusion centers do not even have websites. Further, while we commend those states which have developed fusion center privacy policies, the public needs reassurance that these are being implemented and enforced. Given the veil of secrecy surrounding fusion centers, and the attendant lack of information, public evaluation of the implementation of privacy policies is particularly necessary.

The Privacy Impact Assessment suggests that fusion centers could take a number of steps to enhance privacy. Congressional testimony summarizes these steps as follows:

The PIA made a number of specific recommendations that fusion centers can implement to enhance privacy. These include completing their written Information Sharing Environment privacy protection policies, and creating governance structures and procedures to protect privacy and to understand and implement the set of privacy protections called the Fair Information Practice Principles (FIPPs). These include protections related to data integrity, use limitation, data minimization, and others. Perhaps the most important recommendation in the PIA furthered the transparency principle; the DHS Privacy Office recommends that each fusion center conduct a PIA evaluating its own operations, make it available to the public, and then engage with its local communities.<sup>9</sup>

Since the public does not know the degree to which these recommendations have been implemented, and whether privacy has been successfully enhanced both at the state/local and federal level, it is difficult for it to evaluate how the current proposal will affect privacy interests more broadly. Reports should be developed and released on each state's development and implementation of a privacy plan to help mitigate this problem.

### *Existing Mechanisms for Information Collection*

---

State and Major Urban Area Fusion Centers, A Supplement to the Fusion Center Guidelines, Sept. 2008, available at <http://www.it.ojp.gov/documents/baselinecapabilitiesa.pdf> [hereinafter Baseline Capabilities].

<sup>8</sup> *Id.* at 27-31.

<sup>9</sup> Riegle statement.

Any meaningful response to the agency's proposed Fusion System requires the public to evaluate the need for such a system *against the existing databases and other mechanisms for information collection already available to fusion centers*. Insufficient details are available on these existing mechanisms for information collection to enable the public to meaningfully evaluate the need for the new Fusion System.

From the available information on fusion centers, the public recognizes that there are existing mechanisms which perform the functions of the new Fusion System. For example, the government already has mechanisms to coordinate information between state and local levels:

The Homeland Security Data Network (HSDN), which allows the federal government to move information and intelligence to the states at the Secret level, is deployed at 27 fusion centers. Through HSDN, fusion center staff can access the National Counterterrorism Center (NCTC), a classified portal of the most current terrorism-related information.<sup>10</sup>

The government has a secure web portal for sharing information as well:

I&A launched the Homeland Security State and Local Community of Interest (HS SLIC) about one year ago. HS SLIC is a "virtual community" of intelligence analysts from Federal, State, and local entities. Intelligence analysts collaborate via weekly threat conference calls, biweekly secure video teleconferences, analytic conferences, and a secure Web portal for intelligence information sharing at the controlled unclassified information (CUI) level, via HS SLIC.<sup>11</sup>

Additionally, as the proposal for notice and comment makes clear, the government already has a record-keeping system which the new system is designed to replace:

Some of the records in this system are in part transferred from the Department of Homeland Security/Information Analysis and Infrastructure Protection—001 Homeland Security Operations Center Database system of records, April 15, 2005, with the overall intent of narrowing the focus of these records to the specific purpose outlined in this system of records notice. It is the Department's intent, after all records are transferred into this and other system of records, to retire the Department of Homeland Security/Information Analysis and Infrastructure Protection—001 Homeland Security Operations Center Database system of records.<sup>12</sup>

Finally, other documents make clear that there are other law enforcement entities, such as the National Surveillance Integration Center,<sup>13</sup> the Federal Bureau of Investigation's

---

<sup>10</sup> Department of Justice, State and Local Fusion Centers, [http://www.dhs.gov/files/programs/gc\\_1156877184684.shtm](http://www.dhs.gov/files/programs/gc_1156877184684.shtm).

<sup>11</sup> Riegle Testimony.

<sup>12</sup> 75 FR 69689.

