UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

NATIONAL DAY LABORER ORGANIZING NETWORK, et al., Plaintiffs, -v - UNITED STATES IMMIGRATION AND CUSTOMS ENFORCEMENT, et al., Defendants.	Civil Action No. 10-CV-3488 **DECLARATION OF RYAN LAW**

I. INTRODUCTION

1. I am the Deputy FOIA Officer of the United States Immigration and Customs Enforcement ("ICE") Freedom of Information Act Office (the "ICE FOIA Office"). I have held this position since May 9, 2010. Prior to this position, I was a Senior Paralegal Specialist and Paralegal Specialist within the ICE FOIA Office beginning in February 2007. Prior to my employment with ICE, I was a FOIA Specialist within the Transportation Security Administration's FOIA Office beginning in September 2005.

2. The ICE FOIA Office is responsible for processing and responding to all Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, and Privacy Act, 5 U.S.C. § 552a, requests received at ICE. The ICE FOIA Office mailing address is 500 12th Street, S.W., STOP 5009, Washington, D.C. 20536-5009.

3. As the Deputy FOIA Officer, my official duties and responsibilities include the general management, oversight, and supervision of the ICE FOIA Office. I manage and supervise a staff of ICE FOIA Paralegal Specialists, who report to me regarding the processing of FOIA and

Privacy Act requests received by ICE. In connection with my official duties, I am familiar with ICE's procedures for responding to requests for information pursuant to provisions of FOIA and the Privacy Act. In that respect, I am familiar with ICE's handling of the FOIA request dated February 3, 2010, submitted by the Center for Constitutional Rights ("CCR"), the National Day Laborer Organizing Network ("NDLON"), and the Immigration Justice Clinic of the Benjamin N. Cardozo Law School ("Cardozo"), the Plaintiffs in the above-captioned action, to which the ICE FOIA Office assigned FOIA case number 2010FOIA2674.

4. I make this declaration in my official capacity in support of ICE's motion for partial summary judgment on the adequacy of its searches for "opt out" and "Rapid Production List" ("RPL") records. The statements contained in this declaration are based upon my personal knowledge, my review of documents kept by ICE in the ordinary course of business, and information provided to me by other ICE employees in the course of my official duties.

5. The purpose of this declaration is to describe, in detail, ICE's search for, and production of, opt-out and RPL records.

II. GENERAL INFORMATION REGARDING ICE'S STANDARD PROCEDURE FOR INITIATING SEARCHES IN RESPONSE TO FOIA REQUESTS

6. Each program office within ICE has a designated point of contact ("POC") who is the primary person responsible for communications between that program office and the ICE FOIA Office. When the ICE FOIA Office receives a FOIA request, its first step is to identify which program offices within ICE are most likely to possess records responsive to that request and to initiate searches within those program offices. Once the ICE FOIA Office determines the appropriate program offices for a given request, it provides the POCs within each of those program offices with a copy of the FOIA request and specific instructions for conducting a search for responsive records. The POCs then review the FOIA request and instructions, and

forward the request and instructions to the individual employees or component offices within the program office that they believe are most likely to have responsive records. Based on their knowledge of the manner in which they maintain their records and the nature of their involvement with the subject matter of the FOIA request, the individuals then conduct searches of all file systems (including both hard copy and electronic files) likely to contain responsive records. Once those searches are completed, the individuals and component offices provide any potentially responsive records to their program office's POC, who in turn provides the records to the ICE FOIA Office. The ICE FOIA Office then reviews the collected records for responsiveness.

7. ICE employees maintain records in several ways. ICE program offices use various systems to maintain records that are accessible to multiple custodians within that office, such as investigative files, records of removable aliens, records regarding the operation of ICE programs, and administrative records. ICE employees may store electronic records on their individual computer hard drives, their program office's shared drive (if the office uses one), DVDs, CDs, or USB storage devices. Additionally, all ICE employees have access to email. ICE uses the Microsoft Outlook email system. During the period in which ICE conducted searches for documents responsive to the RPL and "opt-out" portions of Plaintiffs' request, ICE employees used either the 2003 or 2007 versions of Microsoft Outlook. Each ICE employee stores their files in the way that works best for that particular employee; ICE has no agency-wide policy or regulation that mandates how employees retain and store their emails or other electronic files. ICE employees use various methods to store their Microsoft Outlook email files: some archive their files monthly, without separating by subject; others archive their email by topic or

by program; still others may create PST files of their emails and store them on their hard drive or on a shared drive.

8. ICE employs disaster recovery systems to back up its email and file servers in accordance with Federal and DHS regulations. As part of ICE's disaster recovery plan, the agency maintains systems designed to restore agency email and file servers in the event of a catastrophic loss of data.

9. Prior to December 2008, ICE relied on periodic data archiving of its email servers on backup tapes. ICE used a variety of different systems and the backup tapes were regularly overwritten to maintain the continuity of the archival system for disaster recovery purposes. The intent of the backup systems was not to create a permanent or semi-permanent archive of the agency's emails, but was rather intended to allow the agency to restore its email and file servers in the event of catastrophic loss of data.

10. Beginning in December 2008, ICE implemented a new server-based disaster recovery system for email servers. At present, agency emails are being maintained indefinitely for data backup purposes, i.e. for recovery in the event of catastrophic loss of data.

11. Because the new server based disaster recovery system for email servers retains the complete email archive for every ICE employee, it contains an enormous quantity of data. As a result, searches of the servers and data retrieval from the disaster recovery system are extremely time consuming and require the services of the agency's Office of the Chief Information Officer (OCIO). Given the significant time and resource limitations of OCIO, ICE does not leverage the disaster recovery server for conducting routine FOIA searches.

12. It is not part of OCIO's mission to conduct FOIA searches on behalf of the agency and OCIO is not staffed or resourced to routinely take on FOIA searches on behalf of all other ICE program offices.

