JOYCE R. BRANDA
Acting Assistant Attorney General

MELINDA L. HAAG
United States Attorney

ANTHONY J. COPPOLINO
Deputy Branch Director

PAUL G. FREEBORNE
Senior Trial Counsel
Va. Bar No. 33024

KIERAN G. GOSTIN
Trial Attorney
D.C. Bar. No. 1019779

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

Attorneys for the Defendants

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

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

Plaintiffs,

v.

DEPARTMENT OF JUSTICE, *et al.*,

Defendants.

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

NOTICE OF MOTION AND MEMORANDUM OF LAW IN SUPPORT OF DEFENDANTS' MOTION TO DISMISS

Hearing Date: January 8, 2015
Time: 1:30 p.m.
Ctrm: 3, 17th Floor
Judge: Hon. Richard G. Seeborg

TABLE OF CONTENTS

PAGE

TABLE OF AUTHORITIES

PAGE(S)

CASES

STATUTES

RULES & REGULATIONS

EXECUTIVE ORDERS & PRESIDENTIAL MEMORANDA

FEDERAL RULES OF CIVIL PROCEDURE

MISCELLANEOUS

NOTICE OF MOTION TO DISMISS

TO ALL PARTIES AND THEIR ATTORNEYS OF RECORD:

PLEASE TAKE NOTICE THAT on January 8, 2015, at 1:30 p.m., or as soon thereafter as the matter may be heard before the Honorable Richard G. Seeborg, in the District Court for the Northern District of California, in Courtroom 3—17th Floor, Defendants will and hereby do move to dismiss all of the claims presented in Plaintiffs' Complaint, Dkt. 1, pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6) or, in the alternative, to sever Plaintiffs' claims pursuant to Federal Rule of Civil Procedure 21 and to dismiss the claims of Plaintiffs Wiley Gill, James Prigoff, Tariq Razak, and Aaron Conklin pursuant to Federal Rule of Civil Procedure 12(b)(3). Pursuant to the Parties' Stipulation, Dkt. 17, the parties have agreed upon the following briefing schedule: Plaintiffs' Opposition shall be due on November 20, 2014, and Defendants' Reply in support of the above motion shall be due on December 11, 2014.

INTRODUCTION

State and local law enforcement have long been engaged in the practice of gathering information and documenting reports regarding behaviors and incidents associated with crime, including terrorism. Many of these reports do not contain information independently establishing that criminal activity has occurred or will occur in the future. Instead, the information comes in the form of uncorroborated tips and leads that require further investigation by law enforcement personnel. Reports containing these sorts of tips and leads are generally referred to as Suspicious Activity Reports ("SARs").

The Nationwide Suspicious Activity Reporting Initiative ("NSI") is a collaborative initiative between all levels of government to ensure that SARs are effectively and securely shared among federal, state, local, tribal, and territorial law enforcement. Though the practice of gathering and sharing these tips and leads has been a core mission of law enforcement for many years, the President proposed the NSI in 2007 as part of a broader effort to standardize information-sharing practices following the September 11, 2001 attacks in order to better detect and prevent terrorism-related criminal activity.

Plaintiffs' challenge to this initiative focuses on the alleged guidance and training that Defendants provide to participating entities regarding the sharing of SARs in connection with the NSI. They assert two types of claims under the Administrative Procedure Act ("APA"), specifically that: (1) Defendants were required to go through formal notice-and-comment rulemaking procedures before issuing the challenged guidance (Third and Fourth Claims), Compl. ¶¶ 165–68, and (2) the guidance provided by Defendants is arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law (First and Second Claims), *id.* ¶¶ 153–64. Plaintiffs lack standing to raise these claims, fail to plead an action that could proceed under the terms of the APA, and, in any event, fail to present claims that are legally cognizable.

As an initial matter, Plaintiffs lack Article III standing to proceed. *See infra* Argument Part I. Plaintiffs allege that they have been scrutinized by state and local law

enforcement and private security companies as a result of guidance and training provided by Defendants in connection with the NSI. But they have not adequately alleged a sufficient nexus between those alleged injuries and the guidance and training provided by Defendant to satisfy Article III's causation or redressability requirements. Plaintiffs also allege that SARs relating to them have been purportedly uploaded to a federally maintained database and that these SARs are accessible to NSI participants. But assuming that allegation is true, Plaintiffs' alleged injuries as a result of the availability of these SARs (*e.g.*, law enforcement questioning) do not constitute legally cognizable injuries-in-fact, another necessary element of Article III standing. Moreover, because Plaintiffs seek prospective relief against the Federal Defendants, they must allege facts sufficient to establish clearly impending or imminent future harm. Their allegations of future law enforcement scrutiny are too speculative and conjectural to satisfy that requirement.