<sup>13</sup> Department of Homeland Security, Remarks by Homeland Security Secretary Janet Napolitano to the National Fusion Center Conference in Kansas City, Mo. on March 11, 2009, March 13, 2009, [http://www.dhs.gov/ynews/speeches/sp\\_1236975404263.shtm](http://www.dhs.gov/ynews/speeches/sp_1236975404263.shtm).

Regional Data Exchange (R-Dex) and National Data Exchange (N-Dex), the National Crime Information Center, Regional Information Sharing Systems (RISS), Law Enforcement Online (LEO), and the Department of Homeland Security's (DHS) Homeland Security Information Network (HSIN),<sup>14</sup> which might be able to play the role suggested by the Fusion System.

The public lacks answers to crucial questions which would enable it to evaluate the effects of the proposed system on its Privacy Act rights. These include:

- How does the proposed Fusion System differ from these existing mechanisms of data collection?
- Why is it necessary to retire the Homeland Security Operations Center Database? Could the existing database be modified to meet the government's needs?
- What security measures are in place under the current data collection scheme to protect the privacy of individuals? How will these measures be different under the new system?
- Has the operation of fusion centers changed substantially since September 2009, since when the government has published little information on these entities?

***B) The Government Has Failed To Make Available Information Requested Under the Freedom of Information Act***

In an effort to expand public access to information on Fusion Centers, MFIA on October 29, 2009 filed numerous Freedom of Information Act requests to the Under Secretary Office of Intelligence & Analysis (OIA), the Under Secretary for Management, and the Under Secretary for Science & Technology, seeking information on access to information, budgeting, and databasing, both generally and with regard to Federal-Connecticut activities. The Under Secretary Office of Intelligence & Analysis (OIA) referred our requests to Connecticut agencies and to the Federal Emergency Management Agency. Despite our good faith efforts to clarify our requests and to make timely appeals of their decisions, no federal government agency produced a single document based on our request. While we have received some responsive records from the state of Connecticut, such information is not a substitute for transparency in federal dealings.

This response is particularly disturbing because the Department is currently under investigation for referring FOIA requests to the White House for political review. As the Electronic Privacy Information Center's recent letter to the FOIA ombudsman makes clear, this policy both thwarts the purpose of the Freedom of Information Act and inappropriately subjects FOIA requests to political scrutiny.<sup>15</sup> This provides further evidence that the government may not be releasing all information required under the Freedom of Information Act.

---

<sup>14</sup> Fusion Center Guidelines 13, 33.

<sup>15</sup> Letter from Nichole Rustin-Paschal, EPIC Open Gov't Fellow, to Miriam Nesbitt, Dir., Office of Gov't Info. Systems, Nat'l Archives and Record Admin., Dec. 8, 2010.

### ***C) Recommendations***

The above suggests that the Department of Homeland Security is failing to uphold its obligations under relevant law to make available sufficient information to evaluate the proposed Fusion System. The Department's decision to limit the comment period to 30 days (the shortest option available), though it overlapped with a federal holiday, further suggests a lack of interest in adequate information exchange with the public.

We recommend that the Department should make sufficient information available about current data collection methods employed by Fusion Centers before determining whether new information databases are required. Such information includes, but is not limited to:

- The various information collection systems currently available to fusion centers;
- The cost of such information systems, including as a percentage of state and federal fusion center budgets;
- The man hours required to develop such systems;
- The value added by the proposed Fusion System; and
- How individuals will be able to access information through the proposed Fusion System.

We also recommend that the government be responsive to FOIA requests, which would encourage transparency as appropriate, as well as satisfy the curiosity of the public.

## **II) The Proposed Fusion System Does Not Adequately Protect the Public's Privacy**

The recordkeeping procedures, as proposed for the Fusion System, may well suffer from overbreadth and lack of focus. The new system may impose significant costs on government, expand state fusion center missions, and risk privacy abuses. It also provides inadequate mechanisms for the public to access information on themselves and seek redress as necessary.