13. In addition, ICE does not have the capability to conduct routine FOIA searches on retrieved email archives due to storage limitations in ICE's e-discovery platform. ICE currently has 500GB of storage, which is purchased for an annual fee. Conducting routine FOIA searches of archived emails within the e-discovery system on the over 16,000 FOIA requests that ICE receives each year would rapidly overwhelm ICE's data storage capabilities and render the e-discovery platform useless for the litigation purpose for which it was acquired by the ICE Office of the Principal Legal Advisor.

14. Individual employees also archive their own emails according to their individual work-related needs by placing emails into .pst files that are stored either on their individual computer hard drives or on a shared network drive. Individual archives of emails are searched by the individual employees where those employees have identified individual archives as containing potentially responsive documents.

II. PLAINTIFFS' FOIA REQUEST AND THE INSTANT LITIGATION

15. On or about February 3, 2010, ICE received a FOIA request from Plaintiffs for records relating to the ICE immigration enforcement strategy Secure Communities.

16. Secure Communities leverages an existing information sharing capability between the U.S. Department of Homeland Security ("DHS"), of which ICE is a component, and the U.S. Department of Justice ("USDOJ") to quickly and accurately identify aliens who are arrested for a crime and booked into local law enforcement custody. With this capability, the fingerprints of

everyone arrested and booked are not only checked against Federal Bureau of Investigation ("FBI") criminal history records, but they are also checked against DHS immigration records. If fingerprints match DHS records, ICE determines whether immigration enforcement action is required, considering the immigration status of the alien, the severity of the crime and the alien's criminal history. Secure Communities also helps ICE maximize and prioritize its resources to ensure that the right people, processes and infrastructure are in place to accommodate the increased number of criminal aliens being identified and removed. Secure Communities modernizes the identification and removal processes by: (1) using fingerprint-based biometric identification technology, (2) prioritizing resources toward the greatest threats, and (3) sharing information between law enforcement partners.

17. Plaintiffs' FOIA request was 21-pages long and sought records relating to seven broad categories: "Policies, Procedures and Objectives"; "Data and Statistical Information"; "Individual Records"; "Fiscal Impact of Secure Communities"; "Communications"; "Secure Communities Program Assessment Records"; and "Secure Communities Complaint Mechanisms and Oversight". ICE's preliminary estimates indicted that Plaintiffs' request would implicate millions of pages of potentially responsive records.

18. Upon receiving plaintiffs' request, consistent with the general procedures described in paragraph 6 above, the ICE FOIA Office identified the offices and divisions within the agency that had direct oversight over Secure Communities, that may have been tangentially involved with Secure Communities as a part of general agency operations, or that were otherwise likely to have records responsive to plaintiffs' request. The ICE FOIA Office identified the following offices and divisions as likely possessing records

responsive to plaintiffs' request, and tasked them with conducting searches for potentially responsive records:

a. The ICE Office of Enforcement and Removal Operations ("ICE ERO") has direct oversight over Secure Communities. Within ICE ERO's headquarters office, the Secure Communities Program Office implements and manages ICE's Secure Communities strategy. Additionally, each ICE ERO Field Office located throughout the country appoints a point of contact (Supervisory Detention and Deportation Officer or higher) who serves as the Secure Communities Field Coordinator for that Field Office's Area of Responsibility ("AOR"). The Secure Communities Field Coordinators serve as ICE ERO's liaisons on Secure Communities matters to state and local law enforcement agencies within their respective AORs. Their duties include coordinating outreach sessions to law enforcement agencies, developing schedules for deploying Secure Communities within particular jurisdictions, and coordinating activation-related activities in support of achieving nationwide deployment of Secure Communities by 2013. The Secure Communities Field Coordinator assignments are collateral duty positions within each Field Office. Collateral duty assignments are in addition to the existing duties inherent to a position; Secure Communities Field Coordinators are typically Supervisory Detention and Deportation Officers (SDDO) that spend some fraction of their work hours on Secure Communities coordination within the office, but would have spent the majority of their working time on normal SDDO duties.

b. The ICE Office of Policy is responsible for identifying, developing, and effectively communicating ICE priorities and policies. It is responsible for the development and maintenance of agency policies related to Secure Communities.

c. The ICE Office of the Principal Legal Advisor ("ICE OPLA") provides legal advice, training, and services to support the ICE mission and defends the interests of the United States in the administrative and Federal Courts. ICE OPLA provides legal advice and guidance to the ERO program office on a wide range of agency issues, including those related to Secure Communities.

d. The ICE Office of State, Local, and Tribal Coordination ("ICE OSLTC") is responsible for building and improving relationships and coordinating partnership activities for multiple stakeholders – including state, local, and tribal governments, as well as law enforcement agencies and non-governmental organizations. As part of its duties, ICE OSLTC occasionally is involved in discussions with stakeholders concerning Secure Communities.

e. The Office of Congressional Relations ("ICE OCR") represents ICE in a broad variety of federal congressional liaison activities. ICE OCR is responsible for maintaining an effective liaison and promoting greater congressional awareness of ICE operations, national and local policies, as well as the agency's various programs and initiatives. ICE OCR provides briefings and reports to Congress on various ICE programs, including Secure Communities.

f. The ICE Office of Public Affairs ("ICE OPA") is the agency's public face, dedicated to building an understanding of, and support for, the ICE mission through outreach to employees, the media, and the general public. OPA responds to media inquiries and questions from local law enforcement and the general public about Secure Communities.

g. The ICE Office of Homeland Security Investigations ("ICE HSI") is responsible for investigating a wide range of domestic and international activities arising from the illegal movement of people and goods into, within, and out of the United States. ICE HSI investigates immigration crime, human rights violations and human smuggling, smuggling of narcotics, weapons and other types of contraband, financial crimes, cybercrime and export enforcement issues. ICE special agents conduct investigations aimed at protecting critical infrastructure industries that are vulnerable to sabotage, attack, or exploitation. In addition to ICE criminal investigations, ICE HSI oversees the agency's international affairs operations and intelligence functions. The Criminal Alien Program (CAP), an immigration enforcement strategy that was one of the subjects of a portion of plaintiffs' FOIA request, was previously under the direction of HSI.