Assuming, *arguendo,* that they can establish their standing to sue, Plaintiffs have no viable legal claim under the APA, for several distinct reasons. As a threshold matter, Plaintiffs fail to establish subject-matter jurisdiction under the APA. *See infra* Argument Part II. The APA can only supply a basis for federal subject-matter jurisdiction where there are no adequate alternative remedies. Here, Plaintiffs assert that they have been injured as a result of actions undertaken by state and local law enforcement agencies and private security companies, and an action against those entities is not only an adequate alternative remedy, it is the more appropriate remedy if any exists.

Even if Defendants were the appropriate target of Plaintiffs' APA claims, the guidance provided by Defendants in connection with the NSI does not create the sort of binding, legal obligations that are remediable under the APA. The APA was enacted, in part, to regulate the way in which federal agencies wield the legislative authority delegated to them by Congress. This is reflected in at least two aspects of that statute. First, the APA only grants courts subject-matter jurisdiction over final agency actions that determine legal rights and obligations. Second, the APA only requires notice-and-

comment rulemaking procedures to be used when an agency issues a legislative rule that has the same effect as statutory law. Because the NSI guidance provided by Defendants to local entities does not impose any legal obligation on any regulated party, Plaintiffs can neither establish jurisdiction, *see infra* Argument Part III, nor succeed on the merits of their notice-and-comment claims, *see infra* Argument Part IV.A.

Plaintiffs' contention that the NSI guidance is arbitrary-and-capricious under the APA is equally untenable. *See infra* Argument Part IV.B. Plaintiffs assert that Defendants' guidance is contrary to law because Defendants should only permit NSI participants to share SARs with each other that establish reasonable suspicion of criminal conduct. Plaintiffs do not identify any constitutional or statutory prohibition on law enforcement agencies sharing such information in the absence of reasonable suspicion. Instead, Plaintiffs rely on 28 C.F.R. Part 23, a regulation imposing certain operating principles on criminal intelligence systems operating through federal support under the Omnibus Crime Control and Safe Streets Act of 1968 ("Omnibus Act"). *See* 42 U.S.C. §3789g(c); 28 C.F.R. § 23.3(b). But the database used to share SARs in connection with the NSI is not a criminal intelligence system as that term is defined in the regulation, nor a database that even receives Omnibus Act funding. Under the terms of that regulation, a "criminal intelligence system" is a system that is used for the purpose of receiving, storing, disseminating, and analyzing intelligence about individuals or associations that are already reasonably suspected of criminal activity. *See* 28 C.F.R. § 23.3(b). The NSI is not used for that purpose. Rather, it is a collaborative initiative between different jurisdictions to share tips and leads about suspicious incidents and behaviors so that law enforcement agencies can connect the dots between those incidents, efficiently and effectively assess the potential threat, and determine whether to devote resources to particular counterterrorism efforts. There is no legal basis for prohibiting the sharing of those tips and leads in the absence of reasonable suspicion, and the imposition of such a requirement would significantly undermine the effectiveness of this initiative.

Finally, if the Court does not dismiss all of Plaintiffs' claims, Defendants alternatively seek severance of the claims brought by different Plaintiffs in this lawsuit and dismissal of those claims where venue would no longer be proper. *See infra* Argument Part V. Plaintiffs' claims were improperly joined because they do not arise from the same transaction or occurrence, a threshold requirement for permissive joinder under Federal Rule of Civil Procedure 20(a). The individual incidents alleged in the Complaint as the basis for Plaintiffs' assertion that venue is proper all arose at different times, from different circumstances, and through the separate actions of different parties. Their claims should therefore be severed from one another, and once severed, the claims of four (Wiley Gill, James Prigoff, Tariq Razak, and Aaron Conklin) of the five Plaintiffs should be dismissed under Federal Rule of Civil Procedure 12(b)(3) for improper venue because these four Plaintiffs do not reside in this district and "a substantial part of the events or omissions giving rise to" their claims did not occur in this district. *See* 28 U.S.C. §1391(e)(1).

