IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT – CHANCERY DIVISION

American Civil Liberties Union of Illinois,
Plaintiff,

v.

Illinois State Police,
Defendant.

No. 10 CH 40840

Judge Mary L. Mikva

ORDER AND OPINION

This cause comes on the Parties' Cross-Motions for Summary Judgment. The Court, having been fully advised on the premises, finds as follows:

Background

In 2008, the American Civil Liberties Union of Illinois ("ACLU") sent a request under the Illinois Freedom of Information Act ("FOIA"), 5 ILCS §140/1 *et seq.*, to the Illinois State Police ("ISP") requesting "any and all records in your custody or control that relate or refer to the Illinois Statewide Terrorism and Intelligence Center." ("STIC") A lengthy correspondence unfolded, in which ISP tendered some documents and declined to tender others. On September 21, 2010, the ACLU filed this action against ISP alleging violations of FOIA. On January 18, 2011, ISP filed its answer to the ACLU's complaint, and on March 17, 2011, ISP filed a FOIA §11(e) Index listing thirteen documents that it had either redacted before giving them to the ACLU, or denied access to altogether. On May 11, 2011, the ACLU indicated that it is challenging only the denial of access to documents 7-13 on the Index. On June 3, 2011, ISP filed a Motion for Summary Judgment, and on June 24, 2011, the ACLU responded, and filed its own Motion for Summary Judgment, both of which are addressed in this opinion.

Analysis

FOIA is intended to provide "all persons...full and complete information regarding the affairs of government and the official acts and policies of those who represent them." 5 ILCS §140/1. Public records are presumed to be open under FOIA, and any exemptions must be read narrowly. *Lieber v. Board of Trustees of Southern Illinois University.* 176 Ill. 2d 401, 408

(1997). Any public body asserting a FOIA exemption has the burden of proving that the exemption applies, by clear and convincing evidence. 5 ILCS §140/11(f).

In this case, there are seven documents at issue, and those documents may fairly be grouped into three categories. The first document is the Memorandum of Understanding ("MOU") between the Illinois National Guard ("Guard") and ISP regarding Guard support to ISP. The second category is "Event Threat Assessments." The third category is distribution lists of "Daily Intell" reports. These documents were all presented to the Court for in-camera review, and ISP has attached an affidavit provided by Brad Camuff, the Bureau Chief with STIC, attesting to the content of the documents and the perceived risks associated with their disclosure. Each of the three groups of documents is addressed separately below.

1. Memorandum of Understanding

The MOU, ex. 7, is a document detailing an agreement between the Adjutant General of the Department of Military Affairs State of Illinois and ISP explaining the circumstances under which the Guard may provide support to Illinois law enforcement, and the requirements of and limitations on that support. ISP argues that this document falls under FOIA exemptions §7(1)(d)(v) and §7(1)(d)(vi). These exemptions exclude the following documents from FOIA requests:

> (d) Records in the possession of . . . any law enforcement or correctional agency for law enforcement purposes, but only to the extent that disclosure would:
> (v) disclose unique or specialized investigative techniques other than those generally used or known . . . and disclosure would result in demonstrable harm to the agency or public body that is the recipient of the request; [or]
> (vi) endanger the life or physical safety of law enforcement personnel or any other person...

5 ILCS §140/7(1)(d)(v), (vi).

ISP argues that the MOU contains investigative techniques unique to shared operations between the Guard and ISP, and that the disclosure of those techniques could cause harm to these entities by allowing their actions to be predicted by criminals. Further, ISP argues that, in making public the role the Guard may play in ISP operations (specifically, whether they will be armed), the lives or physical safety of all personnel involved in these operations may be endangered.

In response, the ACLU argues that the asserted exemptions are inapplicable. Though the ACLU has not seen the documents in question, it emphasizes that it is ISP's burden to prove by clear and convincing evidence that one of the stated exemptions applies to the MOU. Here, the

ACLU argues that ISP has not proven that disclosing the MOU would "result in demonstrable harm" to law enforcement personnel or civilians. Rather, the ACLU argues, ISP's assertion is vague and conclusory, where specificity is required. *NACDL v. Chicago Police Dept.*, 399 Ill. App. 3d 1, 12 (1st Dist. 2010). The ACLU also takes issue with ISP's assertion that the MOU contains "unique or specialized investigative techniques other than those generally used and known." It argues that the exemption is only meant to be applied in circumstances where disclosure would threaten future use of the technique, and that routine techniques are not protected. *In re Marriage of Daniels*, 240 Ill. App. 3d 314, 338 (1st Dist. 1992). The ACLU notes that the affidavit states only that the MOU describes certain Guard techniques and methods, and that the Guard's use of those techniques and methods is not generally known. While ISP characterizes the techniques as "unique or specialized" in their memorandum, the ACLU argues that characterization lacks sufficient detail to be clear and convincing.

