

No. 17-16107

**In the United States Court of Appeals
for the Ninth Circuit**

WILEY GILL; JAMES PRIGOFF; TARIQ RAZAK; KHALED IBRAHIM;
AARON CONKLIN,

Plaintiffs-Appellants,

v.

DEPARTMENT OF JUSTICE; JEFF SESSIONS, Attorney General; PROGRAM
MANAGER – INFORMATION SHARING ENVIRONMENT; and
KSHEMENDRA PAUL, in his official capacity as Program Manager of the
Information Sharing Environment,

Defendants-Appellees.

**FURTHER EXCERPTS OF RECORD
Volume 1 of 1 – Pages 1-56**

On Appeal from the United States District Court
for the Northern District of California
No. 3:14-cv-03120-RS
The Honorable Richard Seeborg, District Judge

Stephen Scotch-Marmo
stephen.scotch-
marmo@morganlewis.com
Michael James Ableson
michael.ableson@morganlewis.com
MORGAN, LEWIS & BOCKIUS LLP
101 Park Avenue
New York, NY 10178
T. 212.309.6000
F. 212.309.6001

Linda Lye
llye@aclunc.org
Julia Harumi Mass
jmass@aclunc.org
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF NORTHERN
CALIFORNIA, INC.
39 Drumm Street
San Francisco, CA 94111
T. 415.921.2493
F. 415.255.8437

Attorneys for Appellants
Wiley Gill, James Prigoff, Tariq Razak, Khaled Ibrahim, and Aaron Conklin
(Additional Counsel on Inside Cover)

Mitra Ebadolahi
mebadolahi@aclusandiego.org
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF SAN DIEGO AND
IMPERIAL COUNTIES
P.O. Box 87131
San Diego, CA 92138
T. 619.232.2121
F. 619.232.0036

Peter Bibring
pbibring@aclusocal.org
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF SOUTHERN
CALIFORNIA
1313 West 8th Street
Los Angeles, CA 90017
T. 213.977.9500
F. 213.977.5299

Hugh Handeyside
hhandeyside@aclu.org
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
T. 212.549.2500
F. 212.549.2654

Jeffrey S. Raskin
jeffrey.raskin@morganlewis.com
Phillip J. Wiese
phillip.wiese@morganlewis.com
MORGAN LEWIS & BOCKIUS LLP
One Market, Spear Street Tower
San Francisco, CA 94105
T. 415.442.1000
F. 415.442.1001

Christina Sinha
christinas@advancingjustice-alc.org
ASIAN AMERICANS ADVANCING
JUSTICE – ASIAN LAW CAUCUS
55 Columbus Avenue
San Francisco, CA 94111
T. 415.848.7711
F. 415.896.1703

Attorneys for Appellants
Wiley Gill, James Prigoff, Tariq Razak, Khaled Ibrahim, and Aaron Conklin

Wiley Gill, et al. v. Dept. of Justice; Jeff Sessions, et al.
U.S. Court of Appeals Ninth Circuit No. 17-16107

Further Excerpts of Record

INDEX

Docket No.	Description	Date	Page No.
1	Privacy Impact Assessment for the eGuardian Threat Tracking Systems (Exhibit 5 to Complaint filed 07/10/2014)	11/25/2008	1-26
28	Defendants' Reply in Support of Motion to Dismiss (<i>excerpts</i>)	12/11/2014	27-34
71	Further Supplemental Joint Case Management Statement	09/04/2015	35-49
72	Order Referring Issues to Magistrate Judge and Continuing Further Case Management Conference; denying request to propound jurisdictional discovery	09/08/2015	50-51
113	Defendants' Notice of Motion for Summary Judgment and Memorandum in Support (<i>excerpts</i>)	08/18/2016	52-56

Exhibit E



**Privacy Impact Assessment
for the
eGuardian Threat Tracking System**

Responsible Officials

Counterterrorism Division

Program Manager

[Redacted]

Threat Monitoring Unit (TMU)

[Redacted]

System Developer

[Redacted]

Foreign Terrorist Tracking Task Force (FTTF)

[Redacted]

Reviewing Officials

[Redacted]

Chief Privacy and Civil Liberties Officer

Federal Bureau of Investigation

[Redacted]

Chief Information Officer

Department of Justice

Approving Official

[Redacted]

Acting Chief Privacy Officer and Civil Liberties Officer

Department of Justice

b6
b7C

November 25, 2008

ACLUEG000047

FINAL

INTRODUCTION

Overview

The National Threat Center Section (NTCS) in the FBI's Counterterrorism Division is the focal point for all threat information, preliminary analysis, and assignment for immediate action of all emerging International Terrorism and Domestic Terrorism threats incoming to the FBI. Within NTCS, the Threat Monitoring Unit (TMU) has the primary responsibility for supporting the FBI's role in defending the United States against terrorism threats. Through coordination with FBI Field Offices, Legal Attaches, and other government agencies, TMU collects, assesses, disseminates, and memorializes all threat information collected or received by the FBI. A companion unit to TMU, the Threat Review Unit (TRU), analyzes the threat information that is collected in order to identify trends and prepares informational products that can be shared.

To help it accomplish its work, in 2003, TMU developed the Guardian Program.¹ Guardian is an information technology system maintained at the Secret level that allows TMU to collect suspicious activity reports (SARs) made to the FBI and review the SARs in an organized way to determine which ones warrant additional investigative follow-up. Guardian's primary purpose is not to manage cases, but to facilitate the reporting, tracking, and management of threats to determine within a short time span (30 days or less) whether a particular matter should be closed or referred for an investigation. Guardian also facilitates the TRU's work in performing its analytical functions because the reports are available for pattern and trend analysis.

Handwritten initials: "DL 24" with a checkmark.

Because of the mandate, expressed in the Intelligence Reform and Terrorism Prevention Act as well as in other statutes and Executive Orders and in the National Strategy for Combating Terrorism, to share terrorism information with other federal, and state, local and tribal (SLT) law enforcement partners, the FBI now proposes to create an unclassified version of its Guardian Program - called eGuardian - that will provide participating partners with access to a reporting system to be hosted on a secure but unclassified Internet network that will be accessed through Law Enforcement Online (LEO). The SARs that are contributed to eGuardian, after initial approval, will be accessible to specially-vetted representatives of other federal law enforcement partners and SLT law enforcement partners. These SARs should help facilitate situational awareness with respect to potential terrorism threats. Sharing these reports should eliminate the jurisdictional and bureaucratic impediments that otherwise delay communication of this important information that is necessary to enhance our national security posture.

Information Sources

The threat information to be contributed to eGuardian may come from three sources: (1) unclassified information from the FBI's Guardian system; (2) reports from other federal agencies with law enforcement functions, including components of the

¹ The Guardian Program was the subject of a Privacy Impact Assessment dated April 13, 2005.

Department of Homeland Security² and law enforcement investigative services within the Department of Defense,³ and (3) SARs contributed by SLT law enforcement.

Unclassified information from the Guardian system that appears to have a potential nexus to terrorism will be passed down to eGuardian, where it will be available for viewing by the participants of eGuardian, including those members of SLT law enforcement and representatives of other federal law enforcement agencies that have been given permission to access the eGuardian system.

For the information coming from other federal agencies with law enforcement functions, including FBI unclassified reporting passed through Guardian Express, TMU will conduct the initial screening of federal suspicious activity reports, other than reports by law enforcement investigative services within DoD. Suspicious activity reports from law enforcement investigative services within DoD will be analyzed in a DoD fusion center-like organization for a further determination whether the information warrants contribution to eGuardian (labeled as the Shared Data Repository (SDR) on Diagram 1.a) and then on into Guardian.

Suspicious Activity Reports from SLT partners will be submitted to the appropriate State or Local Fusion Center for a similar analysis there. If the Fusion Center accepts a report as demonstrating a potential nexus to terrorism, it will be submitted to the SDR and then on into Guardian for the FBI to analyze further to determine if investigative action at the Federal level is warranted. Additionally, once the report is in the SDR, it will be available for viewing by the participants of eGuardian.

From each of these sources, those reports that appear to have a potential nexus to terrorism will be added to the Guardian system for further analysis. Incidents and threats that are found to warrant investigation will be assigned, via Guardian, to a member of one of the FBI's Joint Terrorism Task Forces (JTTFs). Nationwide, all 56 FBI field divisions maintain at least one JTTF. The JTTFs are comprised of SLT law enforcement officers who are deputized as federal agents, as well as law enforcement agents from other federal agencies, including the Department of Homeland Security and the Department of Defense. The JTTFs have the primary responsibility for investigating terrorist threats, events, and suspicious activities with a potential nexus to terrorism.

The eGuardian system will be used to record, review, sort, and prioritize these counterterrorism threats and suspicious activity incidents and present the information to law enforcement partners who will access the eGuardian SDR through a Special Interest Group accessed through LEO. Law enforcement agencies that have contributed information will have read and write access to their reports in the SDR in order to update them as necessary. Other law enforcement partners will have read-only access to the

² These include the Federal Air Marshals Service, Immigration and Customs Enforcement, Customs and Border Protection, and the United States Coast Guard.

³ These include the Army Criminal Investigation Command (CID), the Naval Criminal Investigative Service, and the Air Force Office of Special Investigations. Other DOD components with force protection law enforcement arrest authority may also participate in eGuardian, such as the Pentagon Force Protection Agency.

SDR to ensure appropriate dissemination of these counterterrorism threats and suspicious activity incidents.

Review Process

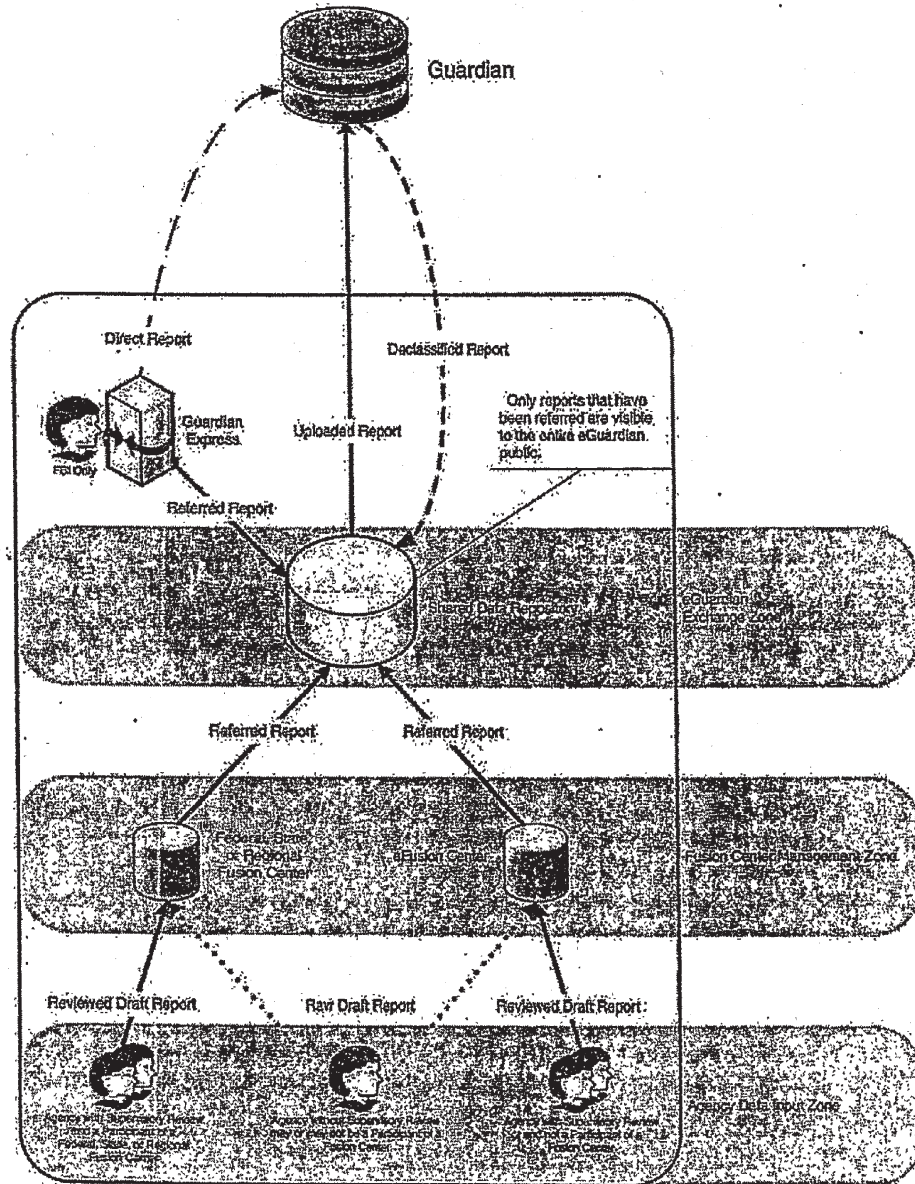
Throughout the initial threat reporting process, regardless of where the report originates, if a determination is made of "no nexus to terrorism," the information will not be added to the eGuardian SDR. Additionally, at the Fusion Center level, the information will be deleted. If a clear determination is made of "a nexus to terrorism," the information will be passed along to the eGuardian SDR for further dissemination and then on to Guardian for analysis. If no determination can be made regarding "a nexus to terrorism," but neither can the nexus be discounted, the information will be added to the eGuardian SDR for pattern and trend analysis.

