BINGHAM MCCUTCHEN LLP
Jonathan Loeb (#162758) jonathan.loeb@bingham.com
Jeffrey Rosenfeld (#221625) jeffreyrosenfeld@bingham.com
Edward Andrews (#268479) edward.andrews@bingham.com
The Water Garden, Suite 2050 North
1601 Cloverfield Boulevard
Santa Monica, CA 90404-4082
Telephone: 310-907-1000
Facsimile: 310-907-2000

AMERICAN CIVIL LIBERTIES UNION FOUNDATION
OF NORTHERN CALIFORNIA
Linda Lye (#215584) llye@aclunc.org
Julia Harumi Mass (#189649) jmass@aclunc.org
39 Drumm Street
San Francisco, CA 94111
Telephone: 415-621-2493
Facsimile: 415-255-8437

ASIAN AMERICANS ADVANCING
JUSTICE - ASIAN LAW CAUCUS
Nasrina Bargzie (#238917) nasrinab@advancingjustice-alc.org
Yaman Salahi (#288752) yamans@advancingjustice-alc.org
55 Columbus Avenue
San Francisco, CA 94111
Telephone: 415-848-7711
Facsimile: 415-896-1702

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

Additional counsel listed on signature page

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO-OAKLAND DIVISION

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

Plaintiffs,

v.

DEPARTMENT OF JUSTICE; ERIC H. HOLDER, Jr., in his official capacity as the Attorney General of the United States; PROGRAM MANAGER - INFORMATION SHARING ENVIRONMENT; KSHEMENDRA PAUL, in his official capacity as the Program Manager of the Information Sharing Environment,

Defendants.

No. 3:14-cv-03120-RS

PLAINTIFFS' OPPOSITION TO MOTION TO DISMISS

TABLE OF CONTENTS

Page

I. INTRODUCTION 1

II. BACKGROUND 3

A. Defendants Have Created a Uniform, National System for Collecting, Vetting, and Disseminating Intelligence About Individuals Considered to Have a Potential Nexus to the Crime of Terrorism 3

1. Overview of SAR Information Flow 4

2. Individuals Reported in SARs Face Law Enforcement Scrutiny 5

3. Collection and Dissemination of Personal Information 6

4. The Governing Standard for Reporting Criminal Intelligence 6

5. Defendants' Standards for Collecting, Vetting, and Disseminating Intelligence Related to Terrorism Conflict with 28 C.F.R. Part 23 and Were Issued Without Notice and Comment 8

6. The NSI Has Not Proven Effective in the Fight Against Terrorism 10

B. Plaintiffs Have Been Reported As "Suspicious" for Their Lawful Conduct 10

III. LEGAL STANDARD 13

IV. ARGUMENT 13

A. Plaintiffs Allege Sufficient Facts to Establish Standing 13

1. Plaintiffs' Injuries Are Particularized, Concrete, and Cognizable 13

2. Plaintiffs' Injuries Are Fairly Traceable to Defendants' Standards 17

B. The Complaint States Claims Under the Administrative Procedure Act 19

1. A Suit Against Local Police or Private Guards Is Insufficient to Remedy Harms Caused by the Federal Defendants 19

2. Plaintiffs Have Adequately Alleged That Functional Standard 1.5 and DOJ's SAR Standard Each Constitute Final Agency Action 22

3. Functional Standard 1.5 and DOJ's SAR Standard Are Arbitrary and Capricious 25

(a) 28 C.F.R. Part 23 Applies to SARs and the NSI 26

(b) Functional Standard 1.5 and DOJ's SAR Standard Are Arbitrary and Capricious Because They Conflict with 28 C.F.R. § 23.20(a) 28

4. Defendants Failed to Adopt Their SAR Standards Through Notice and Comment 31

C. Defendants' Request for Severance Is Meritless 33

1. Joinder Is Appropriate 33

2. Venue Is Proper in this District 34

V. CONCLUSION 35

TABLE OF AUTHORITIES

Page(s)

Cases

United States ex rel. *Accardi v. Shaughnessy*,
347 U.S. 260 (1954) 29

Am. Mining Cong. v. Mine Safety & Health Admin.,
995 F.2d 1106 (D.C. Cir. 1993) 31, 32

ASARCO, LLC. v. Union Pac. R.R. Co.,
765 F.3d 999 (9th Cir. 2014) 27, 28

Bennett v. Spear,
520 U.S. 154 (1997) 3, 22, 23, 24

Bowen v. Georgetown Univ. Hosp.,
488 U.S. 204 (1988) 30

Bowen v. Massachusetts,
487 U.S. 879 (1988) 20, 21

Brem-Air Disposal v. Cohen,
156 F.3d 1002 (9th Cir. 1998) 21, 22

Camreta v. Greene,
_U.S._, 131 S. Ct. 2020 (2011) 13

Cantrell v. City of Long Beach,
241 F.3d 674 (9th Cir. 2001) 17

Chang v. United States,
327 F.3d 911 (9th Cir. 2003) 20, 21

Chubb Custom Ins. Co. v. Space Sys./Loral, Inc.,
710 F.3d 946 (9th Cir. 2013) 30

City of Los Angeles v. Lyons,
461 U.S. 95 (1983) 17

Clapper v. Amnesty Int'l, U.S.A.,
_U.S._, 133 S. Ct. 1138 (2013) 16

Coker v. Sullivan,
902 F.2d 84 (D.C. Cir.1990) 21

Columbia Riverkeeper v. U.S. Coast Guard,
761 F.3d 1084 (9th Cir. 2014) 24

Coughlin v. Rogers,
130 F.3d 1348 (9th Cir. 1997) 34

Ctr. for Auto Safety v. Nat'l Highway Traffic Admin.,
452 F.3d 798 (D.C. Cir. 2006) 25

Erringer v. Thompson,
371 F.3d 625 (9th Cir. 2004) 32

Food Town Stores v. Equal Emp't Opportunity Comm'n,
708 F.2d 920 (4th Cir. 1983) 20, 21

Garcia v. McCarthy,
No. 13-CV-03939-WHO, 2014 WL 187386 (N.D. Cal. Jan. 16, 2014) 22

Garcia v. Vilsack,
563 F.3d 519 (D.C. Cir. 2009) 22

Habeas Corpus Res. Ctr. v. Dep't of Justice,
No. C 13-4517 CW, 2014 WL 3908220 (N.D. Cal. Aug. 7, 2014) 20, 21

Haro v Sebelius,
747 F.3d 1099 (9th Cir. 2014) 17

Hart v. McLucas,
535 F.2d 516 (9th Cir. 1976) 30

Heckler v. Chaney,
470 U.S. 821 (1985) 20

Hein v. Freedom From Religion Found., Inc.,
551 U.S. 587 (2007) 18

Hemp Indus. Ass'n v. DEA,
333 F.3d 1082 (9th Cir. 2003) 15, 31, 32, 33

Humane Soc'y v. Hodel,
840 F.2d 45 (D.C. Cir. 1988) 18

Ibrahim v. Dep't of Homeland Sec.,
669 F.3d 983 (9th Cir. 2012) 13, 14, 16

Jersey Heights Neighborhood Ass'n v. Glendening,
174 F.3d 180 (4th Cir. 1999) 22

Joint Anti-Fascist Refugee Comm. v. McGrath,
341 U.S. 123 (1951) 15

Judalung v. Holder,
_ U.S. _, 132 S.Ct. 476 (2011) 31

Krottner v. Starbucks Corp.,
628 F.3d 1139 (9th Cir. 2010) 15, 16

League to Save Lake Tahoe v. Tahoe Reg'l Planning Agency,
558 F.2d 914 (9th Cir. 1977) 34

Lee v. City of Los Angeles,
250 F.3d 668 (9th Cir. 2001) 5, 28

Lujan v. Defenders of Wildlife,
504 U.S. 555 (1992) 13, 14

Meese v. Keene,
481 U.S. 465 (1987) 15

Melendres v. Arpaio,
695 F.3d 990 (9th Cir. 2012) 17

Mendia v. Garcia,
768 F.3d 1009 (9th Cir. 2014) 18, 19

Motor Vehicle Mfrs. Ass'n of the U.S., Inc. v. State Farm Mut. Auto. Ins. Co.,
463 U.S. 29 (1983) 30

Oregon Natural Desert Ass'n v. U.S. Forest Serv.,
465 F.3d 977 (9th Cir. 2006) 23, 24, 25

Paralyzed Veterans of Am. v. McPherson,
No. C064670SBA, 2008 WL 4183981 (N.D. Cal. Sept. 9, 2008) 5

Renee v. Duncan,
686 F.3d 1002 (9th Cir. 2012) 18

Reno-Sparks Indian Colony v. U.S. EPA,
336 F.3d 899 (9th Cir. 2003) 31

Rimmer v. Holder,
700 F.3d 246 (6th Cir. 2012) 22

Rodriguez v. Cal. Highway Patrol,
89 F. Supp. 2d 1131 (N.D. Cal. 2000) 35

Service v. Dulles,
354 U.S. 363 (1957) 29

In re Sony Gaming & Customer Data Sec. Breach Litig.,
996 F. Supp. 2d 942 (S.D. Cal. 2014) 14, 29

Toxco Inc. v. Chu,
724 F. Supp. 2d 16 (D.D.C. 2010) 21

Transohio Sav. Bank v. Dir., Office of Thrift Supervision,
967 F.2d 598 (D.C. Cir. 1992) 20

Turner v. LaFond,
No. C 09–00683 MHP, 2009 WL 3400987 (N.D. Cal Oct. 20, 2009) 34

Turner v. Secretary of U.S. Dep't of Hous. and Urban Dev.,
449 F.3d 536 (3rd Cir. 2006) 22

United States v. Mississippi,
380 U.S. 128 (1965) 34

Vill. of Arlington Heights v. Metro. Hous. Dev. Corp.,
429 U.S. 252 (1977) 14

W. Ctr. for Journalism v. Cederquist,
235 F.3d 1153 (9th Cir. 2000) 13

Warth v. Seldin,
422 U.S. 490 (1975) 13

Washington Legal Found. v. Alexander,
984 F.2d 483 (D.C. Cir. 1993) 22

Yesler Terrace Cmty. Council v. Cisneros,
37 F.3d 442 (9th Cir. 1994) 18, 33

Statutes

5 U.S.C. § 553 31

5 U.S.C. § 702 20

5 U.S.C. § 706(2)(A) 25, 28

6 U.S.C. § 485(f)(1) 32

18 U.S.C. § 2332b 26

28 U.S.C. § 1391(e)(1) 35

28 U.S.C. § 2401(a) 19

42 U.S.C. § 1391(e) 35

42 U.S.C. § 3711. ..... 7, 27

42 U.S.C. § 3789g(c) ..... *passim*

5 U.S.C. § 500, *et seq.* ..... *passim*

Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. 90-351, 82 Stat. 197 (1968) 6

Other Authorities

28 C.F.R. § 23 (1993) ..... *passim*

43 Fed. Reg. 28,572 (June 30, 1978) 7, 30

58 Fed. Reg. 48,448 (Sept. 16, 1993) 30

58 Fed. Reg. 48,451 (Sept. 16, 1993) 7

Fed. R. Civ. P. 20(a)(1) 34, 35

Fed. R. Evid. 201(b)(2) 5

I. INTRODUCTION

This action challenges the National Suspicious Activity Reporting Initiative ("NSI"), a nationwide program that collects, vets, and disseminates intelligence with a possible nexus to terrorism, but uses an overly broad standard that causes innocent Americans to be wrongly branded as potential terrorists. Defendants Department of Justice ("DOJ") and Program Manager-Information Sharing Environment ("PM-ISE") have issued rules defining the types of activities that Defendants deem to have a potential nexus to terrorism and that state and local law enforcement then transmit to the federal government in the form of "Suspicious Activity Reports" ("SARs"). These rules authorize the collection and dissemination of SARS even if unsupported by reasonable suspicion of criminal activity. Defendants' rules directly conflict with a duly promulgated regulation of Defendant DOJ, 28 C.F.R. Part 23, that was adopted to protect constitutional and privacy rights, and that prohibits the collection of criminal intelligence unless supported by reasonable suspicion. Defendants' rules on SAR reporting violate the Administrative Procedure Act ("APA"), 5 U.S.C. § 500, *et seq.*, because they conflict with 28 C.F.R. Part 23, are not in accordance with law, and are arbitrary and capricious, and because they were issued without notice and comment. Plaintiffs are five U.S. citizens who were swept up in Defendants' surveillance net based on entirely innocent activity, such as taking photographs and buying computers. As a result, Plaintiffs' personal information has been disseminated to law enforcement agencies nationwide, and they have faced undue law enforcement scrutiny, among other harms.