BACKGROUND

I. STATUTORY AND REGULATORY BACKGROUND

A. The Information Sharing Environment

In the aftermath of the September 11, 2001 attacks, it became apparent that federal, state, local, tribal, and territorial agencies were often failing to share the intelligence information—including tips and leads—needed to conduct counterterrorism operations effectively. *See* Program Manager, *Progress and Plans Annual Report to The Congress* at 1–2 (June 2009), *available at* http://fas.org/irp/agency/ise/2009report.pdf. To remedy this shortcoming, both the President and Congress took actions to establish an information sharing environment ("ISE") that would allow for the free flow of pertinent information among federal, state, local, tribal, and territorial governments, and where appropriate, with the private sector and foreign partners. *Id.* The ISE is not a single database, or set of databases, used to share information among government and private entities. *Id.* It is a decentralized "system of policies, business practices, architectures,

standards, and systems that enable routine, controlled information sharing among all ISE participants." *Id.*; *see also* 6 U.S.C. § 485(b)(2) (describing the ISE as a "decentralized, distributed, and coordinated environment").

The President created the ISE in August 2004 through Executive Order 13556. *See* Exec. Order No. 13356, 69 F.R. 53599 (Aug. 27, 2004). Shortly thereafter, in December 2004, Congress passed Section 1016 of the Intelligence Reform and Terrorism Prevention Act ("IRTPA"), 6 U.S.C. § 485, to provide congressional support for the development of the ISE. *See id.* § 485(a), (b). Section 1016 directs the President to (1) "create an [ISE] for the sharing of terrorism [and homeland security] information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties"; (2) "designate the organizational and management structures that will be used to operate and manage the ISE"; and (3) "determine and enforce the policies, directives, and rules that will govern the content and usage of the ISE." 6 U.S.C. §§ 485(a)(3), (b)(1).

IRTPA also created the office of the "Program Manager" to assist the President in performing these duties. 6 U.S.C. § 485(f). The Program Manager, among other things, is responsible for: (1) planning, overseeing, and managing the ISE; (2) "assist[ing] in the development of policies, as appropriate, to foster the development and proper operation of the ISE"; and (3) issuing "governmentwide procedures, guidelines, instructions, and functional standards" that are consistent with the direction of the President, the Director of National Intelligence, and the Director of the Office of Management and Budget. *Id.* § 485(f)(2)(A)(i)–(iii). The Program Manager serves at the discretion of the President. *Id.* § 485(f)(1).

B. The Nationwide Suspicious Activity Reporting Initiative

In connection with this effort to develop an ISE, the President released his National Strategy for Information Sharing in 2007. *National Strategy for Information Sharing* (Oct. 2007), *available at* http://nsi.ncirc.gov/documents/National_Strategy_for_Information_Sharing.pdf. Among

other things, that strategy calls for the creation of "a unified process to support the reporting, tracking, processing, storage and retrieval" of "locally generated" reports about "suspicious incidents, events, and activities." *Id.* at A1-6. In response, a collaboration of federal, state, local, tribal, and territorial agencies developed the NSI. *See* Compl. ¶ 22.

The NSI builds on the already existing practice of local and state agencies gathering and documenting reports of suspicious activity as part of their general law enforcement responsibilities. *See* Compl., Ex. D at 58–59; SAR Support and Implementation Project, *Findings and Recommendations* at 1, 6 (Oct. 2008), *available at* http://it.ojp.gov/documents/SAR_Report_October_2008.pdf. Many of these activities are initially observed by private citizens, representatives of private sector partners, or government officials. *See* Compl., Ex. D at 60–61. These observations, however, are often relayed to local law enforcement and documented by those agencies as SARs. *See id.*

These SARs are then frequently made available to collection points called fusion centers that are owned and operated by local or state governments (with funding support from the federal government). *See* Compl. ¶ 23.[1] When a SAR is provided to a fusion center, it is reviewed by an analyst or law enforcement officer. *See* Compl. ¶¶ 25–26. If the officer or analyst determines that the SAR has a sufficient nexus to terrorism, the fusion center may then choose to make that information available to federal, state, local, tribal, and territorial participants in the NSI. *See id.* ¶ 26.

C. Functional Standard for Suspicious Activity Reporting Version 1.5

Law enforcement has long engaged in the practice of gathering tips and leads about suspicious incidents. In the absence of national guidance, however, individual jurisdictions established their own policies and procedures for sharing this information with other agencies. The federal government, through the NSI, has developed guidance

[1] Fusion centers are not exclusively used to collect and analyze SARs. Compl. ¶ 25. They are information repositories used to store a wide variety of "security information." *Id.* ¶¶ 23, 25. There are currently seventy-eight fusion centers nationwide. *Id.* ¶ 23.

designed to promote the standardization of that process in order to enhance the effectiveness of information sharing while protecting privacy and civil liberties.