h. The ICE Office of the Chief Financial Officer ("ICE CFO") is responsible for providing financial and asset management services and guidance for ICE. Plaintiffs' request sought budget and funding information pertaining to Secure Communities that was likely in the possession of ICE CFO.

i. The ICE Office of Acquisitions ("ICE OAQ") is responsible for managing ICE's procurement operations. ICE OAQ facilitates the acquisition of goods and services through contracts. Plaintiffs' request sought budget and funding information pertaining to Secure Communities, which could possibly involve information maintained by ICE OAQ.

j. The ICE Office of Professional Responsibility ("ICE OPR") is responsible for investigating allegations of employee misconduct impartially, independently, and thoroughly. ICE OPR prepares comprehensive reports of investigation for judicial or

management action. ICE OPR inspects and reviews ICE offices, operations and processes in order to provide executive management with an independent review of the agency's organizational health and assesses the effectiveness and efficiency of the overall ICE mission. ICE OPR screens potential ICE employees for character and suitability. Plaintiffs' original request sought information on complaints arising from Secure Communities, including claims of racial profiling or other constitutional violations; to the extent ICE had received any such complaints, subsequent investigations would likely have involved ICE OPR.

k. The ICE Office of Training and Development ("ICE OTD") is responsible for providing technical, educational, and career development and training programs for ICE employees. Plaintiffs' request sought information on training materials pertaining to Secure Communities which would likely have been created and maintained by ICE OTD.

l. The ICE Office of the Assistant Secretary ("ICE OAS") includes the offices of the Director, the Deputy Director, the Assistant Deputy Directors, and the Chief of Staff. OAS is responsible for the overall day-to-day operation of all of ICE's programs and enforcement strategies, including Secure Communities. ICE OAS oversees agency operations and is involved with higher level decision making on sensitive issues impacting the agency.

m. The Office of the Executive Secretariat ("Exec Sec") is responsible for responding to all public, governmental and congressional correspondence addressed to the agency. The office is also responsible for maintaining a repository for incoming letters, internally-generated tasks, and legislative records. The Office of Executive Secretariat Information Management System

(OESIMS) is a central repository for all incoming correspondence received by ICE and any outgoing responses. OESIMS also contains internal memoranda.

19. Also consistent with the general procedures described in paragraph 6 above, the POCs for each of the program offices and divisions described in paragraph 18 were provided with copies of plaintiffs' FOIA request, and were instructed to identify the employees within their respective offices who might reasonably be expected to have responsive documents. The POCs, in turn, tasked the appropriate employees with conducting searches for responsive records. Each employee was instructed to search paper files, email files, electronic files (including shared network drives and individual computer hard drives) and database files as appropriate. In addition, each employee was required to fill out a search tracker form that described the actions taken by the employee to search for potentially responsive records, including noting search terms to the extent they were used. All potentially responsive documents and search tracker forms were to be returned to the ICE FOIA Office.

20. The initial request was so broad and covered such a wide swath of documents that it was not possible for the ICE FOIA Office to provide suggested search terms to the program offices tasked with the searches. Because the original FOIA request sought so many different documents from across the agency, ICE FOIA determined that the program offices were in the best position to formulate the terms of each office's search in accordance with the types of records each office might be likely to have.

21. ICE FOIA does not typically provide search instructions that specify how specific types of documents should be searched. Agency employees are expected to be familiar with computer functions, including the search capabilities of agency operating

systems such as Windows. Further, because there is no agency-wide requirement for how employees maintain documents, detailed search instructions would be ineffective and possibly cause unnecessary delays. Employees could also inadvertently overlook potentially responsive documents because generic instructions would not take into account individual document maintenance practices.

22. ICE maintains records in a wide variety of electronic formats in the manner best suited to support agency operations. This may include .zip files, .pdf files and .txt files that are stored on agency shared drives, the individual hard drives of agency employees, removable storage devices, such as thumb drives and DVD and CD-roms, and as attachments to emails. Some .pdf files are text searchable, and others may not have undergone the optical character recognition process, but all files are maintained in the regular course of business in a manner that supports the agency's mission.

23. Employees are instructed to search electronic media and files as appropriate, which may include all the file types referred to in Paragraph 22. Some employees may conduct manual searches of such files by opening individual documents and attachments, while others may conduct searches utilizing search terms. ICE FOIA does not require employees provide search information at such a granular level in its search tracker forms and therefore, information on the treatment of specific file types is unavailable.

24. Beginning in March 2010 and continuing through September 2010, the ICE FOIA Office received potentially responsive documents from the following offices: ICE OCR, ICE OPA, ICE OPLA, ICE ERO, ERO-Secure Communities, ICE OAS, and ICE OSLTC. The following offices completed their searches for records responsive to

plaintiffs' request but indicated that they had not located any potentially responsive records: ICE CFO[1], ICE OTD[2], ICE HSI[3] and ICE OPR.[4]

25. On April 27, 2010, before ICE had produced any records, Plaintiffs commenced the instant litigation.

III. ICE'S RAPID PRODUCTION LIST SEARCHES

26. Following Plaintiffs' filing of the instant litigation, ICE, through its attorneys, engaged Plaintiffs in numerous negotiations aimed at narrowing the scope of the extremely broad request.