Defendants' motion to dismiss is largely an effort to shift the blame to state and local law enforcement for the program they created and the rules they issued. Their arguments also rest on characterizations of the NSI that depend on facts outside of or contrary to the Complaint, which is impermissible on a motion to dismiss. In particular, Defendants portray the rules they have issued as mere guidance that state and local actors are free to disregard and describe SARs as "uncorroborated tips and leads" (Gov. Br. at 1). However, the Complaint and Defendants' own documents attached thereto show that the stated purpose of the NSI is to collect intelligence about the crime of terrorism; that the NSI relies on state and local actors to collect reports; that Defendants issued their rules for SAR reporting to create uniformity in the vetting of such reports;

and that only SARs evaluated to comply with those rules are uploaded to federally maintained databases for national dissemination. Thus, the NSI is not merely a repository of "uncorroborated tips and leads," but a unified process for collecting and evaluating SARs for their potential relevance, in Defendants' view, to the crime of terrorism and for disseminating nationally only the intelligence that meets Defendants' rules. The agencies that reported Plaintiffs as "suspicious" did so not because they are rogue actors, but because they were implementing Defendants' rules. Defendants' suggestion that participants in the NSI are free to disregard their rules would undermine the very purpose of those rules – to standardize SAR reporting.

Accepting the well-pleaded allegations of the Complaint as true and construing them in favor of Plaintiffs, Defendants' motion to dismiss must be denied. First, Plaintiffs have standing to bring this suit. They have each been reported as "suspicious" because they engaged in activity that, while wholly innocent, is defined by Defendants to have a potential nexus to terrorism. This alone gives them the requisite personal stake in this litigation. They have also suffered additional injuries as a result of being reported, including: the wrongful dissemination of their personal information; reputational injury from being branded as potential terrorists; undue law enforcement scrutiny, including questioning and investigation by the FBI; anxiety and stress from the wrongful dissemination of their information; and interference with their artistic pursuit of photography. Defendants fail to acknowledge most of these injuries, which are concrete and cognizable. These injuries also establish standing for prospective relief because they are ongoing, and stem from Defendants' policies or officially sanctioned practices.

Moreover, Plaintiffs' injuries are fairly traceable to Defendants. Defendants directly inflict some harms – such as the wrongful dissemination of Plaintiffs' personal information. And the entities that reported Plaintiffs did so because they were implementing Defendants' Standards.

Second, Plaintiffs lack an adequate alternative remedy to this APA challenge. A suit against local police would not result in review of Defendants' unlawfully promulgated rules. Nor would it remedy Plaintiffs' injuries. Local police lack the ability to remove Plaintiffs' information from federally maintained databases or stop the FBI from investigating Plaintiffs.

Third, Defendants' rules constitute final agency action. The Supreme Court has rejected

Defendants' argument that agency action is only final if it *requires* compliance. *See Bennett v. Spear*, 520 U.S. 154, 177-78 (1997) (agency action final even though affected entity "not legally obligated" to comply). In any event, Defendants' rules have the practical effect of being binding, and Defendants have repeatedly evinced the expectation that NSI participants will comply.

Fourth, Defendants' rules purport to authorize action that is prohibited by federal regulation and are thus not in accordance with law. They directly conflict with 28 C.F.R. Part 23's requirement that criminal intelligence not be collected or maintained unless supported by reasonable suspicion, and they therefore have dramatically expanded the universe of personal information that is shared nationwide. Defendants' only defense is that the regulation does not apply. This contention rests on disputed factual assertions about the purpose of the NSI, the nature of SARs, and the databases and systems used to share them. Defendants also read the regulation to mean that it does not apply unless the information collected is already supported by reasonable suspicion; in other words, because SARs are unsupported by reasonable suspicion, they may be collected and maintained. This entirely circular reading of the regulation would mean that its core privacy protection does not apply in precisely those circumstances when it is being violated. This interpretation strays from the regulatory text and renders the regulation meaningless. It must be rejected.

Fifth, Defendants' rules are also invalid because they are legislative rules that were issued without notice and comment.

Finally, Plaintiffs may be joined in this action because they all challenge the same government policies.

II. BACKGROUND

A. Defendants Have Created a Uniform, National System for Collecting, Vetting, and Disseminating Intelligence About Individuals Considered to Have a Potential Nexus to the Crime of Terrorism

The federal government created the NSI to facilitate the nationwide sharing of information potentially related to terrorism. *See* Compl. ¶ 22. The premise of the NSI is that state, local, and tribal law enforcement agents – so called "front line" personnel – are well situated to capture threat information on the ground, but that the information they report must be vetted according to

uniform standards. *See id.*, Exh. D at 58, 60. Defendant Department of Justice ("DOJ") and Program Manager of the Information Sharing Environment ("PM-ISE") have thus each issued a rule governing SAR reporting, the purpose of which is to provide a uniform standard for evaluating information collected by front line personnel before it is disseminated nationally. *Id.* ¶¶ 10, 16, 42, 53, 48, 61.

DOJ set forth its standard ("DOJ SAR Standard") in various documents, including the eGuardian 2008 Privacy Impact Assessment ("2008 eGuardian PIA"). *Id.* ¶¶ 54, 56-58 & Exhs. E-J. PM-ISE set forth its standard in a document titled "Information Sharing Environment (ISE) – Functional Standard (FS) – Suspicious Activity Reporting (SAR) Version 1.5." *Id.* ¶ 44 & Exh. D ("Functional Standard 1.5" and collectively hereinafter "Defendants' Standards").[1]

1. Overview of SAR Information Flow

The SAR process created by Defendants proceeds in three stages: collection by front line personnel, vetting by trained analysts at fusion centers, and dissemination to law enforcement nationwide. *Id.*, Exh. D at 60-62.

Collection. Front line personnel are trained in Defendants' Standards, collect information about people engaged in activities that purportedly have a potential nexus to terrorism, and submit the information in the form of a SAR either directly to the Federal Bureau of Investigation ("FBI"), a component of Defendant DOJ, or to a fusion center. *Id.* ¶ 24.

Vetting. Fusion centers are focal points of the NSI. *Id.* ¶ 23. Fusion centers, which are federally funded, gather, receive, store, analyze, and share intelligence, including SARs, related to terrorism and other threats. *Id.* ¶¶ 23, 25. Although local collecting agencies perform some vetting, this responsibility rests primarily with fusion centers, whose staff are trained in Defendants' Standards and review SARs for compliance with those Standards. *Id.* ¶¶ 23-26 &

[1] Defendants contend that DOJ adheres to the same standard as PM-ISE, as evidenced by an updated privacy impact assessment dated January 2013. Gov. Br. at 10. This factual contention does not appear relevant to the legal issues in this motion and moreover conflicts with the Complaint's allegations and should therefore be disregarded. *See, e.g.*, Compl. ¶¶ 54 (according to March 2013 government report, which postdates January 2013 privacy impact assessment, FBI uses definition of SARs set forth in 2008 PIA); 59 (according to same report, the FBI trains fusion center analysts to submit SARs even when they do not satisfy the PM-ISE standard).

Exh. D at 60-61, 84-86.

Dissemination. SARs that meet Defendants' Standards are then disseminated both regionally through the fusion center's database, and also nationally through eGuardian and/or another national database. *Id.* ¶ 26 & Exh. D at 86.[2] The FBI oversees eGuardian, which allows thousands of law enforcement personnel across the country to access the SARs that have been uploaded to it. *Id.* ¶ 11. The federal government maintains SARs sent to eGuardian for 30 years – even when the FBI has determined that a particular SAR has *no nexus* to terrorism. *Id.* ¶ 26.

2. Individuals Reported in SARs Face Law Enforcement Scrutiny

Under the process Defendants have created for handling SARs, individuals reported in a SAR automatically face law enforcement review and scrutiny, as well as an increased risk of being questioned or actively investigated by the FBI and other agencies.

At the collection stage, Defendant PM-ISE instructs the front line agency to respond to a reported observation of suspicious activity before submitting it to a fusion center by "gather[ing] additional facts through personal observations, interviews, and other investigative activities. This may, at the discretion of the [responding] official, require further observation or engaging the suspect in conversation." *Id.* ¶ 27(a) (quoting Functional Standard 1.5 at 32).

At the vetting stage, Defendant PM-ISE instructs fusion center personnel to assess SARs before providing them to the FBI, including by engaging in investigative work "such as interviewing the individual engaged in suspicious activity." *Id.* ¶ 27(b).

After the fusion center disseminates a SAR, the subject faces additional scrutiny. The FBI takes action on all SARs it receives from fusion centers, including by interviewing the subject of

[2] Plaintiffs object to Defendants' request for judicial notice of the asserted fact that eGuardian is the *only* system used to share SARs. *See* Gov. Br. at 9 n.3. This "fact" conflicts with the Complaint's allegations that multiple databases are involved. *See* Compl. ¶¶ 26 (SARs vetted by fusion centers uploaded to one or more national databases); 73 ("state, local, and tribal law enforcement agencies and fusion centers" also operate systems used to collect, maintain, and disseminate SARs). Courts may only take judicial notice of facts "not subject to reasonable dispute." Fed. R. Evid. 201(b)(2); *see Lee v. City of Los Angeles*, 250 F.3d 668, 690 (9th Cir. 2001) (district court erred in taking "judicial notice of *disputed* facts stated in public records" on motion to dismiss) (emphasis in original). There is no exception for "facts…on government websites." *See* Gov. Br. at 9 n.3; *Paralyzed Veterans of Am. v. McPherson*, No. C064670SBA, 2008 WL 4183981 at *5 (N.D. Cal. Sept. 9, 2008) (facts judicially noticed were "not disputed").

the SAR, engaging in a threat assessment, or opening a full-blown investigation. FBI agents have admitted that they are required to follow up on SARs even when they know the individual does not pose a threat. *Id.* ¶ 27(c)-(d). Once uploaded to a national database, the subject of a SAR also faces further scrutiny and potential investigation by the many law enforcement agencies across the country, besides the FBI, with access to the database. *Id.* ¶ 27(e).

3. Collection and Dissemination of Personal Information

A SAR effectively creates an intelligence "file" about the individual; the file contains her personal information and is disseminated to law enforcement agencies through one or more databases of information related to potential terrorist activity. SARs contain "[p]ersonally identifiable information (PII) …, such as name, date and place of birth, unique identifying numbers, physical description, and similar attributes." *Id.*, Exh. E at 95. SARs in the eGuardian system are shared within Defendant DOJ and externally with other federal, state, local, and tribal law enforcement agencies. *See id.*, Exh. E at 102-03. Defendant DOJ acknowledges the "significant risk … that dissemination of personal information will be overly broad and will include agency officials who have no need to know the information"; the "privacy risk … that the sum of the data entered into eGuardian may be greater than its component parts…, as well as a risk of public misperception and possible misunderstanding." *Id.*, Exh. E at 97 & 105.

4. The Governing Standard for Reporting Criminal Intelligence

Long before the creation of the NSI, Congress and DOJ addressed the privacy concerns DOJ would later identify in connection with the dissemination of SARs. The solution was to prohibit the collection, maintenance, and dissemination of criminal intelligence absent reasonable suspicion of criminal activity.