In connection with this effort, the Program Manager released a functional standard—the Functional Standard for Suspicious Activity Reporting Version 1.5 ("Functional Standard")—for the NSI in May 2009. *See* Compl. ¶ 16. The purpose of the Functional Standard is to "support the sharing . . . of information about suspicious activity, incidents or behavior . . . that have a potential terrorism nexus" by providing a "standardized means for sharing information." Compl., Ex. D at 59. In service of this goal, the Functional Standard, among other things, provides guidance to analysts and law enforcement officers at fusion centers (and participating federal agencies) regarding when to make a SAR available to other NSI participants. *See id.* at 61–62.

Plaintiffs focus on two aspects of this guidance in their Complaint: (1) the Functional Standard's definition of the term "suspicious activity" as "[o]bserved behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity," Compl. ¶ 44; Compl., Ex. D at 54, 58; and (2) the Functional Standard's "Criteria Guidance"—*i.e.*, its description of sixteen categories of behavior that may have a potential nexus to terrorism.[2] Compl. ¶ 46; Compl., Ex. D at 58, 61, 81–82.

Importantly, the Functional Standard does not mandate that any NSI participant share SARs that are reasonably indicative of pre-operational planning related to terrorism. Instead, the Functional Standard is descriptive in nature. It describes the

[2] The Functional Standard explicitly recognizes that some of these categories of behaviors may implicate First Amendment rights. To accommodate for this concern, it provides that this information "should not be reported in a SAR or ISE-SAR absent articulable facts and circumstances that support the source agency's suspicion that the behavior observed is not innocent, but rather reasonably indicative of criminal activity associated with terrorism, including evidence of pre-operational planning related to terrorism." Compl., Ex. D at 81 n.11. The Functional Standard further provides that "race, ethnicity, national origin, or religion affiliation should not be considered as factors that create suspicion." *Id.*

process that analysts and law enforcement officers undertake in deciding whether to share a report with other NSI participants and the factors they may consider:

> The determination of a [SAR that is reasonably indicative of pre-operational planning related to terrorism] is a two-part process. First, at the State or major urban area fusion center or Federal agency, an analyst or law enforcement officer reviews the newly reported information against ISE-SAR behavior criteria. Second, based on available knowledge and information, the analyst or law enforcement officer determines whether the information meeting the criteria has a potential nexus to terrorism.

Compl., Ex. D at 85; *see also* Compl., Ex. D at 61–62. A SAR that is determined to have the requisite nexus to terrorism is referred to as an ISE-SAR. *See id.* at 54. If there is a sufficient nexus to terrorism, the Functional Standard indicates that the analyst or officer should consider making that ISE-SAR accessible to other NSI participants. *See id.* at 61–62, 85. But the Functional Standard does not require fusion centers to share ISE-SARs or create any enforcement mechanism to ensure that fusion centers only share ISE-SARs. Indeed, the Functional Standard stresses that "the officer or analyst will apply his or her professional judgment to determine whether the information has a potential nexus to terrorism." *Id.* at 61.

When a fusion center decides to make an ISE-SAR available to other NSI participants, it does so by creating and sharing an incident report in a national database. *See* Compl. ¶ 26. There were initially two systems—called ISE Shared Spaces and eGuardian—that allowed sharing of ISE-SARs among NSI participants. *See id.* ¶¶ 11, 26; Compl., Ex. E at 91–92; U.S. Gov't Accountability Office, GAO-13-233, *Information Sharing: Additional Actions Could Help Ensure that Efforts to Share Terrorism-Related Suspicious Activity Reports are Effective* at 8 (2013), *available at* http://www.gao.gov/assets/660/652995.pdf. However, in January 2014, the program was migrated to a single database, the SAR Data Repository maintained

by the Federal Bureau of Investigation ("FBI") in its eGuardian Threat Tracking System ("eGuardian").[3]

D. The eGuardian Privacy Impact Assessment

Plaintiffs make several allegations relating to the FBI's Privacy Impact Assessment for the eGuardian Threat Tracking System ("Privacy Impact Assessment"). *See* Compl. ¶¶ 53–55, 65–70, 153–58, 165–66; Compl, Ex. E. The Privacy Impact Assessment was published by the FBI to satisfy its obligations under Section 208 of the E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899 (2002) (Dec. 17, 2002). Section 208(b)(1)(A)of that Act requires federal agencies to create a privacy impact assessment when developing or procuring certain information technology systems defined in the Act or initiating a new collection of information. *Id.* The assessment must address what information is to be collected under the system, why the information is being collected, the intended use of the information, with whom the information will be shared, how individuals can consent to the use of their information, how the information will be secured, and whether a system of records is being created under the Privacy Act. *Id.* § 208(B)(2)(b)(ii).