In keeping with the retention period currently in effect for state criminal intelligence systems under 28 C.F.R. Part 23, suspicious activity reports in this third category (reports for which a determination cannot be made whether or not a nexus to terrorism exists) will be retained for a period of five years and will be used for analytical purposes and/or to demonstrate trends. eGuardian considers all reports submitted to the system to be the property of the submitting agency; therefore, should a submitting agency desire that a report be removed from the system prior to the five-year mark, the report will be removed. Otherwise these reports also can be available for trend and other analyses.

User Access/Security

The eGuardian system will ensure consistency of process and of handling protocols by using a uniform user agreement for each agency or law enforcement entity that connects to eGuardian through LEO. By signing the user agreement, the parties will agree to the Fusion Center or TMU policies, which reflect the conditions of use and privacy and security requirements of eGuardian. All users will be required to assent to these rules of behavior each time they log on to the system. Additionally, all users will be required to complete robust system training that will incorporate eGuardian policies and procedures concerning privacy and civil liberties. Audit controls will be employed to ensure that the use of eGuardian is consistent with its intended purpose.

The following diagram (Diagram 1a) provides an overview of the eGuardian system described in this Privacy Impact Assessment. Data is input at an initial level but reviewed at a Fusion Center or similar entity before being passed to eGuardian if the information appears to be linked to terrorism. The "Agency Data Input Zone" represents law enforcement contributors of suspicious activity reports with a potential nexus to terrorism. The Fusion Center Management Zone represents the vetting that must occur before these reports are shared with eGuardian participants. The eGuardian Exchange Zone is where this information sharing will actually occur, once a determination has been made that the report has a potential nexus to terrorism. The FBI's role is to serve as both a contributor of information from its Guardian system and a recipient of eGuardian reports that warrant additional investigation at the Federal level.



e-Guardian System
Internal Data Flows
Diagram 1a

Section 1.0

The System and the Information Collected and Stored within the System

1.1 What information is to be collected?

eGuardian will collect terrorism threat information and/or suspicious activity information having a potential nexus to terrorism. "Suspicious activity" is defined as observed behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal or other illicit intention. This definition is consistent with the definition utilized by the Program Manager/Information Sharing Environment (PM/ISE). Suspicious activities may include surveillance, cyber attacks, probing of security and photography of key infrastructure facilities. Personally identifiable information (PII) to be collected will include all available identifiers regarding the subject of a report or incident, such as name, date and place of birth, unique identifying numbers, physical description, and similar attributes.

1.2 From whom is the information collected?

Suspicious activity reports and threats that have a potential nexus to terrorism may be reported to law enforcement from private citizens or may come directly from law enforcement personnel who observe or investigate activities.

1.3 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

FBI suspicious activity reports that are entered into eGuardian at the federal level will have been analyzed initially by TMU to determine whether sufficient facts exist to warrant placement of the information into the system. Suspicious activity reports from SLP law enforcement and other federal agencies will be required to pass through a Fusion Center or similar analytical construct prior to being passed to eGuardian. In all cases of data ingest, trained analysts or law enforcement personnel will make the judgment that the information rises sufficiently to the level that a report should be added to eGuardian.

eGuardian users will be advised in an online tutorial that frequent checking of the database for updates will be necessary, at intervals no less than 30 days, and will be encouraged to ensure that information they have entered initially is supplemented whenever new facts are uncovered. In the work flow that is created for eGuardian, contributors will be able to add notes that help clarify the contributed information.

eGuardian has developed a set of guidelines for the types of information that cannot be entered into the system by any participating entity, including the FBI. For example, no entry may be made into eGuardian based solely on the ethnicity, race or religion of an individual or solely on the exercise of rights guaranteed by the First Amendment or the lawful exercise of any other rights secured by the Constitution or the laws of the United States. These restrictions will be prominently displayed when an

Handwritten initials: "R-27"

individual accesses eGuardian and he or she will have to affirmatively indicate agreement to abide by these rules before being permitted to proceed to view reports.

In addition, the following specific categories of information will not be permitted to be entered into eGuardian: classified information; information that divulges sensitive methods and techniques; FISA-derived information; grand jury information; federal taxpayer information; sealed indictments; sealed court proceedings; confidential human source and witness information; Title III subject and intercept information; and other information that is subject to legal restriction. The eGuardian Program Manager will have personnel assigned to monitor the system to ensure that these categories of information are not included in eGuardian reports.

All information will be subject to threshold screening by the submitting law enforcement officer before being placed in the system and then will be submitted to a Fusion Center, to TMU or to the DOD fusion center-like organization [hereinafter collectively referred to as a "responsible entity"] within the Fusion Center Management Zone (see Diagram 1a) for a decision regarding adding the report to eGuardian. This screening will ensure that trained law enforcement personnel and/or analysts make the initial decision that a report warrants further review. Furthermore, the eGuardian workflow architecture is designed to restrict the ability to view submitted reports to the reporter, the reporter's supervisor, and the approving responsible entity. Incidents submitted to eGuardian will not be viewable to the eGuardian users outside this workflow until the report is approved at the responsible entity level.

Section 2.0

The Purpose of the System and the Information Collected and Stored within the System.

2.1. Why is the information being collected?

The National Strategy for Combating Terrorism recognizes that the war on terror requires greater flexibility and resilience to confront threats facing our nation from a transnational terrorism movement designed to destroy our way of life. The collection of information in eGuardian is consistent with this national strategy and also with the emphasis placed by the President and the Congress on sharing terrorism information with our law enforcement partners. It also recognizes that the police officer on the street is often in the best position to observe suspicious behavior that may have national security implications. eGuardian and Guardian provide a dynamic tool to accomplish this sharing to increase awareness and foster review of threats and suspicious activities in a timely manner so that they can be mitigated appropriately. It is also very important to note that eGuardian is at its very essence, simply a platform to standardize the disparate SAR systems currently utilized by agencies to collect information, which will enhance communication among law enforcement entities as well as situational awareness.

2.2 What specific legal authorities, arrangements, and /or agreements authorize the collection of information?

The FBI's general investigative authority in 28 U.S.C. 533 and its general authority to collect records in 28 U.S.C. 534 provide the statutory basis for the activities ascribed to eGuardian. The FBI is also assigned the lead role in investigating terrorism and in the collection of terrorism threat information within the United States by 28 C.F.R. § 0.85 and Annex II to National Security Presidential Directive 46. In addition, the Intelligence Reform and Terrorism Prevention Act requires the President to establish an information sharing environment for sharing terrorism information in a manner that is consistent with national security and applicable legal standards pertaining to privacy and civil liberties. Further, the President's National Strategy for Information Sharing supports the eGuardian initiative; it identifies suspicious activity reporting as one of the key information exchanges between the Federal Government and State and local partners.

2.3 Privacy Impact Analysis: Given the amount and type of information collected, as well as the purpose, discuss what privacy risks were identified and how they were mitigated.

The most significant privacy risk is that information which first appears to be suspicious will turn out, upon further vetting, to be innocuous, resulting in the over collection of data. A related significant risk is that dissemination of personal information will be overly broad and will include agency officials who have no need to know the information. Both risks are mitigated in several ways.

First, a standard definition of what constitutes a suspicious activity will be used by all participating agencies. As mentioned previously, the suspicious activity definition will be the definition currently developed by the PM/ISE. The PM/ISE suspicious activity definition will be augmented by describing the kinds of information that cannot be entered into the system. The definition with these qualifiers will be incorporated into the User Agreement that appears on the LEO eGuardian Special Interest Group page where eGuardian incidents will be placed and individuals accessing the system will have to confirm that they have read and understand the Agreement and agree to be bound by the constraints articulated therein.

Second, eGuardian is intended to function as an alert, recording and reporting system and not as a long-term data repository. As a result, decisions about SARs will be made promptly so that the data can move quickly through the system. All SLT and federal law enforcement agencies with missions that pertain to homeland security will be encouraged to enter terrorism-related threats and suspicious activity incidents into eGuardian for an appraisal by the appropriate Fusion Center, the FBI's TMU or the DOD equivalent.

In general, Fusion Centers are becoming the focal points for information sharing and will function as an additional layer of review to confirm that the incident warrants treatment as suspicious or potentially connected to terrorism. With the proper training of personnel who perform system management and analytical functions (as discussed elsewhere in this assessment), the use of Fusion Centers as an intermediary should lead to

an effective and standardized vetting process that moves reports quickly through the eGuardian system. There will be vigorous efforts to police eGuardian and eliminate irrelevant, erroneous or otherwise improper reporting. Suspicious activity, incidents and threats that are found to warrant investigation due to a likelihood of having a potential terrorism nexus will be assigned to a member of the FBI's Joint Terrorism Task Forces (JTTFs).

Within the eGuardian system, suspicious activity reports that appear to have a potential nexus to terrorism will be entered by the FBI or a law enforcement partner into the eGuardian system where a record will be created to summarize the nature of the incident for subsequent analytical assessment. The assessment is intended to take place within no more than 30 days and result in one of the following dispositions:

1. **DRAFT** – threat or report of suspicious activity is reported to the agency reporting space (see Diagram 1a for information flow from Agency Data Input Zone to Fusion Center Management Zone) eGuardian system by an authorized user;
2. **REFERRED** – a threat or report of suspicious activity has been referred to the SDR of eGuardian (see Diagram 1a for information flow from Fusion Center Management Zone to eGuardian Exchange Zone) and uploaded to eGuardian for further assessment by a FBI/JTTF investigator; or
3. **CLOSED** – a threat or report of suspicious activity has been reviewed and found to have no nexus to terrorism.

The eGuardian system handles Draft reports in two ways depending on where in the eGuardian workflow the draft exists and how the agency has configured their agency eGuardian workflow. When an agency creates (enters) a suspicious activity report in the eGuardian system, the report is only visible to the eGuardian account holders from that agency. At this point the report is considered to be at agency-level control (see Diagram 1a, Agency Data Input Zone). The report cannot be seen by the Fusion Center responsible for the agency nor can it be seen by the FBI or any other law enforcement agency (LEO, eGuardian Special Interest Group). This design enhances privacy protection by restricting access to PII to the agency that created the report. This design function also allows the agency complete control over information they enter into eGuardian.

At the Agency Data Input Zone, the agency reporter or the agency supervisor (if applicable) may elect to retain the information with the eGuardian system pursuant to their agency policy, but for no more than five years. The agency makes the determination whether to share the report by submitting it to their responsible Fusion Center or the TMU, if the agency does not participate in a Fusion Center. The agency may also decide to close the report. If the agency closes the report at the agency level, neither the Fusion Center nor the FBI nor any other agency will ever see the report. If the agency elects to submit the incident to the appropriate Fusion Center, the report continues to remain in draft status and becomes viewable only by the responsible Fusion Center and the FBI. The Draft report is not yet viewable to other law enforcement partners. At the Fusion Center Management Zone (see Diagram 1a), the draft report will be analyzed in an attempt to identify a potential nexus to terrorism.

As noted above, if the Draft report is determined to have no nexus to terrorism, the Draft report will be closed by the Fusion Center and will not be made available for viewing by any other law enforcement partner. Furthermore, closed Draft reports that are determined to have no nexus to terrorism will be deleted from the eGuardian system.

Draft reports in which a threat or report of suspicious activity is indeed found by the appropriate Fusion Center, including the FBI's TMU or DOD equivalent, to have a potential nexus to terrorism are passed to the eGuardian SDR in the eGuardian Exchange Zone and loaded into Guardian. The copy of the report retained in eGuardian will have its status changed from Draft to Referred. At this point the report will be viewable to other law enforcement partners that are members of the LEO eGuardian Special Interest Group. Also, as noted above, if a nexus to terrorism can neither be substantiated nor discounted, the Referred report is determined to be inconclusive, marked as such, and then referred to Guardian for further assessment by the JTTF. Again, at this point, the Referred report will be viewable to other law enforcement agencies with eGuardian accounts. The report will continue to remain in the eGuardian system for tracking and further analytic review. The information in these reports — where a nexus to terrorism is inconclusive or a nexus to terrorism has been substantiated — will be maintained for five years.

This illustrates that the eGuardian workflows heavily restrict information while in "Draft" stage. Reports are only accessible to the eGuardian user community after a potential terrorism nexus is identified or the report is found to be inconclusive in which case the report remains in eGuardian and is referred to Guardian for additional assessment and/or investigation. Likewise, inconclusive reports may later be closed and deleted if, after subsequent analytical evaluation or the passage of time, the report is found to be erroneous, irrelevant or later determined to have no nexus to terrorism.

In addition, in terms of access to the system, the eGuardian user community will consist of only those law enforcement partners who qualify for access to LEO and who are specifically granted access to the eGuardian SIG by TMU.

Other ways that the privacy risk presented by this system is mitigated is through the use of technology. eGuardian will have the ability to conduct data optimization which will identify and eliminate duplicate data objects. This will improve the quality of the data. The system will also be able to provide data segmentation so that disparate rules of SLT law enforcement and federal agencies for limiting collection and access can be implemented. In other words, different rules regarding retention and use that are required by state laws can be incorporated as attributes of the contributed data. Finally, as noted above, the retention period for eGuardian reports generally will be relatively short (5 years) in an effort to balance the need to retain information long enough to discern potential terrorism planning activities but short enough to protect the privacy of individuals whose information is maintained.

Section 3.0 Uses of the System and the Information

3.1 Describe all uses of the information.

eGuardian is first and foremost a reporting system that standardizes existing reporting. Reports will be placed into eGuardian to assist in assessing terrorism-related threats and suspicious activities. In addition, the information derived from the reports that are placed in eGuardian may show links, relationships, and matches among data elements, which will provide the opportunity for analysis and interpretation. The use of the tools in eGuardian will enable analysts, officers, detectives, agents, and other law enforcement investigators to develop leads and identify potential suspects more quickly. Once vetted by a responsible entity, this information will be shared with law enforcement at all levels in order to more effectively identify threats and threat patterns and take actions to mitigate such threats.