In 1968, Congress enacted the Omnibus Crime Control and Safe Streets Act, Pub. L. 90-351, which among other things created the Law Enforcement Administration Agency ("LEAA") within DOJ to oversee the distribution of federal grants to state and local law enforcement programs. *See* Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. 90-351, 82 Stat. 197. The statute also vested LEAA – and then its successor, the Office of Justice Programs ("OJP"), a component of Defendant DOJ – with the authority to prescribe "policy standards" that ensure that

"criminal intelligence systems operating through support under this chapter" do not "collect, maintain, [or] disseminate criminal intelligence information … in violation of the privacy and constitutional rights of individuals." 42 U.S.C. § 3789g(c) (2012).

The agency initiated a rulemaking process in 1978. Commenters on the then-proposed regulation "were concerned that the collection and maintenance of intelligence information should only be triggered by a reasonable suspicion that an individual is involved in criminal activity." *See* 43 Fed. Reg. 28,572 (June 30, 1978). The agency concurred, and the proposed regulation was "revised to require this criteria as a basis for collection and maintenance of intelligence information." *Id.* The first "[o]perating principle[]" of the final rule therefore provides that a "project shall collect and maintain criminal intelligence information concerning an individual only if there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity." 28 C.F.R. § 23.20(a).

DOJ amended the rule in 1993 to include a definition of "reasonable suspicion." *See* C.F.R. § 23.20. During that rulemaking, a commenter argued that the "reasonable suspicion" requirement was "not necessary." 58 Fed. Reg. 48,451 (Sept. 16, 1993). But the agency disagreed, replying:

> the potential for national dissemination of information in intelligence information systems, coupled with the lack of access by subjects to challenge the information, justifies the reasonable suspicion standard as well as other operating principle restrictions set forth in this regulation. Also, the quality and utility of 'hits' in an information system is enhanced by the reasonable suspicion requirement. Scarce resources are not wasted by agencies in coordinating information on subjects for whom information is vague, incomplete and conjectural.

Id. The regulation has remained unchanged since its last amendment in 1993. *See* Compl. ¶ 40.

The regulation is "applicable to all criminal intelligence systems operating through support under … 42 U.S.C. § 3711, et seq., as amended." 28 C.F.R. § 23.3(a). Section 3711 establishes OJP. *See* 42 U.S.C. § 3711. The regulation therefore applies to all criminal intelligence systems that operate through support from OJP.

In short, the regulatory history shows that DOJ adopted the reasonable suspicion requirement to protect privacy by constraining the type of information collected, maintained, and disseminated through OJP-funded criminal intelligence systems.

5. Defendants' Standards for Collecting, Vetting, and Disseminating Intelligence Related to Terrorism Conflict with 28 C.F.R. Part 23 and Were Issued Without Notice and Comment

Defendants PM-ISE and DOJ have created a uniform system for the collection, vetting, and dissemination of SARs, but they have done so by issuing standards that do not require reasonable suspicion and were not issued through APA notice and comment procedures.

The stated purpose of the NSI is to collect, vet, and disseminate intelligence about activities related to terrorism. According to Defendant PM-ISE, SARs "provid[e] specific indications about possible terrorism-related crimes" and are "vital to assessing, deterring, preventing, or prosecuting those involved in criminal activities associated with terrorism." *Id.*, Exh. D at 58.

In creating the SAR program, Defendants expressed the view that "the police officer on the street is often in the best position to observe suspicious behavior that may have national security implications," *id.*, Exh. E at 96, but that the information reported has to be vetted uniformly to maximize its utility in combating terrorism. *Id.*, Exh. D at 58 ("Standardized and consistent sharing of suspicious activity information … is vital"). The program thus relies on "[l]ocal law enforcement agencies or field elements of Federal agencies [to] gather and document suspicious activity information." *Id.*, Exh. D at 60. Defendants have issued Standards to create a "unified process" for SAR reporting by these various agencies. Gov. Br. at 6; *see also* Compl. ¶¶ 48, 61.

Defendant PM-ISE's Functional Standard 1.5 defines suspicious activity as "[o]bserved behavior *reasonably indicative* of pre-operational planning related to terrorism or other criminal activity." *See id.* ¶ 44 & Exh. D at 54 (emphasis added). The Standard also identifies sixteen categories of activity that satisfy its definition. These include criminal acts (cyber attacks, vandalism), but also entirely non-criminal, and in some instances First Amendment-protected, activities (photography, observation/surveillance). *See id.* ¶ 46 & Exh. D at 81-82.

PM-ISE expressly acknowledges that Functional Standard 1.5 requires "less than the 'reasonable suspicion' standard." *Id.* ¶ 45.

Like PM-ISE, DOJ has also issued a standard for suspicious activity reporting – "observed behavior that *may be indicative* of intelligence gathering or pre-operational planning related to terrorism, criminal or other illicit information." *See id.* ¶ 54 & Exh. E at 95 (emphasis added).

DOJ's SAR Standard is even broader than Functional Standard 1.5. *Id.* ¶ 55. For example, only 10% of the SARs from one fusion center that met DOJ's SAR Standard also satisfied Functional Standard 1.5. *Id.* ¶ 63. DOJ's SAR Standard is articulated in its 2008 eGuardian PIA. *See id.* ¶ 54. DOJ has enumerated categories of behavior that satisfy its "may be indicative" standard; these categories include, among other things, possessing a student visa but not being proficient in English, as well as a "catch-all" category of "acting suspiciously." *Id.* ¶¶ 56-58 & Exhs. F-J.

To effectuate the goal of creating a unified SAR process, Functional Standard 1.5 and DOJ's SAR Standard apply to all agencies that participate in the NSI. *Id.* ¶¶ 47, 60 & Exh. D at 53. Defendants train NSI participants to follow the Standards, and NSI participants follow them. *Id.* ¶¶ 47, 49, 59, 60. Both Functional Standard 1.5 and DOJ's SAR Standard purport to define the scope of suspicious activity that should be reported by participating agencies. *See id.* ¶¶ 48, 61. Information that meets these Standards is disseminated nationally. *See id.* ¶¶ 24, 26.

Participants in the NSI are required to adhere to Defendants' Standards. Functional Standard 1.5 states: "This ISE-FS applies to all departments or agencies that possess or use terrorism or homeland security information…." *Id.*, Exh. D at 53. It further provides: "This *ISE-SAR Functional Standard* will be used as the ISE-SAR information exchange standard for all ISE participants." *Id.*, Exh. D at 63 (underline added). Similarly, DOJ's eGuardian PIA states that "a standard definition of what constitutes a suspicious activity *will be used* by all participating agencies." *Id.*, Exh. E at 97 (emphasis added). DOJ enforces its Standard through a user agreement required of all entities accessing eGuardian. *Id.*, Exh. E at 93, 113-14.

Entities that participate in the NSI and that follow Defendants' Standards receive funding from OJP. *Id.* ¶¶ 23, 25, 47, 60, 73. OJP-funded entities, however, are required to comply with 28 C.F.R. Part 23. *See* 28 C.F.R. § 23.3(a). While the regulation permits OJP-funded entities to collect and maintain information only if supported by reasonable suspicion, *see* 28 C.F.R. § 23.20(a) & *supra* Part II-A-4, Functional Standard 1.5 and DOJ's SAR Standard expand the universe and purport to authorize OJP-funded entities to collect, maintain, and disseminate information even absent reasonable suspicion. *See* Compl. ¶¶ 45, 75. Functional Standard 1.5 and DOJ's SAR Standard, moreover, were issued without notice and comment. *Id.* ¶¶ 42, 53.

6. The NSI Has Not Proven Effective in the Fight Against Terrorism

Although tens of thousands of SARs have been found to satisfy Defendants' Standards and uploaded to national databases, the U.S. Government Accountability Office has faulted the program for failing to demonstrate *any* results-oriented outcomes, such as arrests, convictions, or thwarted threats. *Id.* ¶ 28; *id.* (citing another report discussing how SARs have "flooded…security entities with white noise"). SARs from fusion centers in California show that the NSI targets First Amendment-protected photography and encourages racial and religious profiling. Examples of SARs that met Defendants' Standards and were uploaded to the FBI's eGuardian database include: "Suspicious ME [Middle Eastern] Males Buy Several Large Pallets of Water" and "Female Subject taking photos of Folsom Post Office." *Id.* ¶ 29.

B. Plaintiffs Have Been Reported As "Suspicious" for Their Lawful Conduct

Plaintiffs have each been reported as "suspicious" for engaging in innocent activity.

Wiley Gill, a U.S. citizen and graduate of California State University, Chico, is the subject of a SAR. *Id.* ¶ 80-81. He converted to Islam after learning about the religion in a class. *Id.* ¶ 80. In 2012, the Chico Police Department ("CPD") conducted a search of his home without a warrant or voluntary consent, and for reasons later acknowledged to be unfounded; CPD reported the encounter and two earlier interactions with Gill in a SAR. *Id.* ¶¶ 83-86. The SAR notes that Gill "is unemployed" and states that he had "potential access to flight simulators via the internet" because his computer displayed a webpage titled something "similar to 'Games that fly under the radar.'" *Id.* ¶ 83 & Exh. A. Gill, a video game enthusiast, was likely viewing a website about video games. *Id.* ¶ 84. The SAR concludes by describing as "worthy of note" Gill's "full conversion to Islam as a young WMA [white, male adult]" and his "pious demeanor." *Id.* ¶ 83 & Exh. A. In describing Gill's religion as "worthy of note," CPD implicitly acknowledges that it found Gill suspicious because he is a devout Muslim. *Id.* ¶ 93. A few months later, a CPD officer called Gill, stated he had a report about him, asked him to take down his Facebook page (on which he displays a picture of the Shahada, the Muslim statement of faith), and warned him he was on a watchlist. *Id.* ¶ 92. The FBI has created a file about him. *Id.* ¶ 82.

Khaled Ibrahim, a U.S. citizen of Egyptian descent who works in accounting, is the subject

of a SAR describing his attempt to purchase "a large amount of computers." *Id.* ¶¶ 118, 121 & Exh. B. Ibrahim, who then worked as a purchasing agent, was seeking to make a bulk purchase of computers for his employer. *Id.* ¶¶ 118-21. Ibrahim resides in San Jose, California and the electronics store at issue is located in Alameda County (Dublin). *Id.* ¶¶ 118-19.

Tariq Razak, a U.S. citizen of Pakistani descent, is the subject of a SAR describing him as a "Male of Middle Eastern decent [sic] observed surveying entry/exit points" at the Santa Ana Train Depot, and departing with "a female wearing a white burka head dress." *Id.* ¶¶ 126-28 & Exh. C. At the time, Razak was visiting the county employment resource center, which is located at the train station; not having been there before, he had to look for the center. *Id.* ¶ 130. He was with his mother, who was wearing a head scarf, not a burka. *Id.*

Aaron Conklin, a graphic design student and amateur photographer with an interest in industrial architecture, is the subject of a SAR. *Id.* ¶¶ 137, 147. He has twice been prevented from photographing oil refineries. *Id.* ¶¶ 138-45. In an almost hour-long ordeal at the Shell refinery in Martinez, California, he was questioned by private security, and then detained and searched by Contra Costa Sheriff's deputies, who told him he had to be placed on an "NSA watch list." *Id.* ¶¶ 141-45. The incident occurred in Contra Costa County. *Id.* ¶ 141.

James Prigoff, a U.S. citizen and renowned photographer of public art, is the subject of a SAR or SAR-like report. *Id.* ¶ 101, 110. While attempting to photograph a famous piece of public art on a natural gas storage tank near Boston, he was harassed by private guards and prevented from taking photographs from his preferred location. *Id.* ¶¶ 102-06. Although he provided the guards no identifying information, the FBI subsequently tracked him cross-country, visited his home in Sacramento, and questioned a neighbor about him. *Id.* ¶¶ 104, 109-11.

Each Plaintiff engaged in entirely innocent conduct that does not give rise to any reasonable suspicion of criminal activity. *Id.* ¶¶ 89, 107, 120, 132, 146. But their conduct falls within categories Defendants have designated as "suspicious":

- Gill, who most likely was looking at a website about video games, was described as potentially having access to flight simulator games and being unemployed. *Id.* ¶ 83 & Exh. A. This fell under Defendant PM-ISE's categories of "[a]cquisition of [e]xpertise" and Defendant DOJ's categories of "no obvious signs of employment" and the catch-all category of "acting suspiciously." *Id.* ¶¶ 56(b), 57, 81, 94 & Exh. D at 82.