27. Plaintiffs and ICE were unable to come to any agreement on narrowing the scope of the Plaintiff's FOIA request. However, on June 25, 2010, Plaintiffs presented ICE and the other defendant agencies with a "Rapid Production List" ("RPL") that identified ten broad categories of records and certain specific documents that Plaintiffs sought on a priority basis. On July 19, 2010, ICE agreed to produce records responsive

[1] ICE CFO, through the office's FOIA POC, confirmed that the Secure Communities program office handles their own finances, and as a result, ICE CFO would not be likely to have any responsive records.
[2] ICE OTD, through the office's FOIA POC, confirmed that OTD does not provide training services for or on behalf of the Secure Communities program office, and as a result, OTD would not be likely to have any responsive records.
[3] ICE HSI, through the HSI Information Disclosure Unit, confirmed that the only HSI component that had contact with Secure Communities was the Law Enforcement Service Center (LESC). The records held by the LESC were records on individuals identified through interoperability. As the parties had agreed to dispose of Plaintiffs' request for individual records through production of anonymized statistics and data, LESC records were not collected for either the RPL or the opt-out productions. LESC did provide two sample Immigration Alien Reports (IARs), which were posted to ICE's FOIA Reading Room. ICE HSI determined the office would not be likely to have any other responsive records.
[4] ICE OPR stores investigative records in the Joint Intake Case Management System (JICMS). Records within JICMS are maintained according to the name of the complainant and do contain some searchable free text fields. However, ICE OPR does not require the name of an operation or program to be noted in the free text fields so there is no clear way to identify which complaints may be connected with a specific operation or program. An ICE OPR agent conducted an initial keyword search of their database, using the terms "secure" and "communities"; this search revealed no responsive records. The ICE OPR Director and Deputy Director concluded, based upon the type of information that is placed in JICMS, that there would be no reasonable method to isolate any complaints that were connected to Secure Communities. In addition, at the time of the initial request, ICE was not aware of any complaints related to Secure Communities.

to the RPL on an expedited basis. A copy of Plaintiffs' RPL is attached hereto as Exhibit A.

28. As described above, at the time it agreed to the RPL, ICE had identified records that were potentially responsive to plaintiffs' FOIA request but had not completed its review of those records and had not released any records to plaintiffs. Thus, ICE commenced its search for records responsive to the RPL by reviewing the records that the offices and divisions described above had already identified as potentially responsive to plaintiffs' overall FOIA request. The ICE FOIA Office, in conjunction with agency counsel and the Secure Communities Program Office, manually reviewed and identified a number of records collected during the initial searches that were both responsive to the RPL and of interest to the general public. Those records were processed and posted to the ICE FOIA Library, ICE's electronic reading room, which is available online at http://www.ice.gov/foia/library/index.htm#47. Plaintiffs were informed that those records had been made available online.

29. ICE also conducted new searches for records responsive to the RPL. Given the types of information that the RPL requested, ICE often was able to pinpoint the specific offices or divisions likely to possess such records and task those offices and divisions with searching for records responsive to specific RPL categories:

a. Item I of the RPL requested a) Copies of all regularly generated statistical reports and b) copies of any cumulative statistics compiled on SC. ICE FOIA and agency counsel directed this portion of the RPL to the ICE ERO Secure Communities Program Office, specifically the Communications and Outreach Branch, which is responsible for maintaining statistics on

Secure Communities. The ICE ERO Secure Communities Communications and Outreach Branch then compiled all regularly generated statistical reports and cumulative statistics by locating such reports from files on the shared drive within the Secure Communities folder where the reports were stored as part of the office's normal business practice. The reports were generated for Plaintiffs and were also posted to the ICE FOIA Reading Room. Monthly statistical reports on Secure Communities continue to be posted to the ICE FOIA Reading Room on a regular basis as they are generated.

b. Item II of the RPL requested "opt-out" records. ICE's search for the opt out records is described in detail at paragraphs 35 through 57 below.

c. Item III of the RPL requested copies of executed agreements related to Secure Communities between ICE/DHS and the FBI, as well as agreements between DHS/FBI and local government or law enforcement agencies. Based upon a manual review of the material on the ICE FOIA Reading Room, ICE determined that all copies of agreements between DHS/ICE and state governments were already publicly available on the ICE FOIA Reading Room, and informed plaintiffs of that fact. The Secure Communities Deployment Branch, which is the entity within Secure Communities which is responsible for the deployment and technical aspects of Secure Communities, determined based on the knowledge of Deployment Branch employees that there was a single agreement between ICE and FBI regarding Secure Communities. ICE

located and produced to Plaintiffs a copy of the ICE/FBI agreement on September 10, 2010.

d. Item IV of the RPL requested a technical explanation of all databases that could contain information responsive to the sections of Plaintiffs' FOIA request that sought individual records, including a list of all databases that contain information on individuals identified by Secure Communities, a list of all fields in each database containing information on individuals identified by Secure Communities, and records that describe how interoperability functions. ICE determined that it does not maintain a list of databases that contain information on individuals identified by Secure Communities. Further, ICE does not maintain a list of all of the fields in the databases that contain information on individuals identified by Secure Communities. However, the Deployment Branch of the ICE ERO Secure Communities Program Office conducted a supplemental search and located documents describing the function of interoperability. The search was done without the use of search terms as Deployment Branch staff was familiar with the limited number of documents describing interoperability functions. Those documents were produced to Plaintiffs as part of the July 2010 and February 25, 2011 productions.

e. Item V of the RPL requested certain records that had been identified by the DHS Office of the Inspector General ("OIG") and referred to ICE for direct response. ICE processed the referred documents and released them to Plaintiffs as part of the September 2010 production.

f. Item VI of the RPL requested records related to the creation or revision of three specific media documents. Agency counsel contacted ICE OPA and identified the two OPA employees who worked on creating and revising the media documents in question. The two employees then conducted a search for records related to the creation or revision of the documents. The employees searched their e-mail files based on a date range that preceded the date of the final versions of the three documents. The date range was selected to capture the time period in which OPA would have been reviewing the documents. Because of OPA's normal document revision process, all documents and comments were known to be transmitted through email. The OPA employees identified a number of responsive e-mails, which were produced to plaintiffs as part of the July 2010 production.