[3] Defendants request that the Court take judicial notice pursuant to Federal Rule of Evidence 201(b)(2) of the fact that, as of January 2014, eGuardian's SAR Data Repository is the system used by NSI Participants to share ISE-SARs in connection with the NSI. This fact is reflected in the January 14, 2014 update to the privacy impact assessment for the FBI's eGuardian system, which is available on the FBI's official website. FBI, Privacy Impact Assessment Update for the eGuardian System (Jan. 14, 2014) ("[T]his Privacy Impact Assessment (PIA) update reflects the technical transition of the Nationwide SAR Initiative (NSI) that occurs in early 2014. The technical transition will result in eGuardian becoming the [SAR Data Repository] that all [federal, state, local, tribal and territorial law enforcement partners] use to report SARs."), *available at* http://www.fbi.gov/foia/privacy-impact-assessments/eguardian-threat. Courts regularly take judicial notice of facts reflected on official government websites. *Gustavson v. Wrigley Sales Co.*, 961 F. Supp. 2d 1100, 1113 n.1 (N.D. Cal. 2013) ("The Court may take judicial notice of materials available on government agency websites."); *Jarvis v. JP Morgan Chase Bank, N.A.*, No. CV 10-4184-GHK, 2010 WL 2927276, at *1 (C.D. Cal. July 23, 2010 (collecting cases where courts have taken judicial notice of information on government websites); *Paralyzed Veterans of Am. v. McPherson*, No. C06- 4670SBA, 2008 WL 4183981, at *5 (N.D. Cal. Sept. 9, 2008) (same).

In accordance with these statutory requirements, the Privacy Impact Assessment describes the content of information that will be stored in the eGuardian system. According to that description,

> eGuardian will collect terrorism threat information and/or suspicious activity information having a potential nexus to terrorism. "Suspicious activity" is defined as observed behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal or other illicit intension.

Compl., Ex. E at 95; *see also* Compl. ¶ 54. The Privacy Impact Assessment further explains that this definition of suspicious activity "is consistent with the definition utilized by the [Program Manager in the Functional Standard]." Compl., Ex. E at 95.

Plaintiffs allege that the FBI, by releasing the Privacy Impact Assessment, established a broader definition of "suspicious activity" than that used by the Program Manager in the Functional Standard. *See*, *e.g.*, Compl. ¶ 55. In fact, when the Privacy Impact Assessment was signed by the FBI, the Program Manager had not yet released the current version of the Functional Standard.[4] Instead, a prior iteration of the functional standard (Version 1.0) was in place that used the same definition of "suspicious activity" as that in Privacy Impact Assessment. *See* Information Sharing Environment, Functional Standard for Suspicious Activity Reporting Version 1.0 (Jan. 25, 2008), *available at* http://ise.gov/sites/default/files/ISE-FS-200%20(SAR%20Functional%20Standard_Issuance_Version_1.0_Final_Signed).pdf. The FBI has since released an updated privacy impact assessment, which uses the same definition of "suspicious activity" as that in the current Functional Standard. FBI, Privacy Impact Assessment for the eGuardian System (Jan. 4, 2013), *available at* http://www.fbi.gov/foia/privacy-impact-assessments/eguardian-threat.

[4] The Privacy Impact Assessment was signed on November 25, 2008, Compl., Ex. E at 90, whereas the Functional Standard was not signed until May 21, 2009, Compl., Ex. D at 56

E. 28 C.F.R. Part 23

Plaintiffs rely on 28 C.F.R. Part 23 as a substantive legal basis for their APA claims. That regulation was promulgated pursuant to the Omnibus Act, a separate and distinct statute from that which established the ISE. Among other things, the Omnibus Act created the Law Enforcement Assistance Administration ("LEAA") to oversee federal grants for the implementation of crime fighting technologies and strategies by state and local governments. *See* Compl. ¶ 32. The LEAA has since been reconstituted as the Office of Justice Programs ("OJP"), a bureau of the Department of Justice ("DOJ"). *See* 28 C.F.R. § 0.1; Compl. ¶ 33. Pursuant to the Omnibus Act, OJP is generally authorized "to establish such rules, regulations, and procedures as are necessary to the exercise of [its] functions," 42 U.S.C. § 3782(a), and is specifically authorized to issue standards governing the operation of "criminal intelligence systems [that] collect, maintain, and disseminate criminal intelligence information" where the systems are operated through funding support under the Omnibus Act, *id.* § 3789g(c).