3.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern? (Sometimes referred to as data mining.)

The eGuardian system will contain an analytical functionality to find potential links and patterns between terrorism suspects and suspicious events. Rather than facilitating the search for anomalies based on patterns, however, the point of the system is to collect reports about activities that may be linked to terrorism and then to refer the information for further investigation as necessary and to analyze it for potential linkages that can enhance the ability of the FBI and other law enforcement agencies to take preventative action. There is no capability to use eGuardian for pattern-based data mining as described in section 804 of the Implementing Recommendations of the 9/11 Commission Act of 2007. Should that capability be added and exploited for pattern-based data mining, this assessment will be updated and the activity will be reported to Congress as required by the Act.

3.3 How will the information collected from individuals or derived from the system, including the system itself, be checked for accuracy?

The data will be collected in accordance with procedures established by the respective agencies' policies for collecting data related to suspicious activities that may pertain to terrorism. The information will then be examined by trained investigators for accuracy and authenticity. The system itself will be able to identify duplicate data items and all records will be date and time-stamped. Information that is forwarded to Fusion Centers from SLT law enforcement partners will be subject to additional checks for accuracy and the integrated data available at the Fusion Centers will be utilized to help determine information that is accurate or that is suspect.

3.4 What is the retention period for the data in the system? Has the applicable retention scheduled been approved by the National Archives and Records Administration (NARA)?

e-Guardian has coordinated records retention policies with the FBI's Records Management Division. A determination has been made that information contributed by SLT and other federal agency partners remains under the control of those agencies. The reports that are maintained in the eGuardian SDR are also uploaded to the FBI's Guardian system. The retention schedule for Guardian records will therefore be applied to this information, which will be retained in that system.

As noted earlier, information entered into eGuardian will be characterized in one of three ways: initially, the reported incident will remain in "DRAFT" status until such time as the incident is approved, normally by the responsible entity. While in draft form, the incident is only viewable by the originating agency reporter, and the reporter's supervisor if applicable. If the agency reporter's supervisor decides to share the report outside the originating agency, the supervisor submits the report to the responsible Fusion Center. At this point, the report is only viewable by the reporter, the reporter's supervisor(s), the responsible Fusion Center Administrators and TMU (eFusion Center) personnel. When the incident appears to have a potential nexus to terrorism, upon approval the categorization will change to "REFERRED." Referred indicates the incident has been electronically forwarded, or referred, to the FBI JTF/Guardian squad for further investigative assessment. If a nexus to terrorism can neither be substantiated nor discounted, the incident remains as "REFERRED," and it will stay in the system for tracking and analytic review. If no nexus to terrorism is established for a particular incident, it will be deleted from the eGuardian system.

3.5 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

26
Access to eGuardian will be available through a secure interface to Law Enforcement Online (LEO). LEO, which is a sensitive but unclassified and for authorized use only secure web-based network containing only authorized membership, will provide authentication services for eGuardian users. Each individual LEO user is issued and required to use a login and password that is unique to that user. Passwords must be changed every 90 days. eGuardian will be accessed through a Special Interest Group (SIG) on LEO. Membership in the SIG is by application only and will be drawn only from agencies that have an originating agency identifier (ORI) and thus are recognized law enforcement entities. Membership must also be approved by TMU. In the event an agency with an operational need to share/receive information does not have an ORI, one will be created for that agency by the eGuardian developers/programmers provided appropriate criteria are met. The use of an ORI designation will help to ensure that only those law enforcement personnel who have been cleared for access actually

* Information that suggests possible criminal activity may be referred to the appropriate division in the FBI. See section 4.2 below.

have it. Furthermore, members of the SIG will have to agree to a User Agreement each time they log in to eGuardian that dictates how information in the system is to be ingested, maintained and disseminated. The User Agreement will counsel that recorded information should be accurate to the extent possible, timely and relevant to a suspicious activity with a potential nexus to terrorism. Users will be cautioned not to enter information that describes First Amendment protected activities or personal information based solely on ethnicity, race or religion. SIG users' activities while online will be tracked and available for audit so that these rules can be enforced.

Other safeguards to ensure compliance with proper use rules include the limited exposure and non-retention for incidents that do not clear Fusion Center vetting; the retention and deletion controls enforced by the eGuardian system administrator; and the ability to audit and trace user identification if improper use is discovered.

Section 4

Internal Sharing and Disclosure of Information within the System.

4.1 With which internal components of the Department is the information shared?

Other DOJ components, including but not limited to the criminal components of the Department of Justice will be provided access to eGuardian if they have an operational need to know the potential terrorism information that the system contains. To the extent that information is received by TMU that pertains to potential criminal offenses with no apparent nexus to terrorism, and thus it is not appropriate for entry into eGuardian, it may be shared or forwarded to the appropriate division within the FBI or within the Department of Justice for further handling. While the information will not reside in eGuardian, referral of information about potential criminal offenses is consistent with current FBI.

4.2 For each recipient component or office, what information is shared and for what purpose?

Information with a potential nexus to terrorism will be shared with other DOJ components that have an operational need to receive the information.

Some information that is entered into eGuardian may reflect potential criminal conduct, but not conduct that amounts to terrorism. That information will be forwarded to the FBI's Criminal Investigative Division or other responsible law enforcement agency for appropriate disposition. This is not unlike the current situation in which members of the public or law enforcement personnel report incidents that are suspicious or otherwise to an FBI Field Office and the Field Office takes action to mitigate the information - either by forwarding it to the appropriate office for disposition, using it as the basis for additional investigative activity, or closing it as reflecting no violation of law.

4.3 How is the information transmitted or disclosed?

Information will be made available electronically through the eGuardian network or through secure electronic media.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

Sharing personally identifiable information carries with it a risk of improper access and/or improper use. The Privacy Act governs the dissemination of information internally within an agency; it is appropriate when there is a need to know. Because other DOJ law enforcement components are expected to be the prime recipients of any data that is shared internally, the internal sharing that is contemplated will meet the Privacy Act requirement. Cookies, which are pieces of text stored on an agency user's computer hard disk, will be used, imbedded in the program, to track access to specific information. Also, only after the incident is approved and REFERRED to Guardian by the Fusion Center is it visible to anyone beyond the original user, the user's immediate supervisor(s), the Fusion Center, and TMU. There is also a risk of data breach from the SIG, but the security features of LEO, coupled with the ability to audit system users, should help mitigate this risk.

Section 5**External Sharing and Disclosure****5.1 With which external (non-DOJ) recipient(s) is the information shared?**

Consistent with the National Strategy for Information Sharing, vetted eGuardian information is intended to be shared with other Federal, State, local and tribal law enforcement agencies, including task force members and analytical support personnel.

5.2 What information is shared and for what purpose?

Suspicious activity or threat information having a potential nexus to terrorism will be shared with the goal of creating an efficient, near real-time mechanism for law enforcement at the State, local, tribal and federal level to share and report terrorist threat data and suspicious activity and to discern any otherwise unknown relationships among reported incidents.

5.3 How is the information transmitted or disclosed?

Information is made accessible either through eGuardian, which will be in a SIG on LEO or hard copy information may be printed and disseminated. Section 3.5 describes how information will be accessed in greater detail. The potential also exists for wireless access to the SIG. User agreements will require that information obtained through eGuardian shall not be re-disseminated without approval of a responsible entity or the originating entity.

5.4 Are there any agreements concerning the security and privacy of the data once it is shared?

By logging onto the SIG, an eGuardian user will be provided a set of behavioral rules, in addition to the standard login disclaimer about the sensitivity of the information, which will describe expectations for use of the information (see attachment 1). In addition, although law enforcement personnel with access to eGuardian are trained officials and understand the rules concerning dissemination of information, additional web-based training of users on the security and privacy requirements of the system as well as system functionality will be provided by LEO. A caveat identifying eGuardian information as Sensitive but Unclassified and For Official Use Only will be included in any dissemination. It is anticipated that these labels will be replaced by a uniform designation as a matter of federal policy; when that policy is fully implemented, the caveat in eGuardian will be amended as required.

5.5 What type of training is required for users from agencies outside DOJ prior to receiving access to the information?

As noted in the previous answer, Web-based training for all users will be required as part of the eGuardian system.

5.6 Are there any provisions in place for auditing the recipients' use of the information?

All users will have to agree to the User Agreement before being granted access, and caveats about use of eGuardian information will be part of the Agreement. Additionally, the required training for all eGuardian users will cover subsequent use of the information. eGuardian will have the capability to determine who has accessed the system and what data they have created or modified and, thereby, will be able to identify the responsible users if incidents of inappropriate use or disclosure are reported. In addition, periodic audit log reviews will be used to discover access patterns as well as indications of inappropriate access, which will lead to firm controls over users, and can also generate leads to inquire into their use of the data.

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

Access to eGuardian via LEO is controlled by the LEO network itself. Users obtain access to LEO by applying for and receiving a LEO network login and password, which is only granted to authorized law enforcement agencies. Passwords must be changed every 90 days and any information that is transmitted will meet current security standards. eGuardian will be accessible through a Special Interest Group (SIG). Membership to the eGuardian SIG is by application only. Account holders will be vetted by the applicant's agency. The agency must have an ORI signifying that it is a recognized law enforcement entity. Finally, agencies must apply for membership in the SIG and be approved by TMU. In the event an agency with an operational necessity to share/receive information does not have an ORI, one will be created for that agency by

the eGuardian developers/programmers. This security control should help mitigate the privacy risk that arises from inappropriate access to the data. In further mitigation, audit logs of search transactions will be reviewed every 180 days to check for anomalous activity. TMU will have the ability to delete user accounts at the individual or agency level. Finally, training on using eGuardian will be provided and this training will help ensure that users fully understand the User Agreement concerning dissemination of information. Given the anticipated large number of external users, the risk of misuse of the information or unauthorized access and dissemination of the information by even a trained user always exists. That risk is mitigated significantly by both the restrictions on access to and dissemination of unvetted information, as described above, as well as by the audit features noted in Section 5.6 above.

Another privacy risk is that the sum of the data entered into eGuardian may be greater than its component parts, with the result that new and different information about incidents and people alleged to be suspicious becomes apparent. This is, in significant part, the purpose of the system, but it also creates a privacy risk, as well as a risk of public misperception and possible misunderstanding. The privacy risk is that seemingly isolated incidents or observations may lead to more discovery of personal information about individuals in an effort to develop relationships (i.e., "connect the dots") between these and other incidents and observations. This risk is mitigated in part by the inherent nature of the process, i.e., in the end only meaningful relationships that affect national security will be developed and acted upon. The incidents or observations containing personal information that remain isolated or the relationships among incidents that do not develop investigative value will not lead to further action and will be retained in eGuardian for the limited time indicated above. These on-going vetting and analytical processes should minimize the risk of unwarranted and inappropriate dissemination of irrelevant personal information.

Section 6.0

Notice

- 6.1 Was any form of notice provided to the individual prior to collection of information? (If yes, please provide a copy of the notice as an appendix. A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?**

General notice concerning the FBI's collection, use and maintenance of law enforcement and intelligence information is provided through the System of Records Notice for the Central Records System (63 Fed. Reg. 8671). As noted above, that notice describes the fact that the FBI maintains computerized investigative information extracted from its own files or those of other governmental sources. Because the

collection of eGuardian information may be done in connection with law enforcement activities, no individual notice will be given.

6.2 Do individuals have an opportunity and/or right to decline to provide information?

eGuardian suspicious activity reports, in many cases, will originate from observations made by law enforcement officers and from information received from the general public. In those situations, no opportunity or right to decline information is provided. The reports that are submitted are nevertheless vetted by trained law enforcement personnel and funneled through a second review at a Fusion Center or comparable entity before being added to the system.

6.3 Do individuals have an opportunity to consent to particular uses of the information, and if so, what is the procedure by which an individual would provide such consent?

Because of the nature of the records at issue, the opportunity to consent to particular uses of the information is not provided.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

The privacy risk associated with eGuardian is the lack of notice that information about individuals is being collected, used and maintained. The FBI has published a Privacy Act System of Records Notice (SORN) for FBI's investigative records, which provides general notice regarding entities with which and situations when the FBI may share investigative records. The FBI's routine uses for its systems and its Blanket Routine Uses provide further notice of the ways in which information collected by the FBI is shared. These notices, therefore, mitigate the privacy risk. No individual notice is provided, however, because the information in this system is collected by law enforcement and personal notice is not feasible.

**Section 7.0
Individual Access and Redress**

7.1 What are the procedures which allow individuals the opportunity to seek access to or redress of their own information?

Applicable regulations found in 28 CFR Part 16, Subparts A and D, which have been issued pursuant to the Freedom of Information and Privacy Acts, govern requests for access to information in FBI files. To the extent that other federal agencies, which contribute information to eGuardian, have processes in place to govern access or redress, those processes will apply to the information contributed by these agencies. As entries into eGuardian will most often be made by state and local law enforcement officers, the

information may be retained in state and local agency records as well. Access to and opportunity to seek redress for those records is controlled by state law and procedures.

7.2 How are individuals notified of the procedures for seeking access to or amendment of their information?

28 C.F.R. 16.41 and 16.46 provide information on individual access and amendment of FBI records. Amendment of FBI records is a matter of discretion as the records are exempt from the Privacy Act amendment provisions.

7.3 If no opportunity to seek amendment is provided, are any other redress alternatives available to the individual.

See previous response.