g. Item VII of the RPL sought all reports and memoranda reporting on Secure Communities to DHS, the Assistant Secretary of Homeland Security in Charge of ICE, or the White House. All agency wide taskings and documents that require review by more than one program office, such as the types of reports and memoranda sought by this portion of the RPL, are logged into the Sharepoint system. Therefore, the Secure Communities Program Office and the Office of the Assistant Secretary determined that, to the extent they possessed documents responsive to this portion of the RPL, such documents would be located in Sharepoint. Because Sharepoint is an agency-wide resource, ICE was able to rely on a

prior, broader search of Sharepoint conducted by a Management Program Analyst within the Secure Communities Program Office. The Program Analyst conducted a manual search of each folder within Sharepoint and reviewed each document therein for responsive material. ICE FOIA and agency counsel reviewed the results of that search and located no documents responsive to Item VII.

h. Item VIII requested specific enumerated records related to Secure Communities and racial profiling. Two employees within ICE OSLTC (a Senior Public Engagement Officer and the Deputy Assistant Director) as well as employees from the ICE ERO Secure Communities Communications and Outreach Branch, conducted a search for responsive records. The two employees from OSLTC were determined by OSLTC to possibly have responsive documents based upon their work responsibilities. The Senior Public Engagement Officer works with governmental and nongovernmental organizations (NGOs) as a liaison for the agency on various issues, including Secure Communities, and was the individual within OSTLC that would have addressed racial profiling questions. The OSLTC Deputy Assistant Director conducted training and outreach to law enforcement groups and organizations and also may have fielded inquires on racial profiling. The Communications and Outreach Branch of Secure Communities was also in contact with NGOs and representatives of the media to answer inquiries about Secure Communities. No responsive documents were located that pertained to

the first category sought by plaintiffs, i.e., "records created in relation to the drafting of Section 1.0 of the Secure Communities Standard Operating Procedures (SOP) or Section VII of the Secure Communities MOA." Records relating to ICE plans to monitor for racial profiling or other Constitutional violations were produced to Plaintiffs in the September 2010 and February 25, 2011 productions. No responsive records were located pertaining to evaluation of any state or local jurisdiction pursuant to Section 1 of the SOP or Section VII of the MOA. ICE is not routinely involved with the assessment of claims of racial profiling or constitutional violations against states and local jurisdictions. The DHS Office of Civil Rights and Civil Liberties is the entity that is charged with addressing such complaints. To the best of ICE's knowledge, at the time ICE conducted the RPL searches, neither ICE nor DHS had received any such complaints.

i. Item IX of the RPL sought records of ICE communications with the states of Florida, California, and Texas related to costs, reimbursements, monetary agreements, or monetary incentives related to Secure Communities. The ICE ERO Secure Communities Program Office conducted a search for the requested documents, but no responsive documents were located. Secure Communities does not involve any monetary agreements and/or incentives or other reimbursements to states and localities. A number of e-mails were located by the Communications and Outreach Branch and the Deployment Branch that conveyed

information to various states about Department of Justice programs that could provide funding to states and localities based on a manual search of emails. These documents were produced as part of the February 25, 2011 production.

j. Finally, Item X of the RPL sought specific documents and categories of documents that were listed in an appendix to the RPL. ICE's search for and production of these records is described in the following paragraphs.

30. All documents and categories of documents requested in Item X of the RPL were located and produced to Plaintiffs in the July and September 2010 productions with the exception of certain funds utilization reports (# 4, RPL appendix), executive monthly status reports (#5, RPL appendix), and PMO status reports (#6, RPL appendix), which were produced in the February 25, 2011 production. ICE conducted manual searches for the documents contained in Item X based upon the knowledge of Secure Communities Program Office Staff.

31. Plaintiffs requested the overall implementation plan for Secure Communities (# 9, RPL appendix), but it was determined by the ICE ERO Secure Communities Program Office that such a document was never created. The document that would best fit such a description would be the Concept of Operations Strategic Plan, which was produced to Plaintiffs in September 2010.

32. Certain categories of documents were not located or were determined to be non-existent, including records relating to the presentations to the National Association of Counties, Office of Management and Budget, and an NEC AFIS briefing (# 11, 12, 13, RPL appendix). ICE FOIA and agency counsel consulted with the Branch Chief of the

Secure Communities Communications and Outreach division. The Branch Chief of the Communications and Outreach division was the coordinator within the agency for training and presentations conducted by the agency on Secure Communities. The Branch Chief advised, based her knowledge about the preparation for presentations and presentation materials themselves, that no lists of attendees were collected, and that most presentations did not have extensive notes, plans, or pre and post-presentation correspondence. The Branch Chief did conduct several manual searches and although the actual presentation materials were located and produced, no records of notes and plans of the meetings, lists of attendees, and correspondence before and following the presentations were located.

33. As a result of the searches described above, documents responsive to Plaintiffs' RPL were released to the Plaintiff on July 30, 2010, September 10, 2010, October 21, 2010, and December 6, 2010.

34. By order dated December 17, 2010, the Court directed ICE to produce the remainder of the RPL documents to Plaintiffs on February 25, 2011. On that date, consistent with the order, ICE produced the remaining 2,014 pages of records it had identified through the searches described above as responsive to the RPL.

V. ICE'S SEARCH FOR OPT-OUT RECORDS

35. In October 2010, plaintiffs informed the defendant agencies for the first time that RPL Item II, requesting opt-out records, was their top priority. Thereafter, ICE initiated a search for opt-out records.