OJP issued the current version of 28 C.F.R. Part 23 in 1993. Compl. ¶¶ 32, 36, 37. That regulation makes clear that 28 C.F.R. Part 23 only imposes its requirements on "criminal intelligence systems" that are funded under the Omnibus Act. *See* 42 U.S.C. § 3789g(c) (authorizing OJP to issue policy standards for "criminal intelligence systems operating through support under [the Omnibus Act]"); 28 C.F.R. § 23.1 ("The purpose of this regulation is to assure that all criminal intelligence systems operating through support under the [Omnibus Act], are utilized in conformance with the privacy and constitutional rights of individuals."); 28 C.F.R. § 23.3 ("These policy standards are applicable to all criminal intelligence systems operating through support under the [Omnibus Act]."); 28 C.F.R. § 23.30 (requiring grantees to adhere to certain funding guidelines); 28 C.F.R. § 23.40 (providing for monitoring and auditing for intelligence systems grants). It defines the term "criminal intelligence system" as "the arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information." 28 C.F.R. § 23.3(b)

(1). And defines the term "criminal intelligence information" as "data which has been evaluated to determine that it: (1) 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, and (2) meets criminal intelligence system submission criteria." 28 C.F.R. § 23.3(b)(3).

If 28 C.F.R. Part 23 is applicable to a criminal intelligence system, the operator of that system is required to abide by certain operating principles. 28 C.F.R. § 23.20. These principles include a variety of civil-liberty and data-security protections, including requirements that the project: "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," *id.* § 23.20(a), refrain from maintaining information collected in violation of any applicable federal, state, or local law, *id.* § 23.20(d); disseminate information only "where there is a need to know and a right to know the information in the performance of a law enforcement activity," *id.* § 23.20(e); establish safeguards to prevent unauthorized access to information maintained in the system, *id.* § 23.20(g); and adopt a satisfactory data retention policy, *id.* § 23.20(h).

Plaintiffs' claims rely on an alleged violation of only one of these operating principles. Specifically, Plaintiffs allege that the NSI is unlawful because the Functional Standard and the Privacy Impact Assessment permit NSI participants to share SARs that are reasonably indicative of pre-operational planning related to terrorism rather than requiring that SARs only be shared where there is reasonable suspicion of criminal conduct. Plaintiffs' claims are not based on any allegation that this information, once shared, is subject to less robust security or other privacy protections than those included in 28 C.F.R. Part 23. Indeed, all of the ISE—including the NSI—is subject to substantial

privacy guidelines issued by the Program Manager and approved by the President pursuant to his statutory duties under IRTPA.[5]

II. PLAINTIFFS' INDIVIDUAL ALLEGATIONS

The five Plaintiffs in this case make distinct allegations about the alleged effects of the NSI. Wiley Gill, a resident of Chico, California, Compl. ¶ 80, alleges that he is the subject of a SAR "created on or about May 23, 2012 [that] purports to document an encounter between [him] and the Chico Police Department (CPD) on or about May 20, 2012" that stemmed from an investigation of a domestic violence incident at Gill's residence involving another individual. *Id*. ¶ 83. The SAR completed by CPD, and allegedly uploaded to eGuardian, purportedly contains information concerning what CPD officers observed on Gill's computer screen when they entered his residence, and statements regarding Gill's conversion to Islam, "pious demeanor," and potential access to flight simulators via the internet" as "worthy of note." *Id*. ¶¶ 82–83. Gill alleges that the search of his home by the CPD based upon an allegation of domestic violence was done as a pretext to investigate him because of his religion. *Id*. ¶ 85.