7.4. Privacy Impact Analysis: Discuss any opportunities or procedures by which an individual can contest information contained in this system or actions taken as a result of agency reliance on information in the system.

Redress is generally not available except to the extent described in Section 7.2 above, but eGuardian is not intended to be a data repository, but a dynamic system where corrections and updates will be made as necessary during the short process of ascertaining whether a particular report merits further investigation because of a potential nexus to terrorism. If no nexus to terrorism is found, the SAR will be deleted from the system.

As a general matter, although FBI records are exempt from Privacy Act access and amendment procedures, the FBI strives to maintain accurate information and will, in its discretion, consider amendment requests.

**Section 8.0
Technical Access and Security**

8.1 Which user group(s) will have access to the system?

eGuardian access will be provided to State, local, and tribal law enforcement officers and agencies that have a law enforcement mission need for suspicious activity reports. Other federal law enforcement entities, including Department of Justice components, DHS and DoD entities with law enforcement missions, including force protection, will be provided access.

8.2 Will contractors to the Department have access to the system? If so, please submit a copy of the contract describing their role with this PIA.

Contractors will have access to the system in order to perform system maintenance and administration. In addition, to the extent contractors are assigned to any

5

of the agencies that will have access to eGuardian, these individuals will also, upon proper vetting and clearances, be able to access the system.

8.3 Does the system use "roles" to assign privileges to users of the system?

Yes. eGuardian will have the following user roles:

1. Police Officer/Investigator/Intelligence Analyst/Support Contractor. These roles are generally reserved for individuals who create eGuardian incidents and are responsible for investigating and/or conducting analysis of terrorist-related threats and suspicious activity reports entered into the system. This role may include, at the discretion of the agency, an agency eGuardian supervisor who will control all eGuardian report dissemination from their agency. All such work will be electronically submitted to a coordinator at a responsible entity for review and authorization to be submitted into Guardian.
2. Coordinator/Administrator: The individual(s) assigned to this role works within the responsible entity to evaluate the information in eGuardian and performs other administrative functions with respect to the system. Individuals with this role have the ability to refer incidents to Guardian.
3. TMU will have overall administrative oversight of eGuardian and the capacity to monitor user roles assigned to each participating agency. Responsible entities will also exercise administrative oversight of users at their locations. With each participating agency, however, the determination of roles will be made locally.

8.4 What procedures are in place to determine which users may access the system and are they documented?

eGuardian will have restricted access and will follow a process regulated by TMU and by LEO. Prospective users must first clear the vetting requirements imposed by the LEO network, which include demonstrating that a proposed user is a member of an authorized law enforcement agency that is assigned an ORI or an agency with an operational necessity to share/receive information. In the event an agency with an operational necessity does not have an ORI, one will be created for that agency by the eGuardian developers/programmers, if appropriate. LEO revalidates all users' agency affiliation twice a year. Additionally, access to the eGuardian SIC will be controlled by TMU, which must approve all users. The procedures for system access are documented in policy and procedure documents developed by TMU for the eGuardian system.

8.5 How are the actual assignments of roles and rules verified, according to established security and auditing procedures?

Individual member agencies will be able to structure user roles and customize the work flow to fit their own needs. The responsible entities, however, will exercise administrative oversight of the system, which will include auditing for appropriate system access and use.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

Each user will have an individual account that requires a login and password for LEO. These accounts will be auditable. Each responsible entity, moreover, will have the responsibility to audit their users and will be obligated to report suspected misuse and security compromise. Rules of Behavior and training will cover the appropriate use of data and the penalties for misusing the information.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

As indicated previously, web-based training will be available to the user to assist with system access and procedure. In addition, eGuardian administrators from responsible entities will be provided classroom training that will emphasize their roles and responsibilities. A privacy statement will also be contained in the user agreement electronically signed by each participating agency.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification and Accreditation last completed?

The Certification and Accreditation of the system is expected to be completed in early July and an Authority to Operate will be issued at that time.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and how were they mitigated?

Privacy risks from this type of system stem from improper access and inadequate security. These risks have been mitigated in several ways: eGuardian access is based on role and function. In order to access the system, users must be sworn law enforcement officers or support personnel assigned to perform law enforcement analysis and/or criminal intelligence, as evidenced by an ORI. All users are vetted through LEO before they are permitted entry into the eGuardian Special Interest Group. Web-based training will be available to the user to assist with system access and procedures and the use of the information contained therein, with emphasis on privacy controls. Once an individual is vetted and authenticated through LEO, and then granted access to the eGuardian SIG, the individual's web-based session is controlled with computer software and hardware components secured behind accredited FBI security infrastructure. Placing eGuardian behind the FBI firewall and under the oversight of TMU will improve the security posture of the system.

Section 9.0 Technology

9.1 Were competing technologies evaluated to assess and compare their ability to effectively achieve system goals?

Yes. Several systems were reviewed and evaluated including an in-house solution. Final system design was based on operational imperatives and privacy and security attributes.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

Data integrity, privacy and security were important considerations in the development of this system. The task was to develop a robust information sharing system that would serve the needs of users for timely, relevant and accurate information in a secure environment while protecting privacy and ensuring data integrity and security. The system is designed to help investigators become aware of and make connections between reports of suspicious activities and terrorism threats in order to improve the security posture of the United States. Operationally the goal is to either close or refer for enhanced investigation all leads within a short period of time.

eGuardian is built upon and incorporates the lessons learned from the Guardian system and is designed to seamlessly interface with it. To enhance privacy protections for information that is added by SLT law enforcement personnel, a decision was made to use Fusion Centers as initial vetting points, as these groups can bring to bear enhanced information availability to ensure that suspicious activity reports and reports of incidents that have a potential nexus to terrorism meet a required threshold for system inclusion. TMU and a DOD fusion-like center will perform the same type of "fusion" for reports from federal entities. System functionality is designed to permit contributors to modify their entries as new information is received, and the need to check the system for updates will be incorporated as part of the required training for all users.

The eGuardian system was placed on an FBI server to enhance security and membership in the Special Interest Group of eGuardian users will be vetted through LEO, which performs this function for a variety of other law enforcement entities. User access will also be audited by TMU personnel.

9.3 What design choices were made to enhance privacy?

The eGuardian system is set up so that participating agencies can restrict the information they contribute in order to deny access to certain groups or individuals. This choice takes into account various state laws which have differing privacy requirements for sharing information and also allows contributors more control over their own information. A decision was also made to control access to reports in eGuardian to sworn law enforcement and analytical support personnel in order to ensure that those with training in handling sensitive law enforcement and terrorism-related information are the only ones who can access the system. The decision was made to use LEO as the hosting organization because it is an FBI-owned, web-based, sensitive but unclassified network.

that provides controlled access to facilitate information sharing. Placement of eGuardian on the Internet allows for ease of use but potentially exposes personally identifiable information to outside attack. LEO provides a restricted and more secure access to this information, which will enhance both privacy and security.

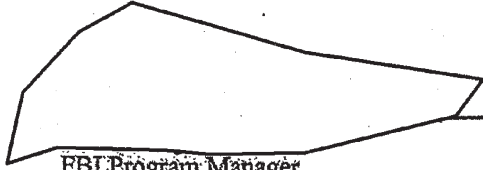

The work flow was created with privacy in mind so that contributors can easily update their information or mark it with a commentary to let other viewers know of particular issues pertaining to data integrity or privacy. Any re-dissemination of information will be subject to permission controls of the responsible or originating entity.



Conclusion

The eGuardian threat tracking system supports the FBI mission to prevent terrorist attacks on the United States. It is designed to mitigate and vet all threats and suspicious activities with a potential nexus to terrorism and assure they are properly addressed and available for trend analysis. Establishing an electronic system that will allow SLT and federal law enforcement partners to enter terrorist threat information and suspicious activity reports with a possible nexus to terrorism and share it with each other will facilitate the type of information sharing envisioned in the National Strategy for Information Sharing.


eGuardian has been designed in consultation with legal, privacy and security personnel in the FBI and elsewhere in order to ensure that privacy protections and security controls are integrated into system development and functionality. This privacy impact assessment is part of the process of ensuring that the system accounts for privacy concerns while creating an electronic environment that will facilitate operational imperatives.


Responsible Officials:

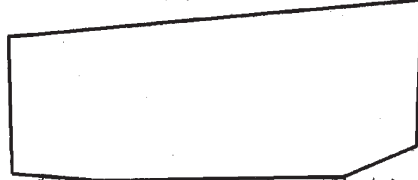
 _____ 11/25/2008
 Date
 FBI Program Manager
 Threat Monitoring Unit (TMU)
 Federal Bureau of Investigation


 _____ 11/25/2008
 Date
 FBI System Developer
 Foreign Terrorist Tracking Task Force (FTTF)
 Federal Bureau of Investigation


b6
b7c

 _____ 9/25/2008
 Date
 Chief Privacy and Civil Liberties Officer
 Federal Bureau of Investigation

 _____ 1/7/2009
 Date
 Chief Information Officer
 Department of Justice

 _____ 11/25/2008
 Date
 Acting Chief Privacy and Civil Liberties Officer
 Department of Justice

Attachment 1



eGuardian User Agreement

Contact your local Joint Terrorism Task Force (JTTF) immediately by phone for any urgent matters with a potential nexus to terrorism.

eGuardian is a sensitive but unclassified system for official use only. Information classified CONFIDENTIAL and above cannot be placed into eGuardian under any circumstances. This includes all information that is SECRET, TOP SECRET OR COMPARTMENTED. Neither FISA-derived information nor Grand Jury 6(e) material nor any other information that is legally restricted may be placed into eGuardian.

The suspicious activities contained in eGuardian may be raw and unvetted data. "Suspicious activity is defined by the Program Manager of the Information Sharing Environment (PM/ISE) as observed behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal or other illicit intention. Suspicious activities may include, but are not limited to, surveillance, cyber attacks, probing of security and photography of key infrastructures and facilities. Do not conduct any unilateral investigation with any reported incident without the coordination of the originating agency/author. Do not arrest any individual based solely on the information in eGuardian unless there is evidence of a violation of State, Local or Federal statutes.

By signing the user agreement, the parties will agree to the Fusion Center and TMU policy that sets forth the mission, goals, functions, management, principles, membership, staffing, information sharing policies and protocols and privacy and security attributes of the eGuardian system.

Membership in the SIG is by application only and will be drawn only from agencies that have an originating agency identifier (ORI) and thus are recognized law enforcement entities.

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

If you determine that information you have previously submitted is erroneous, you are responsible for updating or correcting the information in eGuardian. If you discover information that has been contributed that you know is erroneous, you should notify the submitter so that the information can be corrected.

Proceeding to the eGuardian Threat Tracking System indicates you have been informed of, agree to, and will abide by these restrictions. Incidents not meeting the criteria of suspicious activities or with a potential nexus to terrorism and that, further, do not comply with the above-stated rules, will be immediately deleted from eGuardian. Furthermore, by clicking on the User Agreement check box, you agree to the policies that govern the eGuardian system. For further information about the eGuardian policy, please return to the policy link on the LEO eGuardian member area page.

Information obtained through eGuardian shall not be re-disseminated without the approval of a responsible entity or the originating entity.

The TMU will conduct periodic audits of the system to ensure that the rules are followed. Failure to comply with this agreement will result in the termination of your eGuardian membership.

1 JOYCE R. BRANDA
Acting Assistant Attorney General
2 MELINDA L. HAAG
United States Attorney
3 ANTHONY J. COPPOLINO
Deputy Branch Director
4 PAUL G. FREEBORNE
Senior Trial Counsel
5 KIERAN G. GOSTIN
Trial Attorney
6
7 Civil Division, Federal Programs Branch
U.S. Department of Justice
8 P.O. Box 883
Washington, D.C. 20044
9 Telephone: (202) 353-0543
10 Facsimile: (202) 616-8460
E-mail: paul.freeborne@usdoj.gov

11 *Attorneys for Federal Defendants*

12
13 **UNITED STATES DISTRICT COURT**
14 **FOR THE NORTHERN DISTRICT OF CALIFORNIA**

15 WILEY GILL; JAMES PRIGOFF; TARIQ
16 RAZAK; KHALID IBRAHIM; and AARON
CONKLIN,

17 Plaintiffs,

18 v.

19 DEPARTMENT OF JUSTICE, *et al.*,

20
21 Defendants.
22

No. 3:14-cv-03120 (RS)

**DEFENDANTS' REPLY IN SUPPORT OF
MOTION TO DISMISS**

Hearing Date: January 8, 2015

Time: 1:30 p.m.