36. On November 11, 2010, the ICE FOIA Office instructed ICE ERO (including the ICE ERO Secure Communities Program Office), ICE OPLA, ICE OSLTC, ICE OCR, ICE OPA, ICE

Office of the Director, and, ICE ExecSec, to conduct a targeted supplemental search for opt-out records. The ICE FOIA Office provided these ICE Program Offices with a copy of the Plaintiffs' RPL, instructed the programs to conduct a comprehensive search of paper and electronic files for records that would be potentially responsive to item II of the RPL, and requested that those ICE Program Offices forward any potentially responsive records to the ICE FOIA Office for review and processing. Further, the ICE FOIA Office suggested that those ICE Program Offices use the following search terms during the search for responsive electronic records: "opt-out," "mandatory," "voluntary," "participation," opting-out," choosing," "mandate," and "opt out." Finally, the ICE FOIA Office instructed those ICE Program Offices not to limit their searches to these suggested search terms, but to use their knowledge of their particular record keeping systems and practices to conduct a search that they believed was likely to best uncover records that would be potentially responsive to Plaintiffs' request. The Secure Communities Program office aided agency counsel and the ICE FOIA office in compiling search instructions entitled "How To Search for Opt-Out Records," attached as Exhibit B. The instructions listed the suggested search terms, and specified that the searches were to include the full text of the documents. The instructions did not address the issue of combining any of the search terms or using any connectives.

A. ICE ERO

37. Within the ICE ERO Secure Communities program office, every staff member in each of the Program's six branches was instructed to conduct a search for opt-out records. Those six branches are the Business Transformation Unit ("BT"); the Information Technology Management Unit ("IT Management"); the Deployment Unit ("NDU"); the Enforcement Portfolio Unit ("EPU"); the Strategy and Operational

Analysis Unit ("SOA"); and the Communications & Outreach Unit ("C&O"). Additionally, ICE ERO Secure Communities Program Office front office staff, consisting of the Assistant Director, the Deputy Assistant Director, the Chief of Staff, and mission support personnel[5] also completed searches in accordance with the direction provided by the ICE FOIA Office.

a. BT supports ERO by transforming the criminal alien enforcement process through modernizing systems and enhancing processes. The Unit provides analysis and definition of requirements for projects prior to detailed requirements, design, and software development. This ensures that all investments are aligned with critical ERO needs and that all solutions drive resolution to specific technological or process based challenges. Additionally, the Unit integrates ERO efforts to achieve process and technology efficiency across units by defining the strategy, capabilities, and resource needs required to execute upon program priorities.

b. As a complement to the BT Unit, IT Management provides hands-on portfolio and project management support for ICE IT projects. This team supplies the needed oversight to drive successful project delivery and investment return by ensuring adherence to the ICE System Lifecycle Management processes, implementing best practices, monitoring change requests, and analyzing alternative investments/strategies.

c. NDU manages all functions related to interoperability deployment to achieve nationwide activation by 2013. NDU liaises with ERO Field

[5] Mission support personnel are support staff for the offices. They are responsible for secretarial and administrative tasks. In some offices, mission support employees may help office leadership with scheduling, filing, and other office support.

Operations, SC Field Coordinators, the ICE OSLTC, ICE OPA, ICE OCR, and the Department of Homeland Security (DHS) Intergovernmental Affairs (OIA). Specifically, NDU provides oversight and coordinates training, communication, and deployment activities (including strategy) for new and ongoing technology initiatives. NDU provides critical tactical support to SC initiatives by monitoring ongoing deployments, identifying potential risks, issues, and interdependencies, and adjusting deployments accordingly.

d. EPU manages the interaction between ERO programs and mission support functions. The Unit is critical to successfully coordinating and reporting on law enforcement activities managed by ERO by providing subject matter expertise that extends beyond ERO to HSI, ICE, and local law enforcement agency needs. Additionally, EPU leads specialized, high-impact studies that require deep law enforcement field operations understanding beyond that of other Secure Communities units.

e. SOA conducts performance and operational analysis to continually identify and introduce efficiencies throughout ERO. SOA works in partnership with the ERO Mission Support Division (MSD) and the ICE Office of the Chief Financial Officer to integrate their cost models into our operational analyses.

f. C&O supports many divisions in ERO and ICE by managing communication and outreach efforts and activities to federal, state and local law enforcement partners, media entities, NGOs, Congress and local

elected officials. This unit liaises internally with ERO Front Office, OPA, OCR, OSLTC and DHS IGA to further the transformational mission of SC.

38. All six divisions within the Secure Communities Program Office were tasked with the search for records and all Secure Communities personnel conducted a search for records in an attempt to be as comprehensive as possible given the relatively limited focus of the search.

39. The staff members in each of the ICE ERO Secure Communities Program Office units described above conducted searches of shared network drives, hard drives, and Microsoft Outlook e-mail files for potentially responsive records. Those employees were provided a copy of Plaintiffs' RPL and the instructions provided by the ICE FOIA Office as described in Paragraph 26, above. Secure Communities Program Office staff members were also given a document, entitled "How to Search for Opt-Out Records," (which is attached as Exhibit B) that was created by the Secure Communities Chief of Staff. This document listed the date range for responsive documents, the eight suggested search terms ("opt-out," "mandatory," "voluntary," "participation," opting-out," choosing," "mandate," and "opt out"), a reminder not to be limited by suggested search terms if the employee believed that he/she may have had responsive documents that could have been located using other search terms that were not included, and a step by step guide describing how to use the "Advanced Find" tool within Microsoft Outlook, for those employees who may have been unfamiliar with its operation. The "Advanced Find" tool conducts searches for keywords both in the subject line and body of email messages. Employees serving as the ICE ERO Secure Communities Field Coordinators

at each of the 24 ICE ERO Field Offices conducted searches of their network drives, hard drives, and Microsoft Outlook e-mail files. Those employees were provided a copy of Plaintiffs' RPL and the same instructions provided by the ICE FOIA Office as described in Paragraph 36, above. Additionally, these ERO employees were given a copy of the "How to Search for Opt-Out Records" document. The following Field Coordinators within each Field Office conducted searches for opt-out records:

a. In the Atlanta Field Office, 2 Supervisory Detention and Deportation Officers (SDDO) and 1 Assistant Field Office Director (AFOD) were tasked with searching for responsive records.