Gill also contends "[i]n approximately September 2010, after [he] had converted to Islam, two CPD officers visited him at his apartment and requested to speak to him about supposedly 'anti-American statements' that he had made. One of the officers referred to having a file on [him], refused to explain what 'anti-American statements'

[5] IRTPA instructs the President to issue guidelines that "protect privacy and civil liberties in the development and use of the ISE." 6 U.S.C. § 485(d)(2)(A). By Executive Order and Memorandum, the President ordered that such guidelines be developed and submitted to him for approval. Memorandum for the Heads of Executive Departments and Agencies, 2005 WL 3446759, at *5 (Dec. 16, 2005); *see also* Exec. Order No. 13388, 70 F.R. 62023 (Oct. 25, 2005). The Program Manager subsequently issued privacy guidelines in accordance with those directives. *See* Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment (Nov. 2006), *available at* https://www.ise.gov/sites/default/files/PrivacyGuidelines20061204.pdf. The privacy guidelines are distinct from the Functional Standard, which is used to assist NSI participants in identifying SARs for dissemination to other participants.

[he] had purportedly made or the source of the information[.]" *Id.* ¶ 91. Gill further alleges that because he is the subject of a SAR, he has "been automatically subjected to law enforcement scrutiny" by the CPD, based upon a July 2012 call from the CPD to him in which CPD purportedly inquired about Gill's Facebook page, which included a picture of Shahada, the Muslim statement of faith, and video games he played. *Id.* ¶¶ 92, 97.

Gill alleges that this alleged "religious harassment" is attributable to the guidance and training Defendants provide to local law enforcement in connection with the NSI. *Id.* ¶¶ 90, 94, and 95. Gill "fears further investigative harassment at the hands of the CPD and other agencies caused by the existence of the SAR." *Id.* ¶ 98. Gill also contends that "[t]he SAR about [him] is maintained and will continue to be maintained in one or more national SAR databases, where it can be accessed by law enforcement agencies across the country." *Id.* ¶100.

James Prigoff, a resident of Sacramento, California, Compl. ¶ 101, alleges that, in 2004, two private security guards prevented him from photographing artwork painted on a natural gas storage tank in Boston, Massachusetts. *Id.* ¶ 102–03. Prigoff alleges that when he returned home in Sacramento, he found a note from a member of the Joint Terrorism Task Force, asking that he call the FBI. *Id.* ¶ 109. He also alleges that two agents asked his neighbor about him. *Id.* Based on this 2004 incident, Prigoff contends that he is the subject of a "SAR or SAR precursor," *id.* ¶ 110, filed by the private security guards, *id.* ¶ 112. Prigoff alleges that he was prevented from photographing the storage tank because of the guidance and training provided by Defendants. *Id.* ¶¶ 112, 113. Prigoff also contends that because he is allegedly the subject of a SAR, he has been "automatically subjected to law enforcement scrutiny" and "[t]hat scrutiny has included but may not be limited to a follow-up visit by an agent of the Joint Terrorism Task Force to his home, a telephone call with that agent, and inquiries by that agent of at least one of his neighbors about him." *Id.* ¶ 114. Finally, Prigoff alleges "[o]n information and belief [that the SAR was] uploaded to eGuardian and/or another national SAR or similar counterterrorism database." *Id.* ¶ 112.

Khaled Ibrahim, a resident of San Jose, California, Compl. ¶ 118, alleges that he is the subject of a SAR, allegedly created on November 14, 2011, that describes his purchase of a "large amount of computers." *Id.* ¶ 121. Ibrahim alleges that the purported SAR was "uploaded to FBI's eGuardian database." *Id.* Ibrahim alleges that he is "disturbed that trained law enforcement personnel at a fusion center uploaded the SAR about him to eGuardian, thereby flagging him as an individual with a potential nexus to terrorism." *Id.* ¶ 124. Ibrahim also contends that the SAR was entered "potentially because of his Middle Eastern descent." *Id.* ¶ 124. Ibrahim alleges that the existence of a SAR about him subjects him to "scrutiny" by law enforcement personnel that "may include but is not limited to scrutiny or interviews by any of the law enforcement agencies across the country that have access to the FBI's eGuardian system, to which his SAR was uploaded." *Id.* ¶ 123.