Ctrm: 3, 17th Floor

Judge: Hon. Richard G. Seeborg

TABLE OF CONTENTS

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

INTRODUCTION 1

ARGUMENT 2

 I. PLAINTIFFS FAIL TO ALLEGE FACTS TO ESTABLISH STANDING..... 2

 A. Plaintiffs Fail to Allege Facts of Credible, Real, and Immediate Harm 3

 1. No Credible Threat of Harm is Alleged 3

 2. Speculative and Self-Imposed Harm Is Insufficient 5

 B. Plaintiffs Have Failed to Allege Facts That Would Demonstrate the Third-Party Actions Complained of Were Caused by the Guidance Challenged. 6

 II. THE GUIDANCE CHALLENGED DOES NOT CONSTITUTE BINDING FINAL AGENCY ACTION THAT IS REVIEWABLE UNDER THE APA OR A BINDING LEGISLATIVE RULE REQUIRING NOTICE-AND-COMMENT RULEMAKING..... 7

 III. DEFENDANTS WERE NOT REQUIRED BY STATUTE OR REGULATION TO APPLY 28 C.F.R. PART 23 TO THE NSI 11

 IV. IN THE ALTERNATIVE, ALL BUT PLAINTIFF IBRAHIM’S CLAIMS SHOULD BE DISMISSED FOR LACK OF VENUE..... 15

CONCLUSION..... 15

1 Court determined that the Plaintiff had standing based “on words directly from the mouths of the
 2 relevant third parties explaining why they took actions that caused [plaintiff’s] injury.” *Id.* In
 3 contrast, Plaintiffs’ bald assertions that the guidance challenged caused local police and private
 4 security guards to undertake the actions complained of are insufficient to establish the causal
 5 nexus required to establish standing.³

6 **II. THE GUIDANCE CHALLENGED DOES NOT CONSTITUTE BINDING FINAL**
 7 **AGENCY ACTION THAT IS REVIEWABLE UNDER THE APA OR A BINDING**
 8 **LEGISLATIVE RULE REQUIRING NOTICE-AND-COMMENT RULEMAKING**

9 Even if Plaintiffs did have standing to bring this lawsuit against Defendants, the
 10 challenged guidance is not subject to the APA. The procedural requirements of the APA do not
 11 automatically apply to all actions taken by federal agencies. An agency action is only subject to
 12 judicial review if it determines the rights and obligations of relevant actors. *Bennett v. Spear*,
 13 520 U.S. 154, 178 (1997). And an agency pronouncement is only required to go through notice-
 14 and-comment rulemaking if it is an exercise of delegated legislative power to make rules that
 15 have the same legal force as statutory enactments. *Stoddard Lumber Co. v. Marshall*, 627 F.2d
 16 984, 987 (9th Cir. 1980). When the challenged agency action is the issuance of a purported rule,
 17 these doctrines largely coalesce into a single inquiry: whether the challenged agency rule
 18 establishes a binding norm with the force of law. *See Ctr. for Auto Safety v. Nat’l Highway*
 19 *Traffic Safety Admin.*, 452 F.3d 798, 806 (D.C. Cir. 2006).⁴

20 ³ Contrary to their assertions otherwise, *see* Pls. Opp. at 19–22, Plaintiffs are not left without an
 21 adequate remedy. As explained, *see* Gov. Br. at 22–23, to the extent Plaintiffs claim that they
 22 were improperly investigated by local police and private entities, a lawsuit against those third-
 23 parties under state or federal law is an adequate remedy that precludes APA review. And to the
 24 extent Plaintiffs attempt to proceed under the APA as a means to redress other hypothetical,
 25 speculative harms alleged to have resulted from the challenged guidance, *see* Pls. Opp. at 21
 26 (arguing that collection and dissemination of SAR information has resulted in injury), those
 27 harms fail to provide a basis to proceed under the APA. To proceed under the APA, Plaintiffs
 28 must allege facts demonstrating that they have been “adversely affected or aggrieved” under 5
 U.S.C. § 702, which requires a showing of, among other things, the same “injury-in-fact”
 required by standing doctrine. *Sierra Club v. Morton*, 405 U.S. 727, 733 (1972). As explained,
 Plaintiffs cannot make this showing based on the speculative, hypothetical harm alleged in the
 Complaint.

⁴ Plaintiffs’ focus on the multi-prong test articulated by the D.C. Circuit, and adopted by the
 Ninth Circuit, is misplaced. Pls. Opp. at 31–33 (citing *Am. Mining Congress v. Mine Safety &*

1 Defendants' guidance does not create any such binding norm. Plaintiffs concede that that
2 there is no requirement that any law enforcement agency participate in the NSI, and that even
3 those agencies that do elect to participate are never compelled to share information. Pls. Opp. at
4 22–23. Nonetheless, they argue that Defendants' guidance constitutes final agency action
5 because that guidance prohibits law enforcement agencies that do participate in the NSI from
6 sharing SARs that are not reasonably indicative of preoperational planning related to terrorism.
7 *Id.* While Plaintiffs are correct that Defendants' guidance indicates that NSI participants should
8 refrain from sharing SARs that do not meet the reasonably indicative standard through NSI
9 databases, this guidance does not alter the rights or obligations of these participants, and thus, is
10 not subject to the APA's requirements.

11 Unable to cite any legal requirement that law enforcement agencies comply with
12 Defendants' guidance, Plaintiffs argue that this guidance has the “practical effect” of being
13 binding because Defendants expect compliance with that guidance. *See* Pls. Opp. at 24–25.
14 However, though an expectation of immediate compliance with an agency regulation or order
15 can be an indicator of finality, *see, e.g., Ukiah Valley Med. Ctr. v. F.T.C.*, 911 F.2d 261, 264 (9th
16 Cir. 1990), the standard for whether an agency action is final still requires that the agency action
17 determine rights or obligations. Accordingly, an expectation of compliance is only significant to
18 the extent that it shows that the challenged agency action has the status of law. *F.T.C. v.*
19 *Standard Oil Co. of Cal.*, 449 U.S. 232, 239–40 (1980) (explaining that immediate compliance
20 with an agency regulation requiring prescription drug manufacturers to print certain information
21 on drug labels was expected because the regulation had the “the status of law”); *Oregon Natural*

22
23 *Health Admin.*, 995 F.2d 1106, 1112 (D.C. Cir. 1993)). That test is specifically designed to
24 determine if the interpretive-rule exemption to the APA's notice-and-comment requirements is
25 applicable. 5 U.S.C. § 553(b)(3)(A); *Am. Mining*, 995 F.2d at 1108–12. It is largely irrelevant
26 here because Defendants do not assert that the guidance interprets a pre-existing legal rule
27 governing the sharing of information by state and local law enforcement in connection with the
28 NSI. To the contrary, no such legal rule exists at all. The APA also exempts “general statements
of policy” and “rules of agency organization, procedure, or practice” from its procedural
requirements. 5 U.S.C. § 553(b)(3)(A). Assuming for argument's sake that Defendants'
guidance is a final agency action subject to APA review, these exemptions would more
appropriately be applied to analyze Defendants' guidance than the interpretive-rule exemption.

1 *Desert Ass'n v. U.S. Forest Serv.*, 465 F.3d 977, 987 (9th Cir. 2006) (“We consider whether the
2 [action] has the status of law or comparable legal force, and whether immediate compliance with
3 its terms is expected.” (quotation marks and citation omitted)); *National Ass’n of Home Builders*
4 *v. Norton*, 415 F.3d 8, 15 (D.C. Cir. 2005) (“[I]f the practical effect of the agency action is not a
5 certain change in the legal obligations of a party, the action is non-final for the purpose of
6 judicial review.”). Plaintiffs fail to point to any action by Defendants demonstrating that the
7 guidance satisfies that standard.

8 First, the language that Plaintiffs cite in the Functional Standard and Privacy Impact
9 Assessment, *see* Pls. Opp. at 24, does not demonstrate that the guidance has binding effect. The
10 term “will be used” as employed in the functional standard is not the equivalent of “shall be
11 used” and is consistent with these documents being descriptive rather than imposing an
12 obligation. Unlike in other cases where courts have found that agency guidance is binding based
13 in part on the language of that guidance, neither the Functional Standard nor the Privacy Impact
14 Assessment expressly states that compliance with the standards they describe is mandatory. *See*
15 *Bennett*, 520 U.S. at 170 (“The [biological opinion] at issue in the present case begins by
16 instructing the reader that any taking of a listed species is prohibited unless ‘such taking is in
17 compliance with this incidental take statement’ and warning that ‘[t]he measures described
18 below are nondiscretionary, and must be taken by [the Bureau].’”); *Appalachian Power Co. v.*
19 *E.P.A.*, 208 F.3d 1015, 1023 (D.C. Cir. 2000) (“[T]he entire Guidance, from beginning to end—
20 except the last paragraph—reads like a ukase. It commands, it requires, it orders, it dictates.”).
21 In addition, contrary to other instances where courts have found that agency guidance has a
22 binding legal effect based partly on the language of that guidance, there is no statute or
23 regulation providing that state and local law enforcement agencies are required to comply with
24 Defendants’ guidance or that any sanction will be imposed for a failure to comply. *See Bennett*,
25 520 U.S. at 170; *Appalachian Power*, 208 F.3d at 1017–20.⁵

26
27
28 ⁵ A comparison to 28 C.F.R. Part 23—a regulation that was issued through notice-and-comment
rulemaking—is instructive in this respect. That regulation both expressly conditions federal
funding on a grantee’s adherence to specific operating principles and imposes a monitoring

1 Second, there is no support for the proposition that training provided by Defendants to
2 state and local law enforcement is an indicator of final agency action. *See* Pls. Opp. at 24–25.
3 While such training is undertaken to achieve uniformity in the sharing of SAR information, as
4 explained in Defendants’ initial brief, an agency’s decision to encourage others to follow its
5 guidance does not amount to the imposition of a legal obligation. *See* Gov. Br. at 25.

6 Third, the existence of the eGuardian User Agreement does not transform the issuance of
7 the Privacy Impact Assessment (let alone the Functional Standard) into a final agency action
8 reviewable by this Court.⁶ That agreement, as Plaintiffs must concede, does not require law
9 enforcement agencies to participate in the NSI or compel NSI participants to share incident
10 reports. Instead, the agreement conditions a user’s ability to access eGuardian on the user
11 refraining from sharing incident reports that are not reasonably indicative of preoperational
12 planning related to terrorism through eGuardian. The agreement does not impose any other
13 sanction on an individual who fails to satisfy that condition, and NSI participants remain able to
14 share incident reports that are not reasonably indicative of preoperational planning related to
15 terrorism through channels other than eGuardian. Indeed, if the Functional Standard and Privacy
16 Impact Assessment were independently binding (as Plaintiffs contend), there would be little
17 reason to require users to enter into a voluntary agreement that they will follow Defendants’
18 guidance when using this federally managed database.⁷

19
20 program to ensure compliance. 28 C.F.R. §§ 23.30, 23.40. And a federal statute allows for the
21 imposition of significant civil penalties on any person that fails to comply with these principles.
22 42 U.S.C.A. § 3789g(d). Here, in contrast, there is no corresponding regulatory regime imposing
23 legal rights or obligations, and thus, the APA’s procedural requirements are not implicated.

24 ⁶ Plaintiffs argue that it is not necessary for them to show that the issuance of the Privacy Impact
25 Assessment is a final agency action. Pls. Opp. 23 n.14; *see also id.* at 4 n.1. However, Plaintiffs
26 do not point to any other agency pronouncement (other than a few pamphlets) through which the
27 Department of Justice (“DOJ”) supposedly issued an allegedly binding legislative rule.
28 Plaintiffs’ difficulty in identifying a document issuing a distinct standard for the dissemination of
SAR information is likely because the DOJ has never issued such a standard. Instead, as
explained in Defendants’ initial brief, *see* Gov. Br. at 10, the Privacy Impact Assessment simply
repeats the standard described by the Program Manager in the Functional Standard.

⁷ Plaintiffs also offhandedly suggest that Defendants’ guidance is reviewable because it affects
the rights of individuals whose personal information is shared in connection with the NSI. Pls.
Opp. at 24. This suggestion, however, does not add anything to the analysis. An agency action

1 Plaintiffs, moreover, have failed to cite to any authority that would justify subjecting this
2 guidance to APA review. *Bennett v. Spear*, 520 U.S. 154 (1997), on which Plaintiffs primarily
3 rely, is inapposite. In *Bennett*, the Fish and Wildlife Service issued a biological opinion
4 explaining that a project proposed by the Bureau of Reclamation was likely to harm an
5 endangered species of fish and outlining alternative actions that the Bureau of Reclamation could
6 take to avoid that negative impact. *Id.* While there was no requirement that the Bureau of
7 Reclamation proceed with its planned project, the Supreme Court held that the biological opinion
8 constituted a final agency action because it altered the legal regime to which the Bureau of
9 Reclamation was subject. *Id.* at 178. Specifically, federal regulations prohibited the Bureau of
10 Reclamation from proceeding with its project unless it complied with the conditions of the
11 opinion and provided a safe harbor to any person complying with the biological opinion from
12 otherwise applicable penalties. *Id.* at 170.

13 Defendants' guidance does not similarly alter the legal regime to which state and local
14 law enforcement agencies are subject. Unlike in *Bennett*, there are no federal regulations
15 providing that NSI participants will be deemed to be in compliance with any legal requirement if
16 they follow Defendants' guidance. Plaintiffs suggest that Defendants have granted NSI
17 participants immunity from 28 C.F.R. Part 23 by authorizing them to share reports that are
18 reasonably indicative of terrorism. Pls. Opp. at 24. But Defendants' guidance does not suggest
19 that it provides that protection and there is no federal regulation conferring immunity. In short,
20 the guidance is not subject to APA review because it does not affect the "legal rights of the
21 relevant actors" involved in the NSI process. *Bennett*, 520 U.S. at 178.

22 **III. DEFENDANTS WERE NOT REQUIRED BY STATUTE OR REGULATION TO** 23 **APPLY 28 C.F.R. PART 23 TO THE NSI**

24 The central argument on which Plaintiffs' case rests is that the reasonable suspicion
25 standard in 28 C.F.R. Part 23 applies to the NSI and that Defendants' failure to apply that
26

27
28 is only final if it fixes obligations or rights, or alters the legal regime to which regulated parties
are subject. And Defendants' guidance—which does not bind individuals—has not changed
anything in that regard.