Having reviewed the MOU *in camera*, this Court has determined that §7(1)(d)(v) allows the ISP to exempt the majority of the MOU from disclosure, though not all of it. The MOU, in describing the method and ways of collaboration between the Guard and the ISP, describes unique and specialized investigative techniques, other than those generally used and known. In this Court's view, the disclosure of these would result in demonstrable harm to the ISP. Thus, much of the MOU is exempt under §7(1)(d)(v). In light of the fact that this specific exemption is applicable, there is no need for this Court to determine whether this information is also exempt under section (d)(vi).

However, in this Court's view, portions of the MOU are not exempt under either of the FOIA exemptions cited. Specifically, sections 1-2, and 11-14 do not disclose any investigative techniques. Instead, these sections explain the overall purpose of the MOU, the legal authority for such an agreement, the liabilities of the parties, and the bases for renegotiation and termination of the agreement. Since these sections do not contain any investigative techniques, they clearly do not contain the unique or specialized investigative techniques that might be exempt under §7(1)(d)(v). In addition, these paragraphs contain no information that Mr. Carnduff's affidavit suggests, if disclosed, could endanger the life or physical safety of law enforcement personnel. Thus, neither of the cited exemptions apply to these sections of the MOU. Accordingly, this Court hereby orders ISP to disclose sections 1,2,11,12,13, and 14 of the MOU to the ACLU. All other sections may be withheld under 5 ILCS §140/7(1)(d)(v).

2. Event Threat Assessments

Documents 8, 9 and 10 are three event threat assessments. These documents were drafted in preparation for anticipated protests related to Caterpillar, Inc., at various times in the past, the earliest one being protests expected at the 2006 Caterpillar annual shareholder meeting and the latest being the protests expected at the shareholders meeting in June, 2010. ISP argues that these documents fall under FOIA exemptions §7(1)(b-5), §7(1)(d)(v), §7(1)(f) and §7(1)(v). In this court's view, the applicable exemption is §7(1)(v) which exempts the following documents from FOIA requests:

> (v) Vulnerability assessments, security measures, and response policies or plans that are designed to identify, prevent, or respond to potential attacks upon a community's population or systems, facilities, or installations, the destruction or contamination of which would constitute a clear and present danger to the health or safety of the community, but only to the extent that disclosure could reasonably be expected to jeopardize the effectiveness of the measures or the safety of the personnel who implement them or the public. Information exempt under this item may include such things as details pertaining to the mobilization or deployment of personnel or equipment, to the operation of communication systems or protocols, or to tactical operations.

5 ILCS §140/7 (v).

The ACLU argues that the event threat assessments discuss both unlawful and *lawful* activity, and lawful activity could not reasonably be described as an "attack" on "populations or systems, facilities or installations." The ACLU also notes that the ISP does not argue that the threats contemplated in these assessments could cause destruction that would "constitute a clear and present danger to the health or safety of the community," nor, the ACLU contends, is it clear how disclosure would jeopardize safety or the effectiveness of the measures.

This Court has determined that 5 ILCS §140/7(1)(v) exempts these documents from disclosure. Caterpillar is a facility, the destruction or contamination of which would "constitute a clear and present danger to the health or safety of the community." The Court does not believe that this exemption requires ISP to show that these events must, in and of themselves, constitute a clear and present danger to the health or safety of the community. While the ACLU is correct in noting that the event threat assessments also describe lawful protest activities, any discussion of these lawful activities is inextricably interwoven with discussion of potential attacks. Further, ISP has argued, and this Court agrees, that the disclosure of these documents could reasonably be expected to "jeopardize the effectiveness of the measures or the safety of the personnel who implement them or the public." The methods and information gathering described in the event

threat assessments focus on past events. However, there can be little doubt that future events will likely happen involving Caterpillar and that the information in these assessments will continue to be relevant.