b. In the Baltimore Field Office, 1 AFOD and 1 SDDO were tasked with searching for responsive records.

c. In the Boston Field Office, 6 AFODs and 6 SDDOs were tasked with searching for responsive records.

d. In the Buffalo Field Office, 2 SDDOs and 1 Staff Assistant were tasked with searching for responsive records.

e. In the Chicago Field Office, 2 AFODs, 2 SDDOs, 4 Deportation Officers (DO), and 1 Senior Immigration Enforcement Agent (SIEA) were tasked with searching for responsive records.

f. In the Dallas Field Office, 1 287(g) Program Manager was tasked with searching for responsive records.

g. In the Denver Field Office, the Field Office Director (FOD), the Deputy Field Office Director (DFOD), 1 AFOD, and 1 SDDO were tasked with searching for responsive records.

h. In the Detroit Field Office, 1 AFOD and 1 SDDO were tasked with searching for responsive records.

i. In the El Paso field Office, 1 AFOD, 1 SDDO, and 1 DO were tasked with searching for responsive records.

j. In the Houston Field Office, 1 SDDO and 2 Immigration Enforcement Agents (IEA) were tasked with searching for responsive records.

k. In the Los Angeles Field Office, 1 AFOD and 2 SDDOs were tasked with searching for responsive records.

l. In the Miami field Office, 2 AFODs and 1 SDDO were tasked with searching for responsive records.

m. In the Newark Field Office, 1 SDDO was tasked with searching for responsive records.

n. In the New Orleans Field Office, 1 AFOD was tasked with searching for responsive records.

o. In the New York City Field Office, 2 AFODs and 1 DO were tasked with searching for responsive records.

p. In the Philadelphia Field Office, 1 AFOD was tasked with searching for responsive records.

q. In the Phoenix Field Office, 6 SDDOs were tasked with searching for responsive records.

r. In the Seattle Field Office, 2 AFODs and 1 SDDO were tasked with searching for responsive records.

s. In the San Francisco Field Office, 3 AFODs and 1 SDDO were tasked with searching for responsive records.

t. In the Salt Lake City Field Office, 1 DFOD and 5 SDDOs were tasked with searching for responsive records.

u. In the San Antonio Field Office, 1 AFOD, 1 SDDO, 1 SIEA, 4 IEAs, and 4 DOs were tasked with searching for responsive records.

v. In the San Diego Field Office, 2 SDDOs and 1 DO were tasked with searching for responsive records.

w. In the Saint Paul Field Office, 1 DFOD, 2 AFODs, 5 SDDOs, 4 DOs, 4 SIEAs, and 9 IEAs were tasked with searching for responsive records.

x. In the Washington Field Office, 1 AFOD was tasked with searching for responsive records.

40. The ICE ERO Field Office Directors at each of the 24 ERO Field Offices also conducted searches of their network drives, hard drives, and Microsoft Outlook e-mail files. The ICE ERO Field Office Directors were provided a copy of Plaintiffs' RPL and the instructions provided by the ICE FOIA Office as described in Paragraph 36 above.

41. Moreover, each ICE ERO Field Office Director was asked to instruct those employees within their respective offices who, in their opinion, would be most likely to have information related to Secure Communities to conduct a search for responsive records. Those employees were provided a copy of Plaintiffs' RPL and the instructions provided by the ICE FOIA Office as described in Paragraph 36, above. Additionally, these ERO employees were given a copy of the "How to Search for Opt-Out Records"

document. Over 100 ERO employees throughout the various areas of responsibility conducted searches using this guidance.

42. The records of the ICE ERO Executive Associate Director, and other ERO headquarters staff, namely the Chief of the Modernization and IT Unit, the Chief of the Firearms & Tactics Unit, the Chief of the Program Review Unit, the Chief of Policy Resource Management, the Chief of the Case Management Unit, and the ERO Chief of Staff, were also searched by ICE ERO front office staff using the "How to Search for Opt-Out Records" guidance.

43. Lastly, Headquarters ICE ERO staff conducted searches of the archived e-mail files of a retired ICE ERO Field Office Director. The employees that conducted the search were provided a copy of Plaintiffs' RPL and the instructions provided by the ICE FOIA Office as described in Paragraph 36, above. This employee's archived emails were searched because he retired during the identified search window and was a sufficiently high-ranking official that ICE ERO determined that his archived emails may have contained potentially responsive records.

B. ICE OPLA

44. Within ICE OPLA, a search of the OPLA Homeland Security Investigations Law Division ("HSILD") was conducted. OPLA HSILD is responsible for advising ICE's operational components about immigration and customs enforcement issues. Among other things, OPLA HSILD provides legal support during worksite enforcement operations. OPLA HSILD was searched because that office provides legal advice to ICE's operational offices during the planning and execution of the enforcement operations. Although OPLA HSILD does not typically work with Secure Communities

related issues, the division chief, who may have had some tangential contact with Secure Communities, was tasked with the search. This employee searched network shared drives, hard drives, and Microsoft Outlook e-mail files. The search terms used were "opt-out" and "opt out". The HSILD chief chose to use fewer terms because she knew the other terms were likely to produce large numbers of unresponsive documents unrelated to Secure Communities.

45. Additionally within ICE OPLA, a search of the OPLA Enforcement and Removal Operations Law Division ("EROLD") was conducted. OPLA EROLD is responsible for advising ICE's operational components about a wide variety of detention and removal issues and provides support to the Secure Communities Program Office and other program offices within ICE. EROLD maintains a division of labor that assigns programmatic areas and issues to specified attorneys within the division. Within OPLA EROLD, seven attorneys, including the chief of EROLD and a former chief of the division, conducted manual searches of paper files located in file cabinets or binders as well as electronic searches of hard drives, network shared drives, and Microsoft Outlook email files. These searches were conducted using the following keywords: "Secure Communities"; "opt-out"; "mandatory'; "voluntary"; "participation"; "opting-out"; "choosing"; "mandate"; and "opt out". These seven attorneys were identified based upon their work with the Secure Communities program office and Secure Communities related issues.