- Ibrahim's effort to make a bulk purchase of computers for his employer fell under Defendant PM-ISE's category of "[a]cquisition . . . of unusual quantities of materials," and Defendant DOJ's catch-all of "acting suspiciously," as well as, potentially, DOJ's "Potential Indicators of Terrorist Activities Related to Electronic Stores." *Id.* ¶¶ 57, 58, 122, Exh. D at 82 & Exh. I.

- Razak's efforts to locate the county employment resource center at the Santa Ana Train Depot fell under Defendant PM-ISE's category of "Observation/Surveillance," and Defendant DOJ's categories of "[u]nusual or prolonged interest in . . . [e]ntry points and access controls" and the catch-all of "acting suspiciously." *Id.* ¶¶ 57-58, 133, Exh. D at 82 & Exh. J (DOJ's "Potential Indicators of Terrorist Activities Related to Mass Transportation").

- Conklin's effort to photograph oil refineries fell under Defendant PM-ISE's category of "[p]hotography" of "infrastructure," and Defendant DOJ's catch-all of "acting suspiciously." ¶¶ 57, 147 & Exh. D at 81.

- Prigoff's effort to photograph public art on the side of a natural gas storage tank fell under Defendant PM-ISE's category of "[p]hotography" of "infrastructure" and Defendant DOJ's catch-all of "acting suspiciously." *Id.* ¶¶ 57, 112 & Exh. D at 81.

The SARs about Plaintiffs were each sent to a fusion center and then uploaded to eGuardian and/or another national SAR database, where they are maintained and will continue to be maintained, and where they can be accessed by law enforcement agencies across the country. *Id.* ¶¶ 26, 82, 100, 112, 115, 121, 125, 133, 136, 147.

The front line personnel who reported Plaintiffs and the fusion center personnel who shared Plaintiffs' SARs regionally and uploaded them to eGuardian or another national database were trained in Defendants' Standards. *Id.* ¶¶ 24, 26, 49, 59, 90, 113, 121, 129, 148.[3] Defendants Standards apply to participants in the NSI, who follow them. *Id.* ¶¶ 47, 49, 59-60.

Because they engaged in conduct that fell under Defendants' Standards, Plaintiffs have all been subjected to law enforcement scrutiny. *Id.* ¶¶ 27, 97, 114, 123, 134, 149. Gill and Prigoff have faced actual questioning and investigation. A CPD officer called Gill, querying him about his Facebook page, and the FBI has conducted background checks and created a file about him. *Id.* ¶¶ 82, 92, 97. The FBI visited Prigoff's home, seeking to question him and a neighbor. *Id.* ¶ 114. Gill and Conklin experience worry and stress as a result of their SARs. *Id.* ¶¶ 99, 152.

[3] With respect to Prigoff, Plaintiffs allege that the report about him was collected, maintained, and disseminated based on standards that authorize collection, maintenance, and dissemination even in the absence of reasonable suspicion of criminal activity and that Defendants' Standards ratify that conduct. *Id.* ¶¶ 112-13.

III. LEGAL STANDARD

In ruling on a motion to dismiss, a court must "accept all factual allegations of the complaint as true and draw all reasonable inferences in favor of the nonmoving party." *W. Ctr. for Journalism v. Cederquist*, 235 F.3d 1153, 1154 (9th Cir. 2000). This standard applies to motions to dismiss for lack of standing. *See Warth v. Seldin*, 422 U.S. 490, 501 (1975).

IV. ARGUMENT

A. Plaintiffs Allege Sufficient Facts to Establish Standing

Plaintiffs have standing to challenge Defendants' SAR Standards. Each of the elements of standing – injury, causation, and redressability – is present here. *See Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992).

1. Plaintiffs' Injuries Are Particularized, Concrete, and Cognizable

Plaintiffs allege that they have each been reported as engaged in "suspicious" activity with a potential nexus to terrorism. This alone gives them a sufficient personal stake in this suit for standing. But Plaintiffs also suffer numerous injuries flowing from the collection and dissemination of the SARs about them. Reports containing their personal information have been disseminated to law enforcement agencies nationwide, injuring Plaintiffs' reputations and subjecting Plaintiffs to law enforcement scrutiny. Some Plaintiffs have experienced anxiety and stress, and others have been prevented from engaging in artistic pursuits. Defendants fail to address most of these injuries.

The purpose of the injury-in-fact requirement is to distinguish plaintiffs with a concrete interest in the outcome of the dispute from those with a generalized grievance. *See id*. at 573-74. The "critical" question is whether the plaintiffs possess a "personal stake" in the suit. *Camreta v. Greene*, _U.S._, 131 S. Ct. 2020, 2029 (2011). Gill, Ibrahim, and Razak have a personal stake in the rules governing the SAR program because each is the subject of a SAR. *See* Compl., Exhs. A-C. In addition, the Complaint supports "[t]he reasonable inference" that the remaining two Plaintiffs are also the subject of a SAR or SAR-like report, and thus have the requisite personal stake. *See Ibrahim v. Dep't of Homeland Sec.*, 669 F.3d 983, 992 (9th Cir. 2012) (plaintiff had standing to challenge the inclusion of her name on government watchlists where "[t]he reasonable

inference to draw from [the] complaint is that she is on one or more government watchlists"). Conklin was detained and searched by sheriffs' deputies for photographing a refinery – conduct which falls under at least one of the categories of behavior Defendants define as suspicious (photographing infrastructure) – and told he would be put on an "NSA watchlist." *See* Compl. ¶¶ 138-47. Prigoff was confronted by private security guards in Massachusetts to whom he provided no identifying information, but was subsequently contacted by the FBI at his home in California, also for photographing infrastructure. *See id.* ¶¶ 102-12. Because Plaintiffs were each reported in a SAR for activity that met Defendants' definition of "suspicious," they are "among the injured" in a way that "the public at large" is not. *Lujan*, 504 U.S. at 563, 574. This suffices to establish injury-in-fact.[4]

In any event, Plaintiffs have suffered at least five additional types of injuries resulting from their SARs. Defendants completely fail to address all but one of these harms.

First, Plaintiffs are injured by the wrongful collection and dissemination of their personal information. District courts in this Circuit "routinely den[y] motions to dismiss based on Article III standing where a plaintiff alleges that his personal information was collected *and then wrongfully disclosed*, as opposed to [merely] alleging that his personal information was collected without his consent." *In re Sony Gaming & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 961-62 (S.D. Cal. 2014) (emphasis added). Plaintiffs allege that SARs containing their personal information have been collected *and disseminated* to law enforcement agencies across the country. *See* Compl. ¶¶ 82, 100, 112, 115, 121, 125, 133, 136, 147, 151. Plaintiffs' interest in not having their personal information wrongfully disseminated is the very privacy interest 28 C.F.R.

[4] Defendants offer factual arguments to argue that Prigoff could not have been the subject of a SAR. *See* Gov. Br. at 19. The Complaint supports the reasonable inference that he was the subject of a SAR or SAR-like report: How else could the FBI have tracked him to his home in Sacramento about an incident in Boston? On this motion to dismiss, the Court should not decide factual issues or draw inferences against Plaintiffs. *See Ibrahim*, 669 F.3d at 992 (rejecting government's factual argument that plaintiff could not have been on no fly list because she was allowed to fly and reasonably inferring from other allegations she was on a watchlist). Further, because the other Plaintiffs have standing, the Court need not reach the government's challenge to Prigoff. *See Vill. of Arlington Heights v. Metro. Hous. Dev. Corp.*, 429 U.S. 252, 264 n.9 (1977) (presence of one plaintiff with standing obviates need to consider standing of others).

Part 23 and 42 U.S.C. § 3789g(c) are intended to safeguard. *See supra* Part II-A-4.

Second, Plaintiffs suffer reputational injury from being branded as persons with a potential nexus to terrorism. *See* Compl. ¶ 111 (FBI questioning of neighbor suggested Prigoff committed misconduct) & Exh. E at 105 (eGuardian PIA acknowledging "risk of public misperception" from dissemination of SARs); *see also id.* ¶¶ 2, 99, 117, 124, 135, 151; *Meese v. Keene*, 481 U.S. 465, 474-75 (1987) (plaintiff had standing to challenge statute labeling films he exhibited as "political propaganda" because of "risk of injury to his reputation"); *Joint Anti-Fascist Refugee Comm. v. McGrath*, 341 U.S. 123, 131, 140-41 (1951) (organizations had "clear" standing to challenge loyalty oath based on injury, *inter alia*, to "reputation").

Third, Plaintiffs are injured because the SARs program sweeps them into a law enforcement net. This is the only injury Defendants discuss. Under Defendants' process for vetting SARs, *all* individuals reported in a SAR automatically face law enforcement scrutiny. *See* Compl. ¶ 27 & *supra* Part II-A-2. In addition, a subset of these individuals will face direct questioning and active investigation by the initial responding agency, fusion center staff, the FBI, and/or other law enforcement agencies that have access to a SAR database. *See* Compl. ¶ 27.

In *Hemp Indus. Ass'n v. DEA*, 333 F.3d 1082 (9th Cir. 2003), the Ninth Circuit held that the risk of enforcement proceedings by the DEA, even in the absence of actual enforcement proceedings, gave plaintiffs standing to challenge a DEA regulation. *Id.* at 1086-87. And in *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010), the Ninth Circuit held that plaintiffs had standing to sue Starbucks over the theft of a company laptop containing their personal information because they faced an increased risk of identity theft, even though no plaintiff had yet become a victim of identity theft. *Id.* at 1142. The threat of harm was credible because the laptop had actually been stolen. *Id.* at 1143.

Plaintiffs' injuries easily satisfy the standard set forth in *Hemp Industries* and *Krottner*. Just as the risk of the government instituting an enforcement proceeding constitutes cognizable harm, so too does the government *actually scrutinizing an individual* for a potential connection to terrorism. Defendants' characterization of Plaintiffs' injuries as "conjectural or hypothetical" "future" injuries ignores the allegations of the Complaint, which make clear that all individuals

reported in a SAR suffer the *present* injury of being automatically subjected to law enforcement scrutiny. *See* Compl. ¶¶ 2, 27, 97, 114, 123, 134, 149.

Additionally, Plaintiffs face the related but separate injury that this scrutiny will take the form of direct questioning or an active investigation by law enforcement. As Defendants acknowledge, Gill and Prigoff have been victims of such encounters. *See id*. ¶¶ 97, 114.[5] But even those who have not yet been questioned have standing because they face an increased risk of such intrusions. Defendants' process for vetting SARs places reported individuals into a small pool of people, separate from the general population, who are targeted for questioning and/or investigation. Just as in *Krottner*, in which the theft of the laptop with personal data rendered the risk of identity theft credible for those people whose data had actually been stolen, here Defendants' process for vetting SARs renders the risk of questioning and investigation credible for those who, like each of the Plaintiffs, have actually been reported. The threat of questioning and investigation is credible because that is precisely what Defendants' process calls for.[6]

Fourth, Gill and Conklin suffer frustration, worry, and stress as a result of the dissemination of SARs about them. *See* Compl. ¶¶ 99, 150-52; *Krottner*, 628 F.3d at 1142 (plaintiff alleging "generalized anxiety and stress" as a result of theft of laptop had standing).

Fifth, Prigoff and Conklin have suffered aesthetic and recreational injuries because of the interference with their photography. *See* Compl. ¶¶ 106 (because of harassment by guards, Prigoff forced to photograph from location with inferior lighting), 113, 116, 138-45 (Conklin twice prevented from photographing); *Cantrell v. City of Long Beach*, 241 F.3d 674, 680 (9th Cir. 2001)

---

[5] There is nothing "metaphysical" about being questioned by the authorities. *Cf.* Gov. Br. at 19. At a minimum, such an interaction causes delay and interferes with daily life. *See Ibrahim*, 669 F.3d at 993 (plaintiff had standing where she "will suffer delays…resulting from the presence of her name on the No-Fly list").