3. Daily Intell Lists

There are three "Daily Intell" lists included in the contested documents. These documents are lists of private and public entities that receive regular electronically transmitted intelligence updates containing confidential information from STIC. The ACLU does not seek the information itself; rather, only the list of individuals who *are* receiving this information. Exhibit 11 is the STIC Daily Intell For Official Use Only List of Agencies and contains private and public organizations and law enforcement agencies. Exhibit 12 is the STIC Daily Intell Illinois Wireless information Network List of Agencies. Exhibit 13 is the STIC Daily Intell Law Enforcement Sensitive List of Agencies. Exhibits 12 and 13 include only law enforcement agencies.

ISP argues that these documents are exempt from disclosure under §7(1)(d)(vi) and §7(1)(o). Exemption 7(1)(d)(vi) is set forth above in reference to the MOU. The exemption set forth in section (o) is as follows:

> o) Administrative or technical information associated with automated data processing operations, including but not limited to software, operating protocols, computer program abstracts, file layouts, source listings, object modules, load modules, user guides, documentation pertaining to all logical and physical design of computerized systems, employee manuals, and any other information that, if disclosed, would jeopardize the security of the system or its data or the security of materials exempt under this Section.

5 ILCS §140/7(1)(o).

ISP argues that the disclosure of these lists would endanger the safety of all similar entities that are *not* receiving these lists. The ISP argument is that criminals or terrorists, knowing that certain entities are being regularly brief by STIC, might choose to target entities *not* being briefed, under the supposition that such entities would be less prepared to prevent or ward off an attack. The ISP also argues that (o) applies, in that these lists are administrative information associated with automated data processing operations, and that disclosure of the lists could jeopardize the security of other materials exempt under FOIA, as terrorists, knowing which entities are in possession of this information, could hack into those with weaker computer security systems and locate confidential information.

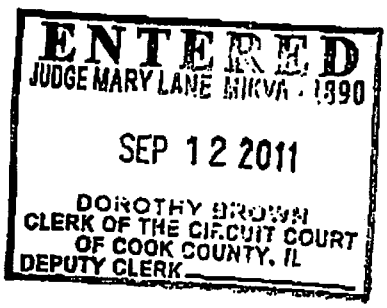
The ACLU asserts that ISP's argument that terrorists would conclude that groups not receiving Daily Intell reports are more vulnerable to attack is based on an assumption without evidence. Further, they contend this argument is even less persuasive when applied to the two Daily Intell lists that only go to law enforcement agencies. With regard to ISP's argument that the lists should be exempt under (o), the ACLU first contends that these circulation lists do not fall under this section, as this is not "technical or administrative information associated with automated data processing operations." Further, the disclosure of the lists would not reveal any computer system vulnerabilities, nor would it diminish the security of any computer systems. The ACLU argues that the distribution lists are not included in the specific examples provided by subsection (o) and their exclusion from these examples strongly suggests that the legislature did not intend to include them as administrative information.

This Court agrees with ISP as to the Daily Intell lists. The lists contain the names of agencies and places receiving information electronically. This is "administrative" information associated with the ISP's automated data processing operations. While the ACLU is correct that such distribution lists are not specifically listed in subsection (o), that subsection also exempts "any other information that would jeopardize the security of the system or its data." The Carnduff affidavit states that the information transmitted to the entities on these lists concerns safety issues and potential threats. Carnduff states that if an agency on one of these lists has security breaches in its computer systems, criminals and terrorists could take advantage of such a breach to gain access to the confidential information sent to these agencies. This is clear and convincing evidence that the exemption applies to all three of the lists.

In addition, the Court finds that §7(1)(d)(vi) applies to the first Daily Intell list, ex. 11, containing names of private entities, in addition to law enforcement agencies. The Court accepts the explanation offered by ISP that if criminal and terrorist elements were aware of which private entities received regular security briefings from law enforcement, those elements could be more inclined to target those private entities that were not privy to such information.

Conclusion

In summary, both the ACLU's and ISP's Motions for Summary Judgment are GRANTED in part and DENIED in part. ISP is ordered to disclose sections 1,2,11,12,13, and 14 of the MOU. The Court agrees with ISP that all other contested documents are exempt from disclosure under FOIA and thus grants ISP's Motion for Summary Judgment as to those documents. The September 26, 2011 status date remains for purposes of addressing any remaining issues in this case and for entry of a final Order.



Entered:

Mary L Mikva 1390

Judge Mary L. Mikva
Circuit Court of Cook County, Illinois
County Department, Chancery Division