46. OPLA Legislative Counsel was also tasked with the search; two attorneys, including the chief of the section conducted manual searches of paper files located in file cabinets or binders as well as electronic searches of hard drives, network shared drives,

and Microsoft Outlook email files. These searches were conducted using the following keywords: "Secure Communities"; "opt-out"; "mandatory'; "voluntary"; "participation"; "opting-out"; "choosing"; "mandate"; and "opt out".

47. Also within ICE OPLA, senior OPLA leadership, consisting of the Principal Legal Advisor, the Deputy Principal Legal Advisor, then Director of Enforcement and Litigation, and the senior counselor to the Principal Legal Advisor also searched for documents. Electronic searches of hard drives, shared drives, and Microsoft Outlook email files were conducted using the following keywords: "Secure Communities"; "opt-out"; "mandatory'; "voluntary"; "participation"; "opting-out"; "choosing"; "mandate"; and "opt out".

48. All ICE employees within OPLA who conducted searches were given a copy of the "How to Search for Opt-Out Records" document prior to commencing their search.

C. ICE OSLTC

49. ICE OSLTC was searched because two staff members in OSLTC, the Deputy Assistant Director and a Senior Public Engagement Officer, have frequent contact with representatives of various NGOs, and the opt-out issue was likely to have come up in some of their communication. Within OSLTC, those two staff members conducted searches of their hard drives, shared drives, and Microsoft Outlook email files using the following keywords: "opt-out"; "voluntary"; and "mandatory".

D. ICE OCR

50. Within ICE OCR, the Assistant Director, both Deputy Assistant Directors, five Congressional Liaisons, one Special Assistant, one HSI Special Agent on detail to OCR, and one ERO Deportation Officer on detail to OCR conducted searches of

electronic files located on hard drives, shared drives, and Microsoft Outlook email files. Prior to beginning their search, OCR staff members were provided with search guidance listing recommended search terms. The following search terms were recommended: "opt-out"; "mandatory'; "voluntary"; "participation"; "opting-out"; "choosing"; "mandate"; and "opt out".

E. ICE OPA

51. Within ICE OPA, a manual search was conducted of paper files located in a file cabinet, as well as an electronic search of hard drives, shared drives, and Microsoft Outlook email files. The electronic searches were conducted using the following keywords: "Secure Communities"; "opt-out"; "mandatory'; "voluntary"; "participation"; "opting-out"; "choosing"; "mandate"; and "opt out". A total of 21 OPA employees searched including the public affairs officers, senior public affairs officers, and a regional communications director/spokesperson. The Director and Deputy Director of OPA both conducted searches.

F. ICE Office of the Director

52. Within ICE Office of the Director, a search of the e-mail files of the ICE Director, ICE Assistant Deputy Director, the ICE Chief of Staff, and the ICE Executive Associate Director for Management and Administration was conducted. The Deputy FOIA Officer forwarded a copy of the FOIA request to the Deputy Chief of Staff for Management and Administration, along with the names of the individuals who needed to be searched and a copy of the "How to Search for Opt-Out Records" document. The individuals tasked with the search were identified by the Office of the Director as having worked on the opt out issue. The Deputy Chief of Staff for Management and

Administration then forwarded the Deputy FOIA Officer's tasking message to the Assistant Deputy Director, the Chief of Staff, the Executive Associate Director for Management and Administration, and the Special Assistant to the ICE Director, who has access to all of the Director's email files and conducted the search on his behalf using the search terms provided in the "How to Search for Opt-Out Records" document.

53. These individuals then searched their respective archived email files[6] utilizing the search function and the search terms provided in the "How to Search for Opt-Out Records" guidance document. At the time of the Opt-Out search, staff used either the Microsoft Outlook 2003 or 2007 versions. The Office of the Director does not use a shared drive. When individuals within the office wish to share a document, they either email a copy of the document stored on their computer's hard drive, or they utilize the SharePoint system, which is managed by ICE Office of the Executive Secretariat (ExecSec).

54. In total, over 200 agency employees expended well over 1000 man hours searching for records responsive to the "opt-out" portion of the RPL.

55. In August 2011, Plaintiffs inquired about the possible existence of responsive documents within the ICE Privacy Office. The Privacy Office was not tasked with searching for documents responsive to either the RPL or the opt-out issue. The function of the ICE Privacy office is to ensure that the agency is complying with the mandates of the federal Privacy Act, 5 U.S.C. Section 522a and the DHS Privacy Policy 6 C.F.R. Part 5. ICE FOIA determined that the ICE Privacy Office would not have records responsive to Plaintiffs request based upon the subject matter. Further, following Plaintiffs' query

[6] Archived emails in this context refer to the individual archived emails that are created by each employee as described in Paragraph 14.

in August 2011, agency counsel contacted the ICE Privacy Office, which confirmed that the Privacy Office would not likely have any records that would be responsive to the Plaintiffs' FOIA request or RPL.

56. As a result of the search described above, ICE identified a total of over 100,000 pages of potentially responsive opt-out records. After review, ICE determined that 12,388 pages were responsive, and produced those pages to plaintiffs on December 6, 2010 and January 17, 2011.

57. ICE has expended thousands of man hours searching for, reviewing, and processing documents in response to this FOIA request. In addition, ICE has expended hundreds of thousands of dollars in the largest and most costly effort ever undertaken by the agency in response to a FOIA request. ICE has detailed information on these costs in previous declarations.

VI. JURAT CLAUSE

I declare under penalty of perjury that the forgoing is true and correct to the best of my knowledge and belief. Signed this 2nd day of March 2012.

Ryan Law, Deputy FOIA Officer
Freedom of Information Act Office
U.S. Department of Homeland Security
U.S. Immigration and Customs Enforcement
500 12th Street, S.W., Stop 5009
Washington, DC 20536-5009