### ***A) The Proposed Fusion System Will Impose Significant Costs and Raise Serious Privacy Concerns***

Fusion centers, as described in available public sources, record and collect vast categories of records in a series of interconnected systems. These categories may cover a significant proportion of the population, and include personal details such as individuals' medical records, financial information, and law enforcement files. Not only does this arrangement prompt privacy concerns, but also raises questions about how precisely such vast and broad information may be used. An overly broad mission statement render the Fusion System especially prone to abuse, including the possibility of overspending, mission creep, and privacy abuses.

### ***Overspending***

In order to function effectively, fusion centers require vast resources. Because fusion centers have a much more expansive scope than other information databases, the amount of money needed for their creation and long-term maintenance is difficult to determine. Nonetheless, huge monetary investments and human expertise will be required to obtain the technology and infrastructure necessary for the proper development of these centers.

The proposed Fusion System may have the unintended and unfortunate effect of siphoning off finite resources that are better spent on projects that could contribute more effectively to enhancing public safety and national security, such as improving the networking capability between existing state and federal information systems. There is an already-existing network of similar databases detailed above, including the existing Department of Homeland Security/Information Analysis and Infrastructure Protection—001 Homeland Security Operations Center Database proposed to be retired. Given the current financial crisis and growing deficit, there should be a predisposition in favor of modifying existing databases rather than developing new ones.

### ***Mission Creep***

The expansive scope of the Fusion System’s mission also lends itself to mission creep. The request explicitly states that the fusion centers will function from an “all-threats and all-hazards” stance. This mission is much broader than the relatively narrow homeland security mission supported by the DHS State, Local, and Regional Fusion Center Initiative.<sup>16</sup> The Fusion System’s overly broad mission could push fusion centers to become unfocused and ineffective. Fusion centers could foreseeably encroach on functions currently handled by other agencies, and such an outcome raises additional issues of redundancy, overlap, and costly excess. Further, without sufficient safeguards, cognizance of possible civil rights and civil liberties violations may well decline given the strong incentives to use the proposed Fusion System for profiling individuals.

These risks are particularly acute given that management of fusion centers is in large part delegated to states. To help mitigate these risks, the Department should consider:

- Closer oversight of state fusion center goals and initiatives;
- Tight tailoring of fusion mission statements to limit the risk of mission creep; and
- Periodic public updates on how state fusion center goals are being achieved.

### ***Privacy Violations***

Most importantly, the proposed Fusion System guidelines seem to encourage wholesale information collection in a way which may threaten personal privacy. Indeed, the stated purpose of the Fusion System suggests the risk that the centers will become sweeping data mining operations that would function as mass surveillance systems. The DHS Privacy Office has acknowledged that data mining raises serious privacy concerns within

---

<sup>16</sup> “The “all crimes and/or all hazards” mission, though adopted by many fusion centers, is “substantially broader than the homeland security mission the Initiative supports.” Privacy Impact Statement at 2.

the public, yet continues to have little knowledge about fusion center data mining activities.<sup>17</sup>

Although the request maintains that “[m]uch of the data within this system does not pertain to an individual,” it admits that “some personal data is captured.” In addition, personal data, like most other information in the system, is typically stored electronically as free text and may be searched according to any word, phrase, or number. This suggests that the proposed system of recordkeeping will contain very detailed and easily searchable profiles of many individuals, without strict standards for determining whether such individuals are a concern to public safety or national security. Even though DHS claims that fusion centers should follow a data minimization principle – holding that personal data should be collected only when “directly relevant and necessary to accomplish specific lawful purpose(s) and only retain[ed] for as long as necessary to fulfill the specified purpose(s)” – this principle is implemented so that the type of personal data which may be collected is expansive.<sup>18</sup>

The DHS Privacy Office has acknowledged that the wide sharing of information that occurs in fusion centers raises the possibility that incorrect or incomplete information will have negative repercussions for individuals.<sup>19</sup> Nonetheless, there are few legal guarantees for the accuracy of the personal data or appropriateness of the information searches, and little to no judicial or legislative oversight of the centers as a whole. These outcomes are particularly disturbing given the recent criticism levied at the DHS Privacy Officer to take adequate steps to secure individual privacy.<sup>20</sup>