1 December 11, 2014

Respectfully submitted,

2 JOYCE R. BRANDA
3 Acting Assistant Attorney General

4 MELINDA L. HAAG
5 United States Attorney

6 ANTHONY J. COPPOLINO
7 Deputy Branch Director

8 PAUL G. FREEBORNE
9 Senior Trial Counsel
10 Va. Bar No. 33024

11 /s/ Kieran G. Gostin
12 KIERAN G. GOSTIN
13 Trial Attorney
14 D.C. Bar. No. 1019779

15 *Attorneys for the Federal Defendants*

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

1
2
3
4 WILEY GILL, et al.,

5 *Plaintiffs,*

6 v.

7 DEPARTMENT OF JUSTICE, et al,

8 *Defendants.*
9

)
)
) No. 3:14-cv-03120-RS
)
)

) FURTHER SUPPLEMENTAL JOINT CASE
) MANAGEMENT STATEMENT
)
)

10 The Parties to the above-entitled action jointly submit this FURTHER
11 SUPPLEMENTAL JOINT CASE MANAGEMENT STATEMENT pursuant to the Court’s
12 August 25, 2015 Order (ECF No. 62), in which the Court instructed the parties to set forth a
13 proposed schedule for cross-summary judgment motions. This supplemental statement provides
14 the parties’ proposed schedules and justifications for their respective positions.

15 Plaintiffs propose that the Court set cross-motions for summary judgment for early 2016
16 to allow for motion practice related to the sufficiency of Defendants’ proffered Administrative
17 Record and for limited and targeted discovery related to the Court’s jurisdiction. Defendants
18 propose that summary judgment briefing proceed immediately. As explained below, Plaintiffs’
19 objections to the sufficiency of the administrative record can be addressed under Rule 56(d).

20 **I. Plaintiffs’ Position**

21 Plaintiffs contend that two substantial issues must be resolved before briefing on
22 summary judgment – whether the Administrative Record as to Defendant PM-ISE’s Functional
23 Standard is complete and whether Plaintiffs are entitled to seek discovery related to the Court’s
24 jurisdiction. Neither of these issues was resolved by the Court’s ruling (ECF No. 60) on
25 Plaintiffs’ motion to seek discovery related to Defendant DOJ’s Standard for suspicious activity
26 reporting. Plaintiffs are mindful that this is a case management statement and not a brief, but
27

1 respectfully submit that proceeding to briefing on summary judgment without prior resolution of
2 these two issues would severely prejudice Plaintiffs and short-circuit the meet and confer
3 process. At the same time, resolution of these issues prior to summary judgment would facilitate
4 the orderly resolution of this case.

5 As to the need to seek jurisdictional discovery, Plaintiffs bear the burden on jurisdictional
6 issues, which cannot be waived by Defendants, Defendants are in the exclusive possession of
7 facts bearing on issues they disputed at the motion to dismiss stage, Plaintiffs have a right to
8 develop a factual record sufficient to meet their burden before this Court and on appeal, and Rule
9 56(d) would not be an adequate mechanism for protecting their right to do so in this case.
10 Moreover, the parties are currently meeting and conferring over the adequacy of the
11 Administrative Record. To the extent that process does not resolve their dispute, the issue
12 should be litigated through noticed motions prior to briefing on summary judgment, so that the
13 Court has before it the whole Administrative Record.

14 **A. Procedural History**

15 The parties have disputed the propriety of discovery in this action from the outset.
16 Plaintiffs have raised the need for discovery and record development in the following three areas:
17 (1) jurisdictional issues; (2) Defendant PM-ISE's Functional Standard; and (3) Defendant DOJ's
18 Suspicious Activity Reporting ("SAR") Standard. *See* ECF No. 59 at 4-5; *see also* ECF No. 36
19 at 7-10; ECF No. 40 at 7-9.

20 On March 12, 2015, the Court held a case management conference in which Defendants
21 argued that review in this case should be limited to the Administrative Record. Plaintiffs argued
22 that discovery was needed as to the issuance of each of the two agency actions challenged in this
23 case – Defendant PM-ISE's Functional Standard and Defendant DOJ's SAR Standard. The
24 Court agreed that Defendants should file an administrative record on the PM-ISE Functional
25 Standard and invited Plaintiffs to submit a brief setting forth Plaintiffs' argument as to why
26 discovery on DOJ's SAR Standard was appropriate. At the March 2015 case management
27

1 conference, Plaintiffs also emphasized the need for discovery of facts bearing on the Court's
2 jurisdiction. *See* ECF No. 40 at 7-8; *see also* *Nw. Env'tl. Def. Ctr. v. Bonneville Power Admin.*,
3 117 F.3d 1520, 1528 (9th Cir. 1997). Defendants did not dispute that review of facts outside the
4 administrative record is appropriate for assessing Plaintiffs' standing (*see* ECF No. 36 at 6:23-
5 24) and suggested that the parties might enter into stipulations. The Court recommended that
6 Plaintiffs pursue Defendants' invitation to explore stipulations and delay taking discovery related
7 to standing until after Defendants filed the Administrative Record for the PM-ISE's Functional
8 Standard and the Court ruled on Plaintiffs' motion regarding discovery on the DOJ Standard.
9 The Court's Minute Order instructed Defendants to provide an Administrative Record and also
10 ordered the parties to meet and confer on further case management issues. *See* ECF No. 41. The
11 parties have followed the Court's instructions.

12 On June 4, 2015, Plaintiffs filed a motion regarding discovery on the DOJ Standard. *See*
13 ECF No. 50.

14 On June 16, 2015, Defendants filed the Administrative Record for Defendant PM-ISE's
15 Functional Standard. *See* ECF Nos. 52-53.

16 Consistent with the Court's suggestion at the March 12, 2015 case management
17 conference, Plaintiffs deferred seeking discovery on standing issues pending resolution of their
18 motion on the DOJ Standard and instead sought to meet and confer with Defendants on both
19 standing and the adequacy of the Administrative Record submitted by the PM-ISE. On July 28,
20 2015, Plaintiffs sent a detailed letter explaining why the Administrative Record was incomplete
21 and exploring the feasibility of entering into factual stipulations that would eliminate or narrow
22 the need for jurisdictional discovery.

23 On August 12, 2015, the parties filed a Joint Case Management Statement, updating the
24 Court as to the status of discovery/record development in each of the three contested areas. *See*
25 ECF No. 59. As to DOJ's SAR Standard, the JCMS noted that Plaintiffs' motion was pending
26 before the Court. *Id.* at 4. As to jurisdiction, the parties noted, among other things, that they

1 were exploring potential factual stipulations. *Id.* at 5. As to the PM-ISE Functional Standard,
2 the JCMS stated: “Plaintiffs have concerns that [the administrative] record is incomplete, but the
3 parties are currently meeting and conferring in an attempt to resolve these concerns without
4 motion practice.” *Id.* at 5. Plaintiffs expressly identified the potential need for motion practice
5 over the adequacy of the Administrative Record and stated that scheduling summary judgment
6 was premature until threshold discovery issues were resolved. *Id.* at 3, 6.

7 On August 14, 2015, the Court issued an order denying Plaintiffs’ motion to seek
8 discovery regarding DOJ’s SAR Standard and inviting the parties to submit a supplemental case
9 management conference statement. *See* ECF No. 60.

10 On August 21, 2015, the parties submitted a supplemental case management statement in
11 which Plaintiffs informed the Court about a recent incident involving the FBI’s questioning of
12 close family members of one of the Plaintiffs in this action and cited the incident as an issue
13 about which discovery was appropriate and necessary because it sheds light on standing.

14 On August 25, 2015, Defendants responded to Plaintiffs’ July 28, 2015 meet and confer
15 letter. Defendants contended that the Administrative Record for the PM-ISE’s Functional
16 Standard is complete, invited Plaintiffs to identify any additional documents they believed
17 missing from the record, and stated that they were not currently willing to enter into Plaintiffs’
18 proposed factual stipulations regarding standing and “final agency action.”

19 The same day, the Court issued an order continuing the case management conference
20 then-set for August 27, 2015 and instructing the parties to file a further case management
21 conference statement proposing a summary judgment schedule. *See* ECF No. 62. The Order
22 stated that “[t]he only subject area that plaintiffs identify as potentially requiring discovery...is
23 the issue of standing.” *Id.* at 2. The Court further stated:

24 Defendants’ challenge to standing at the pleading stage was rejected. It is contemplated
25 that the cross-motions for summary judgment referred to above will be limited to review
26 on the administrative record of the propriety of the challenged agency actions. Because
27 defendants have not proposed that any discovery go forward in advance of those motions,
28 it is unclear how they would advance a challenge to standing that differed from what they

1 presented in the motion to dismiss. In the event defendants nevertheless elect to include a
2 further standing challenge as part of their motion, plaintiffs should respond based on such
3 evidence and arguments as they presently possess, and if they deem it necessary, also
4 seek relief under Rule 56(d). [*Id.*]

5 On August 31, 2015, Plaintiffs responded to Defendants' August 25, 2015 letter, further
6 detailing Plaintiffs' concerns about the incomplete nature of the PM-ISE's Administrative
7 Record, identifying 55 categories of documents missing from the Record, and observing that
8 Defendants' response to Plaintiffs' proposed stipulations on jurisdictional issues underscored the
9 need for discovery. Plaintiffs requested that Defendants respond to their request to complete the
10 Administrative Record by September 10, 2015.

11 **B. Plaintiffs' Motion to Complete the Administrative Record Should Be**
12 **Resolved Before Briefing on Summary Judgment**

13 Where an agency fails to produce a complete administrative record or the administrative
14 record is insufficient to allow the court to conduct the review required by the APA, plaintiffs can
15 seek to complete and/or supplement the record.¹ To facilitate orderly resolution of the claims in
16 this case, the Court should address whether the Administrative Record is complete *before*
17 briefing on summary judgment.

18 In reviewing agency action under the Administrative Procedure Act, "the court shall
19 review the *whole record* or those parts of it cited by a party." 5 U.S.C. § 706 (emphasis added);
20 *see also Natural Resources Defense Council, Inc. v. Train*, 519 F.2d 287, 291 (D.C. Cir. 1975)
21 (reversible error to "proceed[] with ... review on the basis of a partial and truncated record").

22 Plaintiffs have substantial concerns that the Record is not complete; these concerns
23 should be resolved through a noticed motion. Plaintiffs contend the Record is incomplete
24 because (1) Defendants have inappropriately narrowed its scope to materials considered in the
25 development of only one discrete portion of the Functional Standard, even though the Complaint

26 ¹ *See, e.g., Miami Nation of Indians of Indiana v. Babbitt*, 979 F. Supp. 771, 781 (N.D. Ind.
27 1996) (granting in part motion to complete and supplement the record).

1 expressly challenges the Functional Standard as a whole;² (2) Plaintiffs have identified 55
 2 categories of documents that the Record itself makes clear were considered by the agency but are
 3 missing from the Record compiled by Defendants;³ and (3) Defendants have admittedly withheld
 4 “deliberative” materials but have refused to produce a privilege log, thus precluding an
 5 evaluation by Plaintiffs or the Court as to the propriety of these withholdings.⁴

6 To allow for an orderly presentation of issues, the Court should determine whether the
 7 Record is complete before briefing on summary judgment proceeds. To engage in judicial
 8 review under the APA, the Court “must have access to the full record.... [Summary judgment] is
 9

10 ² Defendants must “file the entire administrative record pertinent to the omissions identified in
 11 the complaint.” *Natural Resources Defense Council, Inc. v. Train*, 519 F.2d 287, 292 (D.C. Cir.
 12 1975). They “cannot define the record by compartmentalizing” portions of the Functional
 13 Standard. *Cf. Exxon Corp. v. Dep’t of Energy*, 91 F.R.D. 26, 36-37 (N.D. Tex. 1981) (agency
 14 could not narrowly define record by “attach[ing]” “labels ... to the stages of its decisional
 15 process” and “omitting from the record all materials compiled by ‘the agency’ before rendering
 16 the final decision”). Plaintiffs challenge the Functional Standard – not only its definition of
 “suspicious activity” but also the process for collecting, maintaining, and disseminating
 suspicious activity reports set forth in the Functional Standard. *See, e.g.*, Compl. at ¶¶ 42, 51,
 162, 168 & Prayer for Relief.

17 ³ *See Thompson v. U.S. Dep’t of Labor*, 885 F.2d 551, 555 (9th Cir. 1989) (“The ‘whole’
 administrative record, therefore, consists of all documents and materials directly or indirectly
 18 considered by agency decision-makers and includes evidence contrary to the agency’s position.”)
 (internal quotation marks, citation omitted); *High Sierra Hikers Ass’n v. U.S. Dep’t of Interior*,
 2011 WL 2531138, *9 (N.D. Cal. June 24, 2011) (granting motion to augment record as to
 19 internal agency documents regarding proposed environmental assessment that were considered
 20 by the agency).

21 ⁴ *See Tafas v. Dudas*, 530 F. Supp. 2d 786, 801 (E.D. Va. 2008) (“when claiming deliberative
 process privilege...the government must comply with formal procedures necessary to invoke the
 22 privilege, including the provision of a privilege log”) (internal quotation marks, citation
 omitted”); *Tenneco Oil. Co. v. Dep’t of Energy*, 475 F. Supp. 299, 319 (D. Del. 1979) (“DOE
 23 must identify documents ... with sufficient specificity to enable this Court meaningfully to
 evaluate whether the information sought involves the internal deliberative process by which a
 24 decision or agency position was reached.”); *Guidance to Client Agencies on Compiling the
 Administrative Record*, U.S. Atty. Bull., vol. 42, no. 1 at 9 (Feb. 2000) (“[i]f documents and
 25 materials are determined to be privileged or protected, the index of record must identify the
 26 documents and materials, reflect that they are being withheld, and state on what basis they are
 27 being withheld”).