[6] Defendants' reliance on *Clapper v. Amnesty Int'l, U.S.A.*, _U.S._, 133 S. Ct. 1138, 1147 (2013), is misplaced. The plaintiffs in that case, challenging a program to monitor communications with foreign actors, included human rights organizations that communicated with foreign individuals believed likely to be the targets of U.S. government surveillance. *Id.* at 1145. The Supreme Court held that plaintiffs lacked standing because they "fail[ed] to offer any evidence that their communications have been monitored," and the Court held it too speculative that plaintiffs' communications would someday be surveilled under the statute they sought to challenge. *Id.* at 1148. In contrast, Plaintiffs here allege that they are the subjects of SARs and so are already targets of the program they challenge.

(injury in fact established by allegation that "challenged activity" interferes with plaintiffs' "aesthetic and recreational" interests). They are not merely "chilled," *cf.* Gov. Br. at 21, but have already suffered actual interference with their aesthetic pursuits.

Further, Plaintiffs' injuries establish standing for prospective relief for two independent reasons. *Cf. City of Los Angeles v. Lyons*, 461 U.S. 95 (1983) (standing for injunctive relief requires realistic threat of repetition). Many of Plaintiffs' injuries are present and ongoing, *see, e.g.*, Compl. ¶¶ 100, 115, 125, 136, 147 (continued maintenance and dissemination of Plaintiffs' personal information), rendering inapplicable *Lyons*' requirement to show a threat of repetition. *See, e.g.*, *Haro v Sebelius*, 747 F.3d 1099, 1109 (9th Cir. 2014). In addition, further law enforcement encounters are likely to recur because those encounters arise from Defendants' policies or officially sanctioned practices. "[A] plaintiff can demonstrate that [an] injury is likely to recur" if it stems from "a written policy" and/or a "pattern of officially sanctioned … behavior." *Melendres v. Arpaio*, 695 F.3d 990, 998 (9th Cir. 2012). Plaintiffs allege that such policies and officially sanctioned behaviors – PM-ISE's Functional Standard 1.5 and DOJ's SAR Standard – are the genesis of the SARs filed about them and the law enforcement scrutiny they face. Compl. ¶¶ 95-97, 112-14. 122-123, 133-134, 147-49. Plaintiffs cannot avoid being the subject of a future SAR or further law enforcement questioning related to an existing SAR "by avoiding illegal conduct." *Melendres*, 695 F.3d at 998 ("standing is not appropriate where a plaintiff can avoid injury by avoiding illegal conduct"). "[E]ven if the Plaintiffs comply with all criminal laws," they "remain vulnerable" to law enforcement scrutiny and attention under the NSI precisely because Defendants encourage reporting of information even without reasonable suspicion of criminal activity and require law enforcement follow-up on all SARs. *Id.* at 998.

2. Plaintiffs' Injuries Are Fairly Traceable to Defendants' Standards

Defendants instruct front line personnel to report "suspicious activity" in conformity with Defendants' Standards. The fact that front line personnel submitted the reports about Plaintiffs does not defeat causation. *Cf.* Gov. Br. at 17-18. Indeed, it shows that Defendants' Standards for reporting suspicious activity worked as Defendants intended.

First, Defendants' third-party argument ignores the injuries they directly inflict:

maintenance and dissemination of Plaintiffs' personal information and investigation of individuals reported in SARs by Defendant DOJ's component, the FBI. *See* Compl. ¶¶ 26-27, 82, 100, 114-15, 125, 136, 147.

Second, Defendants promulgated Standards for suspicious activity reporting that they specifically contemplated would be performed by front line personnel. *See supra* Part II-A-5. Defendants plainly evince the expectation that such actors will adhere to their Standards, which they mandate "will be used" for suspicious activity reporting. *See, e.g.*, Compl., Ex. D at 63, Ex. E at 97. Plaintiffs each engaged in behavior defined as "suspicious" under Defendants' Standards. *See supra* Part II-B. The entities that reported Plaintiffs were provided with, trained in, instructed to follow, and did follow Defendants' Standards for reporting suspicious activity. And fusion center personnel vet SARs and upload them to national databases only if they comply with Defendants' Standards. *See id*. ¶¶ 26, 47, 49, 59-60, 94-95, 112-13, 121-22, 129, 133, 147-48. The causal chain between Defendants' Standards and Plaintiffs' harms is anything but "speculative and unfounded." Gov. Br. at 17. It is direct, immediate, and unbroken.[7]

Mendia v. Garcia, 768 F.3d 1009 (9th Cir. 2014), cited by Defendants, supports Plaintiffs' position. *Mendia* found causation where, as here, a plaintiff sued a federal defendant for a harm directly inflicted by a local entity. *Id.* at 1011-12 (plaintiff had standing to sue Immigration and Customs Enforcement for his allegedly unlawful pre-trial detention on state criminal charges by

[7] Implicitly conceding causation, Defendants do not challenge redressability. *Cf. Humane Soc'y v. Hodel*, 840 F.2d 45, 51 n. 5 (D.C. Cir. 1988) (redressability "melds into" causation). This factor is easily satisfied. *See Renee v. Duncan*, 686 F.3d 1002, 1013 (9th Cir. 2012) (plaintiff need only show injury "likely to be redressed by invalidation of the federal regulation"; "plaintiffs' burden is 'relatively modest'") (citation omitted). First, as noted above, Defendants directly inflict injuries on Plaintiffs; these injuries would be redressed by an order requiring Defendants to cease their illegal conduct. *See Hein v. Freedom From Religion Found., Inc.*, 551 U.S. 587, 639 (2007). Second, Plaintiffs' injuries would also be redressed if participants in the NSI ceased collecting, maintaining, and disseminating SARs about individuals, like Plaintiffs, whose conduct does not give rise to reasonable suspicion. Just as participants in the NSI currently follow Defendants' SAR Standards in collecting, maintaining, and disseminating SARs, they would follow any new instructions on SAR reporting issued by Defendants. *See* Compl. ¶¶ 47, 60, 78-79. Third, courts find redressability where, as here, plaintiffs raise a procedural claim under the APA because the injury would be redressed if the agency followed the required notice and comment. *See, e.g., Yesler Terrace Cmty. Council v. Cisneros*, 37 F.3d 442, 447 & n.4 (9th Cir. 1994).

local authorities where ICE lodged immigration detainer and bondsmen declined to provide the bond he needed to post bail when they learned of ICE detainer). "Causation may be found even if there are multiple links in the chain connecting the defendant's unlawful conduct to the plaintiff's injury, and there's no requirement that the defendant's conduct comprise the last link in the chain." *Id.* at 1012. Indeed, causation is substantially stronger here than in *Mendia*. Unlike the third parties in *Mendia*, the front line agencies who submit SARs and the fusion center personnel who vet and forward them are implementing and not merely reacting to the federal agencies' policy.[8]

B. The Complaint States Claims Under the Administrative Procedure Act

1. A Suit Against Local Police or Private Guards Is Insufficient to Remedy Harms Caused by the Federal Defendants

Defendants argue that Plaintiffs' APA claims are barred because Plaintiffs have adequate, alternative remedies – namely, suing the individual local agencies or private guards that collected SARs about them. Gov. Br. at 22. Defendants misunderstand Plaintiffs' claims and their injuries. Plaintiffs seek review of rules that are arbitrary and capricious and promulgated in violation of APA-required notice and comment, in order to remedy injuries flowing from these unlawful rules. APA review is available where, as here, Plaintiffs challenge unlawful agency rules and, relatedly, because Defendants' proposed alternative would not remedy Plaintiffs' injuries. Because local agencies and private guards cannot withdraw Defendants' improperly promulgated SAR Standards, remove Plaintiffs' personal information from federal databases, or stop the FBI from investigating Plaintiffs, the APA does not bar Plaintiffs' claims.[9]

In the APA, Congress waived sovereign immunity for suits challenging federal agency

[8] Defendants suggest that front line personnel who reported Plaintiffs were actually motivated by factors unrelated to Defendants' Standards. That is "the sort of factual issue that can't be resolved in the context of a facial attack on the sufficiency of a complaint's allegations." *Mendia*, 768 F.3d at 1014. Defendants, for example, state that the guard who reported Plaintiff Razak stated that she reported the incident based on training "from a local police agency." Gov. Br. at 19. Plaintiffs are entitled to explore in discovery, *inter alia*, whether the guard correctly recalled the agency that trained her, and whether, if she did receive training directly "from a local police agency," it was based on Defendants' Standards.

[9] Plaintiffs challenge Functional Standard 1.5 and DOJ's SAR Standard, which were issued, respectively, on or about May 21, 2009 and November 25, 2008. *See* Compl. ¶¶ 44, 54, 153-68, Exh. D at 56 & Exh. E at 90. These claims are timely. *See* 28 U.S.C. § 2401(a) (6-year statute).

actions that seek relief other than money damages and for which there is "no other adequate remedy in court." 5 U.S.C. §§ 702, 704. The APA's "generous review provisions must be given a hospitable interpretation" and "only upon a showing of clear and convincing evidence of a contrary legislative intent should the courts restrict access to judicial review." *Heckler v. Chaney*, 470 U.S. 821, 843 (1985) (internal quotation marks, citation omitted). The purpose of the "other adequate remedy" language is not to limit judicial review of agency actions, but to avoid creating "additional judicial remedies in situations where the Congress has provided special and adequate review procedures." *Bowen v. Massachusetts*, 487 U.S. 879, 903 (1988).

There is no bar to judicial review where the "alternative" asserted is insufficient to remedy plaintiffs' injuries. APA review is thus available where the plaintiff challenges agency rule-making and the proposed alternative would not result in a review of that rule-making; any other approach would mean that an agency can illegally promulgate rules without fear of judicial review. *See, e.g.*, *Chang v. United States*, 327 F.3d 911, 924 (9th Cir. 2003) (removal proceedings not adequate because "immigration judge in removal proceedings cannot hear the sorts of claims at issue here, which include . . . whether APA notice and comment was required before promulgating new rules"); *Food Town Stores v. Equal Emp't Opportunity Comm'n*, 708 F.2d 920, 923 n.2 (4th Cir. 1983) (allowing APA challenge to, *inter alia*, EEOC regulation governing availability of subpoenas in administrative proceedings, despite availability of trial on the merits at a later date, because "[t]he EEOC regulation…would not be reviewable in that action"); *Habeas Corpus Res. Ctr. v. Dep't of Justice*, No. C 13-4517 CW, 2014 WL 3908220, at *5 (N.D. Cal. Aug. 7, 2014) (allowing APA challenge to final rule on procedure for certifying fast-track habeas appeals because, although Congress had created a certification review process, "the review provided for... is a review of individual certification decisions, not review of the regulations themselves").

Similarly, a suit that can only yield a money judgment is not an adequate alternative to a claim seeking equitable relief. *See, e.g.*, *Bowen*, 487 U.S. at 925 (money judgment available in Claims Court not adequate substitute for APA claim seeking reimbursement under Medicaid Act); *Transohio Sav. Bank v. Dir., Office of Thrift Supervision*, 967 F.2d 598, 608 (D.C. Cir. 1992) (claim for money damages not an adequate alternative to APA claim seeking declaratory relief).

Defendants mischaracterize the Complaint as alleging improper conduct by non-party police and private security guards. As in *Chang*, *Food Town*, and *Habeas Corpus*, Plaintiffs here challenge rules promulgated in violation of the APA. Compl. ¶¶ 153-68.[10] Defendants have not explained how Plaintiffs could obtain review of these rules, other than through the APA.[11]

Because of Defendants' unlawful rules, Plaintiffs have been reported in SARs and their information continues to be maintained in one or more national databases, with the result that, *inter alia*, (i) their personal information has been widely disseminated; (ii) they have been branded as having a "nexus to terrorism"; (iii) they face undue law enforcement scrutiny; (iv) some have actually been questioned and investigated by the FBI, while the others face an increased risk of such an intrusion; and (v) they suffer stress and anxiety as a result of the dissemination of SARs about them. *See supra* Part IV-A-1.