***B) Making Information on Fusion Centers Publicly Available Would Fit the Purpose of the Privacy Act by Allowing Individuals To Determine Whether Their Privacy Rights Are Being Adequately Protected***

Allowing the public access to information stored about them in the Fusion System is the best way to ensure full enforcement of the Privacy Act of 1974, codified as amended at 5 U.S.C. 552a (2006). The Act focuses on two basic policy objectives that are relevant here. First, the Act is broadly aimed at granting individuals increased rights of access to agency records maintained on themselves,<sup>21</sup> a policy goal that was motivated by the government’s increased use of electronic databases to store and retrieve massive amounts of personal data.<sup>22</sup> Second, the Act is intended to grant individuals the right to seek

---

<sup>17</sup> *Id.* at 28.

<sup>18</sup> *Id.* at 21-22.

<sup>19</sup> *Id.* at 29.

<sup>20</sup> Letter from Am. Ass’n of Univ. Professors, et al, to Bennie Thompson, Chair, U.S. House of Representatives, Comm. On Homeland Sec’y, and Peter King, Ranking Member, U.S. House of Representatives, Comm. On Homeland Sec’y, Oct. 23, 2009. available at [http://epic.org/security/DHS\\_CPO\\_Priv\\_Coal\\_Letter.pdf](http://epic.org/security/DHS_CPO_Priv_Coal_Letter.pdf).

<sup>21</sup> 5 U.S.C. 552a(d)(1).

<sup>22</sup> See Department of Justice, Overview of the Privacy Act at 4, available at <http://www.justice.gov/opcl/1974privacyact.pdf>.



amendment of agency records maintained on themselves upon a showing that the records are not accurate, relevant, timely, or complete.<sup>23</sup>

It is clear upon even the most cursory look at current fusion center information dissemination policy—and also from MFIA’s unsuccessful attempts to gain access to fusion center information—that individuals do not currently have any meaningful right of access to the relevant agency records that may contain information about themselves. Thus, the agency’s current access policies do not achieve the first basic policy objective of the Act.

Further, the more specific and practical goal of the Act—a greater ability for individuals to seek to amend personal information agencies hold—is frustrated by current policy. For individuals to manage their privacy, they require sufficient knowledge on what information the government has retained. Full enforcement of the Privacy Act would bring about meaningful transparency by allowing individuals to determine what personal information is gathered in local databases. The privacy of others and security interests can be adequately protected by narrowly tailoring this information to the individual requesting, and by redacting other names and identifying information as necessary.

### *C) Recommendations*

The Privacy Act recognizes that the collection and sharing of intelligence information in general, and of personal data about American residents in particular, needs to be carried out with the utmost care. However, the guidelines for the proposed Fusion System do not sufficiently take account of this consideration, and a lack of supervision in this regard can result in abuse and privacy violations. We recommend the following steps be taken to ensure that the proposed system meets the goals of the Privacy Act:

- The Department should not implement the Fusion System
- The Department should also make public basic information on state fusion center goals and budgets, so that individuals can assess the breadth of this potentially privacy-infringing framework of database collaboration and determine how the proposed Fusion System will affect information collection.
- Given the sensitivity of the data available in the proposed Fusion System, and the potentially widespread effects it may have on individuals whose information is contained in the System, the Department should not exempt this database from the access and amendment provisions of the Privacy Act.
  - Individuals should be able to request and receive what information is contained about them in the proposed Fusion System and other fusion center databases; such information should be redacted to protect privacy and security interests.
  - The government should provide an avenue for redress if individuals determine that information contained on them is inaccurate or if their Privacy Act rights have been breached.

---

<sup>23</sup> 5 U.S.C. 552a(d)(2).

### **III. Conclusion**

In sum, the lack of well-defined purpose and lack of proper limits on the proposed Fusion System threatens to turn fusion centers into wasteful and misdirected bureaucracies that cannot succeed in their ultimate goal of increasing public safety. Without reform, this System risks instead endangering the privacy rights and liberties of the American people.

Thank you for your consideration of this comment.

The Media Freedom and Information Access Practicum  
mfia@mailman.yale.edu