1 premature until such time as the Court is satisfied the ‘full’ record has been submitted.” *Exxon*
 2 *Corp. v. Dep’t of Energy*, 91 F.R.D. 26, 39 (N.D. Tex. 1981) (requiring “complete ...
 3 Administrative Record ... before DOE’s Motion for Summary Judgment is entertained”).⁵
 4 Defendants rely upon *McCrary v. Gutierrez*, 495 F. Supp. 2d 1038, 1041 (N.D. Cal. 2007), but
 5 plaintiffs’ challenge to the adequacy of the record in that case was heard on a noticed motion
 6 before briefing on summary judgment, which is the process Plaintiffs propose here.⁶

7 Moreover, Plaintiffs have been diligent in raising and attempting to resolve their concerns
 8 and could not have brought a motion to complete the Administrative Record earlier.⁷ At the time
 9 the Court issued its August 25, 2015 Order directing the parties to propose a summary judgment
 10 briefing schedule, the parties were still in the process of meeting and conferring over whether the
 11 Administrative Record is complete.⁸

12 **C. Discovery Related to the Court’s Jurisdiction Should Be Conducted Before**
 13 **Briefing on Summary Judgment**

14
 15 ⁵ See also *State of Calif. v. U.S. Dep’t of Labor*, 2014 WL 1665290 *3 (E.D. Cal. Apr. 24, 2014)
 16 (“court will decide [defendants’ motion for summary adjudication] after ruling on plaintiffs’
 17 motion to supplement the administrative record”); *Autotel v. Bureau of Land Mgmt.*, 2013 WL
 18 5564135 *2 (D. Nev. Oct. 7, 2013) (parties did not move for summary judgment *because*
 19 plaintiffs moved to supplement the record), *order vacated in part on reconsideration*, 2015 WL
 20 1471518 (D. Nev. Mar. 31, 2015).

21 ⁶ The case management order in *McCrary* expressly provided plaintiff the opportunity to seek
 22 discovery or to complete the record *before* summary judgment. See Case No. 06-cv-04174-JW,
 23 ECF No. 21 at ¶ 4 (“In the event that Plaintiff pursues discovery or files an objection to the
 24 record, Plaintiff shall file his motion for summary judgment within 45 days after the completion
 25 of discovery or supplementation of the record, whichever is later, which contemplates a ruling by
 26 this Court on any motions for a protective order that may be sought by Defendants.”).

27 ⁷ Plaintiffs’ motion to *complete* the record will identify known documents that were considered
 28 but not included in the Administrative Record. After Defendants complete the record, it may
 still be necessary to *supplement* the record. See *Southwest Ctr. for Biological Diversity v. U.S.*
Forest Serv., 100 F.3d 1443, 1450 (9th Cir. 1996) (setting forth conditions under which court
 may supplement record with extra-record materials).

⁸ See ECF No. 59 at 3:15-18 (discussing parties’ meet and confer over Plaintiffs’ concerns that
 Administrative Record incomplete and potential need for motion practice over issue), 4:27-5:4
 (same); 6:18-19 (stating Plaintiffs’ position that “the scheduling of summary judgment or trial
 dates would be premature before the threshold discovery issues are resolved”).

1 Plaintiffs will suffer prejudice if they are unable to conduct discovery related to the
2 Court’s jurisdiction *before* the parties submit briefing on summary judgment. Rule 56(d) is not
3 an adequate mechanism for protecting their right to develop the factual record in this case.

4 The rule limiting review to the administrative record in APA cases does not apply to
5 jurisdictional questions, *Nw. Entl. Def. Ctr. v. Bonneville Power Admin.*, 117 F.3d 1520, 1528
6 (9th Cir. 1997), and therefore does not bar Plaintiffs from conducting discovery on the issue of
7 standing. The Court’s August 25, 2015 Order suggests no such discovery would be necessary
8 unless Defendants “elect to include a further standing challenge as part of their motion” for
9 summary judgment. ECF No. 62 at 2. But Defendants cannot waive objections to subject matter
10 jurisdiction and it is the Plaintiffs’ burden to establish standing.

11 Relatedly, Plaintiffs cannot rest on the Court’s rejection at the pleading stage of
12 Defendants’ challenge to Plaintiffs’ standing. In their motion to dismiss, Defendants disputed
13 Plaintiffs’ standing by arguing that Plaintiffs cannot “credibly” allege that their injuries stemmed
14 from Defendants’ conduct and that “merely being the subject of an SAR, in the national
15 database” does not constitute a cognizable injury-in-fact. *See* Order Denying Motion to Dismiss
16 (ECF No. 38 at 7). Opposing these arguments requires further fact development – regarding the
17 extent to which third parties reported Plaintiffs as suspicious because of Defendants’ standards
18 and the consequences of being the subject of a SAR in a national database. The latter subject
19 entails information in Defendants’ exclusive control. Even if the Court were to reject
20 Defendants’ standing arguments on summary judgment – such that Plaintiffs need not develop
21 these facts to prevail on summary judgment – an appellate court might accept those arguments.
22 Plaintiffs are entitled to develop a factual record sufficient to meet their burden before this Court
23 and on appeal.

24 For the same reason, Rule 56(d) is not sufficient to protect Plaintiffs’ right to develop a
25 factual record establishing their standing. That provision affords relief upon a showing by a
26 nonmovant that “it cannot present facts essential *to justify its opposition.*” Fed. R. Civ. P. 56(d)

(emphasis added). If, on summary judgment, Defendants elect not to challenge standing, or to challenge standing only on select grounds, Plaintiffs cannot invoke Rule 56(d) to justify obtaining discovery. But such an election would not prevent Defendants from raising on appeal challenges to standing they chose not to raise at summary judgment. *See, e.g., City of Los Angeles v. County of Kern*, 581 F.3d 841, 845 (9th Cir. 2009) (arguments regarding Article III standing “cannot be waived by any party”). Plaintiffs will therefore be severely prejudiced if they are unable to take jurisdictional discovery before briefing proceeds on summary judgment.

In addition, because Defendants assert that “final agency action” is a question of subject matter jurisdiction, *see* ECF No. 21 at 23 (motion to dismiss); 36 at 2:6-10 (JCMS), Plaintiffs are entitled to discovery related to that issue as well.

Plaintiffs attempted to propose factual stipulations related to standing and final agency action, but the parties’ meet and confer was not fruitful.⁹ Plaintiffs propose to serve limited discovery related to standing and final agency action on or before September 17, 2015. Depositions regarding the written responses may also be necessary. To the extent Defendants contest Plaintiffs’ right to obtain such discovery, the question should be litigated on a motion for a protective order or motion to compel.

* * *

Plaintiffs therefore propose the following schedule:

Sept. 10, 2015	Parties to complete meet and confer over completeness of the administrative record
Sept. 17, 2015	Plaintiffs to propound initial written discovery related to Court’s jurisdiction

⁹ Plaintiffs have consistently reserved their right to seek discovery on facts outside the administrative record that bear on the Court’s jurisdiction. *See* ECF Nos. 36 at 7-8, 40 at 7-8, 59 at 5; ECF No. 50, n. 4. Plaintiffs have not propounded jurisdictional discovery to date based on the Court’s suggestion at the March 12, 2015 CMC that they defer doing so until after the ruling on Plaintiffs’ motion regarding the DOJ Standard and after exploring potential factual stipulations, but are now prepared to do so.

1	Sept. 24, 2015	Plaintiffs to file motion to complete the Administrative Record
2	Oct. 29, 2015	Hearing on Plaintiffs' motion to complete the Administrative Record
3	Jan. 28, 2016	Defendants to file motion in support of summary judgment (40 pages)
4	March 3, 2016	Plaintiffs to file opposition and cross-motion (45pages)
5	April 7, 2016	Defendants to file opposition and reply (40 pages)
6	April 21, 2016	Plaintiffs to file reply (35 pages)

7 **II. Defendants' Position**

8 Consistent with the Court's Order that the parties submit a schedule for briefing summary
9 judgment, Defendants' position is that this case is ready to proceed to summary judgment
10 without any additional motion practice. As Plaintiffs' recitation of the procedural history in this
11 case shows, the Court has already entertained significant preliminary proceedings in this
12 Administrative Procedure Act ("APA") case. Among other things, Defendants have filed an
13 administrative record regarding the issuance of the Functional Standard challenged by Plaintiffs,
14 and the Court has denied Plaintiffs' motion to expand that administrative record to include a
15 purportedly separate "DOJ Standard". To the extent that Plaintiffs assert that there any
16 additional factual issues relevant to the resolution of this action that are not addressed by the
17 administrative record that has been filed, those issues will most efficiently be identified and
18 explained through summary judgment briefing and, as noted in the Court's recent order, under
19 Rule 56(d).

20 This Further Supplemental Joint Case Management Statement is not the appropriate
21 context to brief the issues raised by Plaintiffs concerning the appropriateness of discovery related
22 to their standing to bring these claims or the completeness of the administrative record. As the
23 Court has noted, Plaintiffs will have the opportunity to explain their position that the
24 administrative record is incomplete and that jurisdictional discovery must be permitted through
25 summary judgment briefing—and if necessary, the filing of a Rule 56(d) affidavit. *See* Dkt. 60,
26 8/14/15 Order Denying Motion for Leave to Conduct Discovery at 4 ("If in the course of such
27

1 motion practice, the need for targeted discovery on particular issues, generally consistent with
2 APA proceedings, becomes manifest, the question of permitting discovery can be revisited.”);
3 Dkt. 62, 8/25/14 Order Continuing Case Management Conference and Directing Supplemental
4 Filing (“In the event defendants nevertheless elect to include a further standing challenge as part
5 of their motion, plaintiffs should respond based on such evidence and argument as they presently
6 possess, and if they deem it necessary, also seek relief under Rule 56(d).”). Indeed, in light of
7 the Court’s prior rulings, Defendants do not anticipate making any standing arguments based on
8 the submission of factual evidence in connection with their motion for summary judgment.

9 Though summary judgment is the more appropriate context to address the issues raised
10 by Plaintiffs, Defendants believe it necessary to respond briefly in light of the detailed arguments
11 they have made in this joint statement. Considerable deference is given to the agency to
12 determine whether the administrative record is complete. As this Court has itself stated, “[a]n
13 agency’s designation and certification of the administrative record is treated like other
14 established administrative procedures, and thus entitled to a presumption of administrative
15 regularity.” *McCrary v. Gutierrez*, 495 F. Supp. 2d 1038, 1041 (N.D. Cal. 2007) (Seeborg, J.).

16 Consistent with that discretion, the Program Manager acted appropriately in compiling an
17 administrative record including the documents he relied upon (directly and indirectly) in issuing
18 the definition of suspicious activity utilized in the Functional Standard. Despite the inclusion of
19 allegations in the Complaint relating to other aspects of the Nationwide SAR Initiative (“NSI”),
20 the claims asserted in the Complaint unambiguously challenge the permissibility of the standard
21 by which SAR information is collected and shared in connection with the NSI. Compl. ¶¶ 42–
22 52, 159– 64, 167–68; *see also* Dkt. 38, 2/20/2015, Order Denying Motion to Dismiss at 1
23 (“Plaintiffs contend that defendants Department of Justice (“DOJ”) and the Program Manager-
24 Information Sharing Environment (“PM-ISE”) have issued protocols utilizing an overly broad
25 standard to define the types of activities that should be deemed as having a potential nexus to
26 terrorism.”). And Plaintiffs specifically allege in the Complaint that this “SAR standard” is the

1 definition of suspicious activity in the Functional Standard. *Id.* ¶ 44 (“[Functional Standard 1.5]
 2 sets forth the following standard for suspicious activity reporting: ‘[o]bserved behavior
 3 reasonably indicative of pre-operational planning related to terrorism or other criminal
 4 activity.’”).

5 Plaintiffs are also incorrect that deliberative material should be included in the
 6 administrative record or else identified in a privilege log. To the contrary, courts have held that
 7 deliberative materials need not be designated as part of the administrative record because “the
 8 actual subjective motivation of agency decisionmakers is immaterial as a matter of law—unless
 9 there is a showing of bad faith or improper behavior.” *In re Subpoena Duces Tecum Served on*
 10 *Office of Comptroller of Currency*, 156 F.3d 1279, 1279 (D.C. Cir. 1998). Likewise, “[s]ince
 11 deliberative documents are not part of the administrative record, an agency that withholds these
 12 privileged documents is not required to produce a privilege log to describe the documents that
 13 have been withheld.” *Nat’l Ass’n of Chain Drug Stores v. U.S. Dep’t of Health & Human Servs.*,
 14 631 F. Supp. 2d 23, 27 (D.D.C. 2009).