Defendants do not – and cannot – identify any claims Plaintiffs could bring against "police and private security companies" to address these injuries. *See Toxco Inc. v. Chu*, 724 F. Supp. 2d 16, 25-26 (D.D.C. 2010) (denying motion for summary judgment because "defendant has not explained how the remedies available [] would provide an alternative adequate remedy so as to satisfy the requirements of 5 U.S.C. § 704."). Only Defendants have the power to withdraw their improperly promulgated SAR Standards, which are the source of Plaintiffs' injuries. Nor would a suit against local police or private guards lead to removal of Plaintiffs' information from federally-maintained databases,[12] or prevent the FBI from investigating Plaintiffs. *Cf. Bowen*, 487 U.S. at 925 (money judgment not adequate alternative to equitable relief).

Defendants' cases are distinguishable. *Brem-Air Disposal v. Cohen*, 156 F.3d 1002 (9th Cir. 1998), stands for the unremarkable proposition that where Congress has created a private right

[10] Indeed, in arguing that venue does not lie in this district, Defendants acknowledge that Plaintiffs "challenge[] Defendants[']' issuance of guidance" regarding SARs. Gov. Br. at 33.
[11] Defendants cite *Coker v. Sullivan*, 902 F.2d 84, 90 n.5 (D.C. Cir.1990) for the principle that an alternative remedy does not necessarily have to have an effect "upon the challenged agency action" in order to be found adequate. *See* Gov. Br. at 22. *Coker* was a challenge to an agency's discretionary decision not, as here, a challenge to an unlawful agency rule-making.
[12] The federal government maintains SARs sent to the FBI's eGuardian system for 30 years, even when the FBI determines that the SAR has no nexus to terrorism. Compl. ¶ 26.

of action to challenge improper agency action, plaintiffs must use the remedy provided, not the APA. *Id*. at 1004 (Resource Conservation and Recovery Act provides cause of action to enforce its provisions, thus precluding APA claim). Similarly, *Garcia v. McCarthy*, 13-CV-03939-WHO, 2014 WL 187386 (N.D. Cal. Jan. 16, 2014), turned on the fact that State of California had explicitly created a judicially reviewable procedure by which plaintiffs could challenge the permitting process that had injured them. *Id.* at *13-14. Defendants have not identified any alternative mechanism for challenging the improperly promulgated rules that have injured them.[13]

2. Plaintiffs Have Adequately Alleged That Functional Standard 1.5 and DOJ's SAR Standard Each Constitute Final Agency Action

Both Functional Standard 1.5 and DOJ's SAR Standard constitute final agency action because they have the practical effect of being binding and Defendants expect compliance with their Standards. State and local law enforcement agencies may participate in the NSI, and the SARs they collect will be disseminated, if and only if they comply with Defendants' Standards. Defendants' assertion that NSI participants are not required to follow the Standards mischaracterizes the law and factual allegations. If true, it would also undermine Defendants' purpose in issuing their Standards, which was to ensure uniformity in SAR reporting by NSI participants. In addition, the Standards are final agency action because they affect the rights of individuals not to have their personal information disseminated without reasonable suspicion.

In *Bennett v. Spear*, 520 U.S. 154 (1997), the Supreme Court set out the legal standard for agency action to be considered final:

> First, the action must mark the "consummation" of the agency's decisionmaking process—it must not be of a merely tentative or interlocutory nature. And second, the

[13] Defendants' other cases are also distinguishable because none challenged, as here, an agency rule as unlawful. *See Rimmer v. Holder*, 700 F.3d 246 (6th Cir. 2012) (FOIA was appropriate vehicle for seeking disclosure of agency records); *Garcia v. Vilsack*, 563 F.3d 519 (D.C. Cir. 2009) (challenge to agency's allegedly discriminatory distribution of farm benefits); *Turner v. Secretary of U.S. Dep't of Hous. and Urban Dev.*, 449 F.3d 536 (3rd Cir. 2006) (challenge to agency's determination that there was no reasonable cause to believe plaintiff's landlord had engaged in discrimination); *Jersey Heights Neighborhood Ass'n v. Glendening*, 174 F.3d 180 (4th Cir. 1999) (challenge to federal agencies' allegedly discriminatory siting of highway in plaintiffs' neighborhood); *Washington Legal Found. v. Alexander*, 984 F.2d 483, 486 (D.C. Cir. 1993) (challenge to agency's failure to enforce statute and policy prohibiting discrimination).

> action must be one by which "rights or obligations have been determined," or from which "legal consequences will flow."

Id. at 177-78 (citations omitted). Defendants concede the first prong, but challenge the second, asserting that Functional Standard 1.5 does not impose a "binding legal norm," but merely provides "functional guidance for the operation of the NSI" and that NSI participants are not "require[d]" to follow this guidance. Gov. Brief at 24.[14]

The Supreme Court in *Bennett* rejected Defendants' argument that agency action is only "final" if it *requires* compliance. Petitioners in *Bennett* challenged a biological opinion issued by the Fish and Wildlife Service pursuant to the Endangered Species Act regarding the operation of a dam by the Bureau of Reclamation. *Bennett*, 520 U.S. at 157. The opinion found that the dam's operation would jeopardize endangered fish and identified various measures that would avoid harm. *Id.* at 159. The defendant agency argued that the biological opinion was not "final" because "the Bureau was not legally obligated" to adopt its recommendations. *Id.* at 177. The Supreme Court disagreed: "the Biological Opinion . . . alter[ed] the legal regime" because the Bureau was "authoriz[ed] to take the endangered species if (but only if) it complies with the prescribed conditions." *Id.* at 178.

It is true that neither of Defendants' Standards mandate that any state or local law enforcement agency participate in the NSI and share SARs that meet their Standards. However, Defendants do mandate that *if* a state or local law enforcement agency participates in the NSI and submits SARs, it does so consistent with the SAR standard. *See, e.g.*, Compl., Exh. D at 63 & Exh. E at 97, 114-15. This condition on participation renders Defendants' Standards, like the biological opinion in *Bennett*, final agency action.

In addition, "there are several avenues for meeting the second finality requirement." *Oregon Natural Desert Ass'n v. U.S. Forest Serv.*, 465 F.3d 977, 986 (9th Cir. 2006). Defendants' Standards have a determinative effect on "rights or obligations." *Bennett*, 520 U.S. at 178. In

[14] Defendants confuse the 2008 eGuardian PIA with DOJ's SAR Standard. Plaintiffs do not challenge the preparation of the eGuardian PIA, *cf.* Gov. Br. at 27, so it is not necessary to show that the PIA is a final agency action. Instead, Plaintiffs' challenge DOJ's SAR Standard, which is articulated in the 2008 eGuardian PIA and other documents. Compl. ¶¶ 54, 56-58, 69. That Standard, which Defendants do not address, is final for the reasons discussed above.

particular, 28 C.F.R. Part 23 protects privacy rights and prohibits the collection and maintenance of criminal intelligence absent reasonable suspicion. *See supra* Part II-A-4 & *infra* Part IV-B-3. Defendants' Standards violate the right of individuals not to have their personal information collected and maintained absent reasonable suspicion. And by granting intelligence systems purported authority to collect and disseminate information without reasonable suspicion, these Standards eviscerate the obligations of federally funded intelligence systems.

The Complaint also shows that Defendants' Standards have the "practical effect[]" of being binding. *Columbia Riverkeeper v. U.S. Coast Guard*, 761 F.3d 1084, 1094-95 (9th Cir. 2014) (looking to "practical effects of an agency's decision…, regardless of how it is labeled").

First, Functional Standard 1.5 and DOJ's SAR Standard set forth "a definitive statement of the agenc[ies'] position" on the type of suspicious activity that should be reported and disseminated. *Oregon Natural Desert Ass'n*, 465 F.3d at 982; *see* Compl. ¶¶ 48, 61.

Second, Defendants clearly "expect[]" "compliance" with their Standards. *Oregon Natural Desert Ass'n*, 465 F.3d at 982. The purpose of Defendants' Standards, as Defendants admit, is to standardize SAR reporting at the federal, state, and local levels. *See* Compl. ¶¶ 48, 61 & *supra* at Part II-A-5; *accord* Gov. Br. at 6 ("unified process"). To effectuate this goal, Defendants' Standards apply to all agencies that participate in the NSI. *See id.*, Exh. D at 53 ("applies to *all* departments or agencies that possess or use terrorism or homeland security information ….") (emphasis added). Defendants' suggestion that NSI participants are free to disregard their Standards would defeat Defendants' purpose in issuing their Standards.

Functional Standard 1.5 does not allow NSI participants discretion in determining whether to implement the Functional Standard: "This *ISE-SAR Functional Standard* will be used as the ISE-SAR information exchange standard for all ISE participants." *Id.*, Exh. D at 63 (underline added). Similarly, a DOJ document states that "a standard definition of what constitutes a suspicious activity *will be used* by all participating agencies." *Id.*, Exh. E at 97 (emphasis added). The document further notes that the "definition will be augmented by describing the kinds of information that cannot be entered into [eGuardian]." *Id.*

Defendants further evince an expectation of compliance by training NSI participants to

follow their Standards. *Id.* ¶¶ 24, 26, 49, 59, 64, 67. And Defendant DOJ polices compliance through a User Agreement that it requires of all entities accessing its eGuardian database, in order to "ensure consistency of process and of handling protocols." *Id.*, Exh. E at 93. The User Agreement requires that participating agencies "agree to the policies that govern the eGuardian system" and states that DOJ's component the FBI "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." *Id.* at 114. Whether or not Defendants have previously compelled compliance with their Standards, *cf.* Gov. Br. at 25, Defendants assert the right to do so.[15]

Third, Defendants' Standards have a "'direct and immediate effect on the day-to-day operations" both of participating law enforcement entities – because participants follow these Standards in reporting suspicious activities – and of Defendant DOJ, which uses its SAR Standard to determine which SARs to disseminate nationally through eGuardian. *See Oregon Natural Desert Ass'n*, 465 F.3d at 987; Compl. ¶¶ 26, 47, 60. Defendants emphasize that NSI participants are encouraged to use their professional judgment. Gov. Br. at 24. This is not an invitation to front line personnel to develop their own standards, but instead to exercise judgment in determining whether a report meets Defendants' Standards. This exercise of professional judgment does not authorize NSI participants to submit, or Defendants to include in eGuardian, a SAR that does not comply with Defendants' Standards.

3. Functional Standard 1.5 and DOJ's SAR Standard Are Arbitrary and Capricious

Under the APA, reviewing courts shall "hold unlawful and set aside" any agency action that is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." 5 U.S.C. § 706(2)(A). As discussed *supra* Part II-A-4, 28 C.F.R. Part 23 prohibits entities receiving OJP funding from collecting and maintaining criminal intelligence absent reasonable suspicion of

[15] In *Ctr. for Auto Safety v. Nat'l Highway Traffic Admin.*, 452 F.3d 798 (D.C. Cir. 2006), cited by Defendants, the agency guidelines contained permissive ("may be permissible," "may act favorably") language, *id.* at 809, unlike the mandatory "will be used" language here. Compl., Exh. D at 63 & Exh. E at 97.

criminal activity. *See* 28 C.F.R. §§ 23.3(a), 23.20(a). DOJ and PM-ISE have promulgated Standards for collecting and sharing criminal intelligence even if not supported by reasonable suspicion. These Standards conflict with 28 C.F.R. Part 23 and are therefore not in accordance with law. Defendants' only rejoinder is that the regulation does not apply to SARs. But this argument rests on disputed factual assertions that cannot be resolved on this motion to dismiss and a tautological interpretation of the regulation that is arbitrary and capricious.

(a) 28 C.F.R. Part 23 Applies to SARs and the NSI

The regulation applies to SARs because (1) the stated purpose of the NSI is to collect and share information related, at least in Defendants' view, to the crime of terrorism, (2) SARs are evaluated for their relevance to terrorism, and (3) entities that participate in the NSI receive funding from OJP. Defendants' argument as to the regulation's inapplicability rests on numerous disputed factual assertions.

First, Defendants contend that the regulation only applies to systems that have the purpose of sharing information about suspected criminals, and that the purpose of the NSI, by contrast, is merely to allow the identification of "patterns and trends across jurisdictional lines," "not to create dossiers about individuals." Gov. Br. at 28-29. This factual characterization of the NSI's intended purpose and actual operation conflicts with the Complaint.

Terrorism is a plainly a crime, *see, e.g.*, 18 U.S.C. § 2332b (defining terrorism and listing crimes that can meet the definition), and the stated purpose of the NSI is to collect and share information that has "a potential terrorism nexus" by "providing specific indications about possible terrorism-related crimes." Compl., Exh. D at 58; *see supra* Part II-A-5. Many – though not all – of the categories of conduct designated as suspicious in Functional Standard 1.5 focus on crimes, such as sabotage, vandalism, and cyber attacks. *See* Compl., Exh. D at 81. The improper inclusion in Functional Standard 1.5 and DOJ's SAR Standard of activity that does not support a reasonable suspicion of criminal wrongdoing does not change the stated purpose of the program – to collect and share information about suspected criminal, in particular, terrorist threats. *Id.* ¶ 75. Moreover, the actual operation of the NSI does result in the creation of "dossiers about individuals." *Cf.* Gov. Br. at 28; *see supra* Part II-A-3; Compl. ¶ 82 (FBI created a file about Gill

as a result of his SAR). Defendants' argument – that the actual purpose of the NSI takes it outside the regulation's scope – rests on "fact issue[s] that cannot be resolved on a motion to dismiss." *ASARCO, LLC. v. Union Pac. R.R. Co.*, 765 F.3d 999, 1009 (9th Cir. 2014).

Second, SARs constitute "criminal intelligence information." The regulation defines the term as "data which has been *evaluated* to *determine* that it…is *relevant to…criminal activity*…and…meets criminal intelligence submission criteria." 28 C.F.R. § 23.3(b)(3) (emphasis added). Defendants define a SAR as a report of behavior "that has been *determined* … to have a potential *terrorism nexus* (i.e., to be reasonably indicative of criminal activity associated with terrorism)." Compl., Exh. D at 54 (emphasis added). Under Defendants' system, SARs are evaluated at several levels, including by the local reporting agency and fusion center, to ensure that they meet Defendants' Standards. *See* Compl. ¶ 26-27, 75 & Exh. D at 60-61, 84-85; *supra* Part II-A-1. Defendants' own documents demonstrate that SARs meet the definition of criminal intelligence because they are data that have been *evaluated* to have – in Defendants' view – *relevance* to the crime of terrorism.

Defendants attempt to distinguish SARs from "criminal intelligence" by characterizing them as "uncorroborated tips and leads." Gov. Br. at 1, 28-29. This argument rests on a factual characterization of SARs that is at odds with the Complaint and Defendants' own documents attached thereto. While a "tip or lead" might initially inspire a SAR, Defendants' Standards provide evaluation criteria to identify those tips and leads with (in Defendants' view) a sufficient connection to the crime of terrorism to warrant national dissemination. *See, e.g.*, Compl., Exh. D at 61. This evaluation pursuant to Defendants' Standards distinguishes SARs from "tips and leads" and renders them "criminal intelligence."

Third, the regulation is "applicable to all criminal intelligence systems operating through support under … 42 U.S.C. [§] 3711, *et seq*., as amended." 28 C.F.R. § 23.3(a). Title 42 U.S.C. § 3711 establishes the "Office of Justice Programs within the Department of Justice." The regulation therefore applies to all criminal intelligence systems operating through support from OJP. Defendants contend that eGuardian is the *only* database used to share SARs and that it does not receive OJP funding. *See* Gov. Br. 9 n.3 & 29. This argument, too, rests on a fact issue

inappropriate for resolution on a motion to dismiss and, moreover, inappropriately seeks judicial notice of a disputed fact. *See ASARCO*, 765 F.3d at 1009; *Lee*, 250 F.3d at 690 (9th Cir. 2001); *supra* note 2 (objecting to Defendants' request for judicial notice). Given the multiple steps in the SAR information flow, DOJ's eGuardian system is not the only information system used in connection with SARs. Plaintiffs allege that "state, local, and tribal law enforcement agencies and fusion centers" also operate systems used to collect, maintain, and disseminate SARs and that they operate through support from OJP. *See* Compl. ¶¶ 23, 25, 73-75.

(b) Functional Standard 1.5 and DOJ's SAR Standard Are Arbitrary and Capricious Because They Conflict with 28 C.F.R. § 23.20(a)

Defendants have issued Standards for suspicious activity reporting that directly conflict with the core privacy protection of 28 C.F.R. Part 23. Defendants' argument as to the inapplicability of the regulation rests on, not only the factual arguments discussed above, but also a circular reading of the regulation which strays from its text and undermines its central purpose.

In issuing the regulation, DOJ prohibited entities receiving OJP funding from collecting or maintaining criminal intelligence unless there is reasonable suspicion of criminal activity. *See* 28 C.F.R. §§ 23.3(a), 23.20(a). But through promulgation of Functional Standard 1.5 and DOJ's broader SAR Standard, Defendants instruct and purportedly empower these same entities to disregard the regulation's reasonable suspicion requirement and instead to collect, maintain, and disseminate SARs even if *not* supported by reasonable suspicion. *See* Compl. ¶¶ 45, 55, 73-76. In particular, under Functional Standard 1.5 and the DOJ's SAR Standard, information can be stored whenever it is "reasonably indicative" or "may be indicative" of criminal or terrorist activity. *See* Compl. ¶¶ 44, 54, Exh. D at 54 & Exh. E at 95. PM-ISE has acknowledged that Functional Standard 1.5 requires "less than the 'reasonable suspicion' standard," and DOJ's SAR Standard is even broader than Functional Standard 1.5. *See id.* ¶¶ 45, 55, 62-63. Because SARs constitute "criminal intelligence," *see supra* Part IV-B-3-(a), the actions of *both* PM-ISE and DOJ in promulgating Functional Standard 1.5 and DOJ's SAR Standard are "not in accordance with law," 5 U.S.C. §706(2)(A), in particular, 28 C.F.R. §23.20(a).

As to Defendant DOJ, promulgation of its SAR Standard additionally violates "[o]ne of the

most firmly established principles in administrative law[,] that an agency must obey its *own* rules." 7 West's Fed. Admin. Prac. § 7514 (emphasis added); *see United States* ex rel. *Accardi v. Shaughnessy*, 347 U.S. 260 (1954) (Attorney General enjoined from refusing to exercise judgment as provided by agency regulation in response to application to suspend deportation proceedings); *Service v. Dulles*, 354 U.S. 363, 372 (1957) ("regulations validly prescribed by a government administrator are binding upon him as well as the citizen").

The government relies on the phrase "reasonably suspected" in 28 C.F.R. § 23.3's definition of "criminal intelligence information" to assert that the reasonable suspicion requirement only applies to information that is *already* supported by reasonable suspicion. *See* Gov. Br. at 28. This interpretation is unsupported by the regulation's text and produces absurd results.

The statue that authorized DOJ to issue 28 C.F.R. Part 23 instructed DOJ to issue "policy standards" that govern "criminal intelligence systems" and "are written to assure that … such systems are not utilized in violation of the privacy and constitutional rights of individuals." 42 U.S.C. § 3789g(c). In accordance with this statutory mandate, the regulation enumerates various privacy-protective "[o]perating principles," the first of which states:

> A project shall collect and maintain criminal intelligence information concerning an individual only if there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity.

28 C.F.R. § 23.20(a).

The regulation in turn defines "criminal intelligence" as "*data* which has been evaluated to determine that it…is *relevant* to the identification of and the criminal activity engaged in by an *individual* who or *organization* which is *reasonably suspected* of involvement in criminal activity…." 28 C.F.R. § 23.3(b)(3) (emphasis added). Defendants interpret the regulation to mean that data is not "criminal intelligence" subject to privacy protections, when the information is unsupported by reasonable suspicion. But this reading misplaces the modifier. The phrase "reasonably suspected" modifies "individual" or "organization," and not "data," which is instead modified by "relevant." In other words, data that has been evaluated to be relevant to the identification of criminal activity is "criminal intelligence" under the regulation, *see* 28 C.F.R. §23.3(b)(3), but that does not alter the regulation's first operating principle, which prohibits the

collection of such data absent reasonable suspicion, *see* 28 C.F.R. § 23.20(a).[16]

Defendants' interpretation is a tautology that renders the regulation meaningless and its protections illusory. Setting limits on the collection, maintenance, and sharing of information by law enforcement about individuals' non-criminal and constitutionally protected activities is the central purpose of the regulation and authorizing statute. *See* 42 U.S.C. § 3789g(c). In Defendants' view, OJP-funded entities are free to ignore the regulation's privacy-protecting reasonable suspicion requirement, in precisely those instances when they violate it. This interpretation – which reads the reasonable suspicion requirement of § 23.20(a) completely out of the regulation – "is so implausible that it could not be ascribed to a simple difference of view or the product of agency expertise." *See Motor Vehicle Mfrs. Ass'n of the U.S., Inc. v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983) (setting forth test for arbitrary and capricious agency rule); *see also Hart v. McLucas*, 535 F.2d 516, 519 (9th Cir. 1976) (rejecting construction of regulations that rendered term "surplusage").[17]

Defendants' interpretation also produces absurd results. *See Chubb Custom Ins. Co. v. Space Sys./Loral, Inc.*, 710 F.3d 946, 958 (9th Cir. 2013) (courts must avoid even a literal interpretation if it "would thwart the overall statutory scheme or lead to an absurd result"). Under the government's approach, individuals who have engaged in wholly innocent activity, but have

---

[16] This reading is consistent not only with the plain language of the regulation, but also with DOJ's own interpretation at the time it last amended the regulation: "The finding of reasonable suspicion is a threshold requirement for entering intelligence information on an individual or organization into an intelligence database." Final Revision to the Office of Justice Programs, Criminal Intelligence Systems Operations Policies, 58 Fed. Reg. 48,448 (Sept. 16, 1993). There would be no need to establish this "threshold requirement for entering intelligence information… into an intelligence database" if intelligence databases were only defined to include, as DOJ now urges, information that is already supported by reasonable suspicion.

[17] Defendants assert that DOJ's interpretation should be given deference as DOJ was the promulgating agency. Gov. Br. at 29 n.9. But the "agency's convenient litigating position" is owed no deference over the interpretation it set forth in the regulatory history. *Bowen v. Georgetown Univ. Hosp.*, 488 U.S. 204, 212 (1988); *see* 43 Fed. Reg. 28,572 (June 30, 1978) (agency responded to "concern[s] that the collection and maintenance of intelligence information should only be triggered by a reasonable suspicion that an individual is involved in criminal activity" by "requir[ing] this criteria as a basis for collection and maintenance of intelligence information"). More recently, DOJ's component FBI has acknowledged the relevance of 28 C.F.R. Part 23 to SARs. *See* Compl., Exh. E at 93 (adopting 5-year retention period for certain SARs "[i]n keeping with the retention period currently in effect for state criminal intelligence systems under 28 C.F.R. Part 23").

been branded as having a "nexus to terrorism," would have their personally identifiable information maintained in various criminal intelligence systems and yet be *denied* the "administrative, technical, and physical safeguards" and other privacy protections that the regulation's "[o]perating principles" mandate. *See* 28 C.F.R. § 23.20(g). Those reasonably suspected of criminal activity, however, would *enjoy* the benefit of those protections. Such absurd outcomes are arbitrary and unsupportable. "When an administrative agency sets policy, it must provide a reasoned explanation for its action. That is not a high bar, but is an unwavering one." *Judalung v. Holder*, _ U.S. _, 132 S.Ct. 476, 490 (2011) (Board of Immigration Appeals' rule held arbitrary and capricious because it was "unmoored from the purposes and concerns of the immigration laws"). Defendants not only have failed to provide such a reasoned explanation, but they urge the Court to adopt an interpretation of the reasonable suspicion requirement that is nonsensical.

4. Defendants Failed to Adopt Their SAR Standards Through Notice and Comment

Defendants do not dispute that they promulgated their SAR Standards without notice and comment, but assert that such process was unnecessary because neither Standard constitutes a "legislative rule." Gov. Br. at 26. Both Standards meet the test for "legislative rules."