15 Accordingly, Plaintiffs’ objections to the adequacy of the administrative record are
 16 without basis. The administrative record is complete. In any event, as the Court recognized,
 17 Plaintiffs are able to raise any concerns they have with the completeness of that record through
 18 the briefing of summary judgment under Rule 56(d). Defendants therefore propose the following
 19 briefing schedule, with the following proposed page limits:

20 October 8, 2015	Defendants to file motion in support of summary judgment (40 pages)
21 November 19, 2015	Plaintiffs to file opposition and cross-motion (45 pages)
22 January 14, 2016	Defendants to file opposition and reply (40 pages)
23 February 4, 2016	Plaintiffs to file reply (35 pages)

1 Dated: September 4, 2015

2 _____ /s/ Linda Lye

3 Counsel for Plaintiffs¹⁰

4 AMERICAN CIVIL LIBERTIES UNION
5 FOUNDATION OF NORTHERN CALIFORNIA
6 Linda Lye (#21584)

7 llye@aclunc.org

8 Julia Harumi Mass (#189649)

9 jmass@aclunc.org

10 39 Drumm Street

11 San Francisco, CA 94111

12 Tel: 415.621.2493

13 Fax: 415.896.1702

14 ASIAN AMERICANS ADVANCING JUSTICE –
15 ASIAN LAW CAUCUS

16 Nasrina Bargzie (#238917)

17 nsrinab@advancingjustice-alc.org

18 Yaman Salahi (#288752)

19 yamans@advancingjustice-alc.org

20 55 Columbus Avenue

21 San Francisco, CA 94111

22 Tel: 415.848.7711

23 Fax: 415.896.1702

24 MORGAN, LEWIS & BROCKIUS LLP

25 Stephen Scotch-Marmo (admitted *pro hac vice*)

26 stephen.scotch-marmo@morganlewis.com

27 Michael Abelson (admitted *pro hac vice*)

28 michael.abelson@morganlewis.com

101 Park Avenue,

New York, NY 10178

Tel: 212.309.6000

Fax: 212.309.6001

399 Park Avenue

New York, NY 10022

MORGAN, LEWIS & BROCKIUS LLP

Jeffrey Raskin (#169096)

jraskin@morganlewis.com

Nicole R. Sadler (#275333)

nsadler@morganlewis.com

Phillip Wiese (#291842)

26 ¹⁰ I, Linda Lye, hereby attest, in accordance with Local Rule 5-1(i)(3), the concurrence in the
27 filing of this document has been obtained from the other signatory listed here.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

pwiese@morganlewis.com
One Market Street, Spear Street Tower
San Francisco, CA 94105
Tel: 415.442.1000
Fax: 415.442.1001

AMERICAN CIVIL LIBERTIES UNION
FOUNDATION
Hina Shamsi (admitted *pro hac vice*)
hshamsi@aclu.org
Hugh Handeyside (admitted *pro hac vice*)
hhandeyside@aclu.org
125 Broad Street
New York, NY 10004
Tel: 212.549.2500
Fac: 212.549.2654

AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF SAN DIEGO AND
IMPERIAL COUNTIES
David Loy (#229235)
Mitra Ebadolahi (#275157)
mebadolahi@aclusandiego.org
P.O. Box 87131
San Diego, CA 92138
Tel: 619.232.2121
Fax: 619.232.0036

AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF SOUTHERN CALIFORNIA
Peter Bibring (#223981)
pbibring@clusocal.org
1313 West 8th Street
Los Angeles, CA 90017
Tel: 213.977.9500
Fax: 213.977.5299

Dated: September 4, 2015

/s/ Paul G. Freeborne

Counsel for Defendants

JOYCE R. BRANDA
Acting Assistant Attorney General
MELINDA L. HAAG
United States Attorney
ANTHONY J. COPPOLINO
Deputy Branch Director

PAUL G. FREEBORNE
Senior Trial Counsel

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

KIERAN G. GOSTIN
Trial Attorney

Civil Division, Federal Programs Branch
U.S. Department of Justice
P.O. Box 883
Washington, D.C. 20044
Telephone: (202) 353-0543
Facsimile: (202) 616-8460
E-mail: paul.freeborne@usdoj.gov

CASE MANAGEMENT ORDER

The above JOINT CASE MANAGEMENT STATEMENT & PROPOSED ORDER is approved as the Case Management Order for this case and all parties shall comply with its provisions. In addition, the Court makes the further orders stated below:

IT IS SO ORDERED.

Dated:

UNITED STATES DISTRICT/MAGISTRATE
JUDGE

United States District Court
Northern District of California

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

WILEY GILL, et al.,
Plaintiffs,
v.
DEPARTMENT OF JUSTICE, et al.,
Defendants.

Case No. [14-cv-03120-RS](#)

**ORDER REFERRING ISSUES TO
MAGISTRATE JUDGE AND
CONTINUING FURTHER CASE
MANAGEMENT CONFERENCE**

Upon review of the parties’ further supplemental joint case management statement and good cause appearing, it is ordered:

1. The parties shall complete their ongoing meet and confer negotiations regarding the administrative record, including any further meet and confer efforts that may be required by the magistrate judge prior to motion practice.
2. A randomly-selected magistrate judge shall be assigned to this action to hear and decide any disputes regarding the adequacy of the administrative record that the parties are unable to resolve, as well as any discovery disputes in the event discovery is permitted at some future point in time.
3. Plaintiffs’ request for leave to propound “jurisdictional” discovery at this juncture is denied.
4. The further Case Management Conference is continued to November 19, 2015. In the event the issues regarding the administrative record have not been resolved, one week prior

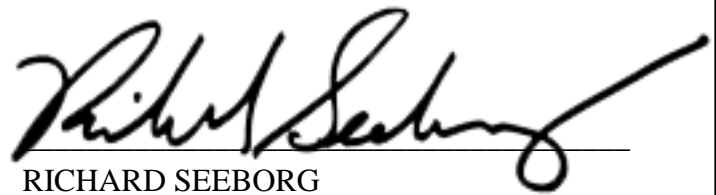
United States District Court
Northern District of California

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

to the conference the parties shall submit a joint status update. If no further challenges to the completeness of the administrative record are then pending, one week prior to the conference the parties shall jointly propose a briefing schedule for cross-summary judgment motions. The parties are advised that the page limits they have proposed will be reduced by five pages per brief.

IT IS SO ORDERED.

Dated: September 8, 2015


RICHARD SEEBORG
United States District Judge

1 BENJAMIN C. MIZER
 Principal Deputy Attorney General
 2 ANTHONY J. COPPOLINO
 Deputy Branch Director
 3 KIERAN G. GOSTIN
 Trial Attorney
 4 D.C. Bar No. 1019779

5 Civil Division, Federal Programs Branch
 U.S. Department of Justice
 6 P.O. Box 883
 Washington, D.C. 20044
 7 Telephone: (202) 353-4556
 Facsimile: (202) 616-8460
 8 E-mail: kieran.g.gostin@usdoj.gov

9 *Attorneys for Federal Defendants*

10 **UNITED STATES DISTRICT COURT**
 11 **FOR THE NORTHERN DISTRICT OF CALIFORNIA**

12 WILEY GILL; JAMES PRIGOFF; TARIQ
 13 RAZAK; KHALID IBRAHIM; and AARON
 14 CONKLIN,

15 Plaintiffs,

16 v.

17 DEPARTMENT OF JUSTICE, *et al.*,

18 Defendants.
 19

No. 3:14-cv-03120 (RS)(KAW)

DEFENDANTS' NOTICE OF MOTION
FOR SUMMARY JUDGMENT AND
MEMORANDUM IN SUPPORT

Hearing Date: December 8, 2016

Time: 1:30 PM

TABLE OF CONTENTS

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

INTRODUCTION..... 1

 I. Statutory and Regulatory Background..... 5

 II. The Nationwide Suspicious Activity Reporting Initiative 6

 III. The Functional Standard for Suspicious Activity Reporting 7

 IV. Criminal Intelligence Systems Funded by the Omnibus Act 10

STANDARD OF REVIEW 12

ARGUMENT..... 13

 I. Plaintiffs’ Notice-and-Comment Claim Fails 13

 A. The Functional Standard is Not a Legislative Rule Subject to Notice-and-Comment Rulemaking..... 14

 B. The PM-ISE’s Process for Formulating the Functional Standard Adequately Protected Plaintiffs’ Substantive and Procedural Interests 18

 II. Plaintiffs’ Arbitrary-and-Capricious Claim Fails 22

 A. Plaintiffs’ Have Brought a Facial Challenge but Are Unable to Satisfy the Requirements Needed to Succeed on Such Challenge 22

 B. Even if Plaintiffs Had Raised an As-Applied Challenge, Such a Challenge Would be Unsuccessful..... 25

 C. The Challenged Decision Was Not Arbitrary or Capricious 28

 1. The APA’s Arbitrary-and-Capricious Standard 28

 2. The Adoption of the “Reasonably Indicative” Operational Concept..... 29

 3. The Rejection of the “Reasonable Suspicion” Standard 31

 III. Remand Without Vacatur Would Be the Only Appropriate Remedy 33

CONCLUSION 35

1 projects receiving Omnibus Act funding are in compliance with the regulation's
 2 requirements, *see* 28 C.F.R. §§ 23.30, 23.40, and set forth specific penalties for any project
 3 that fails to comply with those requirements, *see* 42 U.S.C. § 3789g(d); 28 C.F.R. § 23.30.
 4 The Functional Standard, in contrast, does not establish any monitoring mechanism to
 5 ensure compliance or set forth any penalties for a failure to comply. There is simply no
 6 expectation that the PM-ISE will seek to enforce the Functional Standard against NSI
 7 participants through administrative (or judicial) proceedings, nor has it ever done so.

8 In sum, the Functional Standard is the result of a long-term collaborative effort
 9 between law enforcement partners at the federal, state, local, tribal, and territorial levels of
 10 government to standardize the process of sharing SARs across jurisdictional lines.
 11 Consistent with the collaborative nature of that effort, the Functional Standard does not
 12 attempt to impose mandatory rules, but instead describes guidelines intended to promote
 13 consistent practices. The issuance of this policy guidance is not an exercise of a legislative
 14 function by a federal agency, and therefore, is not subject to the APA's procedural
 15 requirements for rulemaking.

16 * * *

17 In addition to exempting “general statements of policy” from its rulemaking
 18 procedures, the APA only permits review of agency actions that are “final.” 5 U.S.C. § 704.
 19 As explained by the Supreme Court, an action is only deemed final if it is both (i) the
 20 “consummation of the agency’s decisionmaking process” and (ii) an action by which “rights
 21 or obligations have been determined, or from which legal consequences will flow.” *Bennett v.*
 22 *Spear*, 520 U.S. 154, 177–78 (1997). In their motion to dismiss, Defendants explained that
 23 the issuance of the Functional Standard does not constitute a final agency action because it
 24 does not satisfy that latter requirement. *See* Defs.’ Motion to Dismiss, ECF No. 21, at 23–
 25 25; Defs.; Reply in Support of Motion to Dismiss, ECF No. 28, at 7–11. Because this Court
 26 has already rejected that argument, *see* Order Denying Motion to Dismiss, ECF No. 38, at 8–
 27

1 9, Defendants do not repeat it in detail. However, Defendants respectfully disagree with the
2 Court’s ruling, continue to maintain that the issuance of the Functional Standard does not
3 constitute a final agency action, and incorporate the arguments from their motion to dismiss
4 here.

5 B. The PM-ISE’s Process for Formulating the Functional Standard Adequately
6 Protected Plaintiffs’ Substantive and Procedural Interests

7 Plaintiffs’ request that the PM-ISE be ordered to reissue the Functional Standard in
8 accordance with the technical requirements of the APA’s rulemaking procedures is also
9 unwarranted in light of the public process that the PM-ISE has already conducted. The
10 APA instructs federal agencies to follow certain notice-and-comment procedures when
11 issuing legislative rules. As noted, because the Functional Standard does not create the
12 binding legal obligations that are the hallmark of legislative rules, the PM-ISE did not follow
13 those procedures—such as publication of the final rule in the Federal Register.
14 Nonetheless, the formulation of the Functional Standard was a public process that involved
15 extensive participation by interested parties, including an opportunity for advocacy groups to
16 express their concerns with the “reasonably indicative” operational concept that is
17 challenged in this case. Accordingly, even if the Functional Standard were a legislative rule,
18 any failure to comply with the APA’s rulemaking procedures is harmless and does not justify
19 a remand requiring the agency to engage in those technical procedures at significant cost to
20 taxpayers.

21 The APA instructs federal courts to take “due account” of the rule of “prejudicial
22 error” when reviewing agency action to determine whether the agency complied with the
23 APA’s procedural requirements. 5 U.S.C. § 706. Consistent with the principle that district
24 courts act as appellate courts in reviewing agency action, this provision requires district
25 courts to apply the same harmless error rule used by federal courts of appeals in civil and
26 criminal litigation. *Nat’l Ass’n of Home Builders v. Defs. of Wildlife*, 551 U.S. 644, 659 (2007).
27 As one court has explained, “[i]f the agency’s mistake did not affect the outcome, if it did

1 Standard should not be vacated if the Court determines that this matter must be remanded
2 to the agency. Imposing that remedy would result in an increased risk to national security
3 for no valid reason.

4 **CONCLUSION**

5 For the aforementioned reasons, this Court should grant summary judgment in favor
6 of Defendants.

7
8 August 18, 2016

Respectfully submitted,

9 BENJAMIN C. MIZER
10 Principal Deputy Assistant Attorney General

11 ANTHONY J. COPPOLINO
12 Deputy Branch Director

13 */s/ Kieran G. Gostin*

14 Kieran G. Gostin
15 Trial Attorney
16 Civil Division, Federal Programs Branch
17 U.S. Department of Justice
18 P.O. Box 883
19 Washington, D.C. 20044
20 Telephone: (202) 353-4556
21 Facsimile: (202) 616-8460
22 E-mail: kieran.g.gostin@usdoj.gov

23 *Attorneys for Federal Defendants*

CERTIFICATE OF SERVICE

I hereby certify that on March 30, 2018, I electronically filed the Further Excerpts of Record of Appellants with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system.

Participants in the case who are registered CM/ECF users will be served by the appellate CM/ECF system.

Dated: March 30, 2018

/s/ Linda Lye

Linda Lye

Lead Attorney for Appellants

Wiley Gill, James Prigoff, Tariq Razak,

Khaled Ibrahim, and Aaron Conklin