Agency rules may be interpretative or legislative. While the APA's notice and comment requirement, 5 U.S.C. § 553(b)-(c), does not apply to interpretive rules, this exception is "construed narrowly." *Reno-Sparks Indian Colony v. U.S. EPA*, 336 F.3d 899, 909 (9th Cir. 2003); *id*. at 909 n. 11 (agency's characterization of its own rule is given "no deference"). "Interpretive rules merely explain, but do not add to, the substantive law that already exists in the form of a statute or legislative rule. Legislative rules, on the other hand, create rights, impose obligations, or effect a change in existing law pursuant to authority delegated by Congress." *Hemp Indus.*, 333 F.3d at 1087 (citation omitted). Adopting the D.C. Circuit's standard in *Am. Mining Cong. v. Mine Safety & Health Admin.*, 995 F.2d 1106, 1109 (D.C. Cir. 1993), the Ninth Circuit uses the following test to determine if a rule is legislative:

> (1) when, in the absence of the rule, there would not be an adequate legislative basis for enforcement action;

(2) when the agency has explicitly invoked its general legislative authority; or
(3) when the rule effectively amends a prior legislative rule.

Hemp Indus., 333 F.3d at 1087 (citation omitted). Although meeting any one of these three criteria suffices, *id.*, both Functional Standard 1.5 and DOJ's SAR Standard satisfy all three.

First, absent Functional Standard 1.5 and DOJ's SAR Standard, there would be no statutory basis for determining whether a police department or fusion center had collected or disseminated a SAR that complied with the system's purpose and no basis for the FBI to determine which SARs to upload to eGuardian and/or other national SAR databases.

This test turns on whether the underlying statute creates a substantive standard (in which case the rule is interpretive) or instead represents a "pure delegation of authority to the agency to determine a standard" (in which case the rule is legislative). *Erringer v. Thompson*, 371 F.3d 625, 631 (9th Cir. 2004). Thus in *Erringer*, the Ninth Circuit held that federal guidelines for how to assess a Medicare claim were interpretive rules, because the statute itself defined the types of claims ineligible for reimbursement and the rules merely elaborated on that definition. *Id.* at 630-31. By contrast, in *American Mining*, the D.C. Circuit offered, as examples of statutes giving rise to legislative rules, the Securities and Exchange Act of 1934, Section 14 of which "forbids certain persons, 'to give, or to refrain from giving a proxy' 'in contravention of such rules and regulations *as the Commission may prescribe*'" and a separate statute requiring mining operators to maintain "such records … *as the Secretary … may reasonably require* from time to time." *Am. Mining*, 995 F.2d at 1109 (quoting 15 U.S.C. §78n(b) & 30 U.S.C. §813(h)) (emphasis added).

Like the *American Mining* examples of statutory delegations, the Intelligence Reform and Terrorism Prevention Act ("IRTPA") grants Defendant PM-ISE "governmentwide authority over the sharing of … homeland security …, terrorism [and] other information." 6 U.S.C. §485(f)(1). Similarly, Title 42 U.S.C. § 3789g(c) authorizes Defendant DOJ to "prescribe[]" "policy standards" governing the "collect[ion], maint[enance], and disseminat[ion of] criminal intelligence information." Neither statute sets forth a self-executing substantive standard governing the type of information that can be collected, maintained, or disseminated; the statutes instead delegate to Defendants the authority to set forth those standards, as they have done in Functional Standard 1.5 and DOJ's SAR Standard. *See also Yesler*, 37 F.3d at 449 (rule was legislative where underlying

statute did not define tenants' due process rights, instead giving agency "the authority to . . . make due process determinations").

Rather than identifying a statute that provides a substantive standard, Defendants argue that they have never enforced their SAR Standards. Gov. Br. at 26. Prior agency enforcement is not the legal test and, if required, would insulate unlawfully promulgated legislative rules from pre-enforcement challenges. Moreover, if Defendants were correct that their Standards have no binding effect *and* that 28 C.F.R. Part 23 is inapplicable to SARs, then *no* rules would restrict the collection and dissemination of this information about private citizens. That is an unsupportable result. It also undermines Defendants' purpose in issuing their Standards – promoting uniformity in reporting – and is belied by the fact that DOJ has reserved the authority to enforce its Standard. *See* Compl. ¶¶ 48, 61 & Exh. E at 114-15; *supra* Part IV-B-2.

Second, contrary to Defendants' assertion, they explicitly invoked the legislative authority granted to them by Congress when they promulgated Functional Standard 1.5 and DOJ's SAR Standard. Defendant PM-ISE's Functional Standard 1.5 begins with a litany of authority for its issuance, including the "Homeland Security Act of 2002, as amended" and "The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended." Compl., Exh. D at 53. Similarly, the document that lays out DOJ's SAR Standard identifies "specific legal authorities" that "authorize the collection of" SARS, including IRTPA and other statutes. *Id.*, Exh. E at 97.

Third, as demonstrated *supra* Part IV-B-3-(a), Defendants' Standards amended a prior legislative rule because they lowered the minimum standard for the kind of information that may be collected and maintained. Where, as here, an agency's "rule is inconsistent with the current [agency] regulation, which has the force of law[, it] cannot be amended except by another legislative rule." *Hemp Indus.*, 333 F.3d at 1090 (DEA's putative interpretive rule invalid because it conflicted with existing regulation and was issued without notice and comment).

C. Defendants' Request for Severance Is Meritless

1. Joinder Is Appropriate

Plaintiffs are appropriately joined in this action because they all challenge the same governmental policies. Parties may be permissively joined where their claims arise "out of the

same transaction, occurrence, or series of transactions or occurrences," and there is a common "question of law or fact." Fed. R. Civ. P. 20(a)(1). This rule "is to be construed liberally in order to promote trial convenience and to expedite the final determination of disputes, thereby preventing multiple lawsuits." *League to Save Lake Tahoe v. Tahoe Reg'l Planning Agency*, 558 F.2d 914, 917 (9th Cir. 1977). The government does not challenge the common question prong, but contends that Plaintiffs' claims do not arise out of the same transaction or occurrence.

Challenges to a governmental policy or system satisfy the same transaction or occurrence requirement. *See United States v. Mississippi*, 380 U.S. 128, 142-43 (1965); *see also Turner v. LaFond*, No. C 09–00683 MHP, 2009 WL 3400987, at *3 (N.D. Cal Oct. 20, 2009) ("Typically this requirement will be met where plaintiffs collectively challenge a widely-held practice or policy."). In *Mississippi*, a voting rights challenge against the State of Mississippi and six county registrars, the Supreme Court found Rule 20's transaction or occurrence requirement satisfied because the complaint alleged that the "registrars had acted and were continuing to act as part of a [racially discriminatory] state-wide system." *Id.* at 130. Here, Plaintiffs allege that their SARs were collected and disseminated pursuant to a nationwide system created by Defendants through their SAR Standards. *See* Compl. ¶¶ 1, 22-29, 94-96, 112-13, 122, 133, 147-48 & *supra* Part II-A-5. Under *Mississippi*, their injuries arise from the same transaction or occurrence: Defendants' adoption of Functional Standard 1.5 and DOJ's SAR Standard. The fact that the Plaintiffs' claims each "arise out of disparate factual circumstances" does not alter the fact that "the primary thrust of their allegations is identical." *Turner*, 2009 WL 3400987, at *4 (permitting joinder of two plaintiffs who challenged same policy of government agency).[18]

2. Venue Is Proper in this District

Because venue is appropriate as to two Plaintiffs – Conklin and Ibrahim – and the remaining Plaintiffs may be joined pursuant to Federal Rule of Civil Procedure 20, and 42 U.S.C.

[18] *Coughlin v. Rogers*, 130 F.3d 1348 (9th Cir. 1997), cited by Defendants, found severance proper because "Plaintiffs do not allege a pattern or policy of delay in dealing with all applications and/or petitions by the INS." *Id.* at 1349. In contrast, Plaintiffs here clearly allege a central governmental policy regarding SARs. *See* Compl. ¶¶ 22-29; 42-70.

§ 1391(e), venue is proper in this District.

Venue lies in the district where a plaintiff resides, or where "a substantial part of the events or omissions giving rise to the claim occurred." 28 U.S.C. § 1391(e)(1). Moreover, "[a]dditional persons may be joined as parties to any such action in accordance with the Federal Rules of Civil Procedure and with such other venue requirements as would be applicable if the United States or one of its officers, employees, or agencies were not a party." *Id.*

Venue is proper as to Ibrahim because he resides in this district, *see* Gov. Br. at 33; Compl. ¶ 118, and because he became the subject of a SAR based on his effort to purchase computers in Dublin, California, in this District. *See id.* ¶¶ 7, 119. In addition, Conklin became the subject of a SAR based on his attempt to engage in photography in Martinez, California, also in this District. *Id.* ¶¶ 9, 141-48; *see also id.* ¶ 148 (private security guards and sheriffs' deputies in this District were trained in Defendants' Standards). Defendants assert that "this event cannot be said to constitute a 'substantial part' of the events giving rise to his claims." Gov. Br. at 33. This contention is inconsistent with Defendants' repeated argument that the real focus of this suit should be the front line personnel who reported Plaintiffs. It is also legally incorrect. The term "substantial part of the events . . .does not require that a majority of the events have occurred in the district where suit is filed, nor does it require that the events in that district predominate." *Rodriguez v. Cal. Highway Patrol*, 89 F. Supp. 2d 1131, 1136 (N.D. Cal. 2000) (venue proper in Northern District even though only one of three events occurred here).

V. CONCLUSION

For the foregoing reasons, Defendants' motion to dismiss and alternative motion for severance and dismissal should be denied.

Respectfully submitted,

DATED: November 20, 2014

By: */s/ Linda Lye*

Linda Lye

AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF NORTHERN CALIFORNIA

BINGHAM MCCUTCHEN LLP
Jonathan Loeb (SBN 162758)
jon.loeb@bingham.com
Jeffrey Rosenfeld (SBN 221625)
jeffrey.rosenfeld@bingham.com
Edward Andrews (SBN 268479)
edward.andrews@bingham.com
The Water Garden
Suite 2050 North
1601 Cloverfield Boulevard
Santa Monica, CA 90404-4082
Telephone: 310-907-1000
Facsimile: 310-907-2000

BINGHAM MCCUTCHEN LLP
Stephen Scotch-Marmo (admitted *pro hac vice*)
stephen.scotch-marmo@bingham.com
Michael James Ableson (admitted *pro hac vice*)
michael.ableson@bingham.com
399 Park Avenue
New York, NY 10022-4689
Telephone: 212-705-7000
Facsimile: 212-752-5378

AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF NORTHERN CALIFORNIA
Linda Lye (SBN 215584)
llye@aclunc.org
Julia Harumi Mass (SBN 189649)
jmass@aclunc.org
39 Drumm Street
San Francisco, CA 94111
Telephone: 415-621-2493
Facsimile: 415-255-8437

ASIAN AMERICANS ADVANCING
JUSTICE - ASIAN LAW CAUCUS
Nasrina Bargzie (SBN 238917)
nasrinab@advancingjustice-alc.org
Yaman Salahi (SBN 288752)
yamans@advancingjustice-alc.org
55 Columbus Avenue
San Francisco, CA 94111
Telephone: 415-848-7711
Facsimile: 415-896-1702

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
Telephone: 212-549-2500
Facsimile: 212-549-2654

AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF SAN DIEGO AND IMPERIAL COUNTIES
David Loy (SBN 229235)
Mitra Ebadolahi (SBN 275157)
mebadolahi@aclusandiego.org
P.O. Box 87131
San Diego, CA 92138
Telephone: (619) 232-2121
Facsimile: (619) 232-0036

AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF SOUTHERN CALIFORNIA
Peter Bibring (SBN 223981)
pbibring@aclusocal.org
1313 West 8th Street
Los Angeles, CA 90017
Telephone: (213) 977-9500
Facsimile: (213) 977-5299

Attorneys for Plaintiffs