Tariq Razak, a resident of Placentia, California, Compl. ¶ 126, alleges that on May 16, 2011, a Santa Ana police officer at a Santa Ana Train Depot received a call from a security officer who notified the police that Razak was studying his surroundings at the facility. *Id.* ¶ 128. Razak alleges that the police officer filed a SAR based on the incident that describes him to be surveying the facility and eventually leaving with 'a female wearing a white burka head dress.'" *Id.* ¶ 128. Razak alleges that the incident resulted from the guidance and training provided by Defendants. *Id.* ¶¶ 122, 124. Razak contends he has "been automatically subjected to law enforcement scrutiny" because he "is the subject of a SAR that falls under Defendants' standards for suspicious activity reporting" and that this "scrutiny may include but is not limited to scrutiny or interviews by any of the law enforcement agencies across the country who have access to the SAR about him." *Id.* ¶ 134. Razak also alleges "on information and belief [that the SAR] has been uploaded to eGuardian and/or another national SAR database," *id.* ¶ 133, and that the "the SAR . . . is maintained and will continue to be maintained in one or more national SAR databases, where it can be accessed by law enforcement agencies across the country," i*d.* ¶ 136.

Aaron Conklin, the final Plaintiff, resides in Vallejo, California. Compl. ¶ 137. He alleges that in 2011 or 2012 he was photographing a refinery to Benicia, California at around 10:00 p.m., *id*. ¶ 138, and that a private security guard at the refinery told him "not [to] photograph the refinery and issued stern warnings," *id*. ¶ 139. Conklin further alleges that in November 2013 he attempted to photograph another refinery in Martinez, California, and was told by private security guards that he could not do so. *Id*. ¶¶ 141–43. According to Conklin, the guards called the Contra Costa County Sheriff's department, and two officers arrived on the scene and searched Conklin's camera and car. *Id*. ¶ 144. The deputies concluded by "telling [Conklin] that he would have to be placed on an 'NSA watchlist.'" *Id*. ¶ 145. Conklin alleges that he is the subject of a SAR that has been "uploaded to eGuardian and/or another national SAR database," and that he was prevented from photographing at the two refineries because of the training associated with the SAR process. *Id*. ¶ 147–88. Conklin alleges that the SAR "automatically subject[s him] to law enforcement scrutiny," *id*. ¶ 149, and that he is "deeply troubled by what may result from the collection maintenance, and dissemination in a national database of a report describing him has engaging suspicious activity with a potential nexus to terrorism," *id*. ¶ 151. Conklin also alleges that he has been "chilled" because "he is afraid to continue photographing industrial sites for fear of being stopped and questioned or, worse, arrested." *Id*. ¶ 150.

ARGUMENT

Plaintiffs seek prospective relief invalidating the guidance Defendants have provided to NSI participants regarding the information that they should consider sharing with one another in connection with the NSI, and requiring Defendants to instead impose the operating principles of 28 C.F.R. Part 23 on entities participating in the NSI. As explained below, the Court cannot grant that relief for several reasons: (1) Plaintiffs lack standing to bring their claims (Part I); (2) this Court lacks subject-matter jurisdiction under the APA to hear those claims (Parts II–III); (2) Plaintiffs' notice-and-comment and

arbitrary-and-capricious claims are legally deficient (Part IV); and (3) this Court is not the appropriate venue to resolve the claims of four of the five Plaintiffs (Part V).

I. PLAINTIFFS HAVE FAILED TO ALLEGE THE NECESSARY ELEMENTS OF STANDING

Plaintiffs have failed to establish the elements required for Article III standing. *See Wilbur v. Locke*, 423 F.3d 1101, 1107 (9th Cir. 2005) ("A Plaintiff has the burden of establishing standing." (quotation marks and citations omitted)), *abrogated on other grounds by Levin v. Commerce Energy, Inc.*, 560 U.S. 413 (2010).[6] To carry their burden of establishing standing, Plaintiffs must demonstrate: (1) an "injury-in-fact," (2) "a causal connection between the injury and the conduct complained of," and (3) a likelihood "that the injury will be redressed by a favorable decision." *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560–61 (1992) (quotation marks and citations omitted). To show causation and redressability, Plaintiffs must demonstrate that the injury complained of was not "th[e] result [of] the independent action of some third party not before the court," *id* at 560–61 (quotation marks and citation omitted), and that "it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision," *id.* Even "accepting as true all the material allegations" in the Complaint, and construing the Complaint "in a light most favorable" to Plaintiffs, as the Court must, *Schmier v. U.S. Ct. of Appeals for the Ninth Circuit*, 279 F.3d 817, 820 (9th Cir. 2002), Plaintiffs cannot satisfy these requirements.

First, Plaintiffs' assertion that the actions allegedly undertaken by state and local law enforcement agencies and private security companies were the result of guidance and training provided by Defendants is purely speculative and unfounded. When the "existence of one or more of the essential elements of standing depends on the unfettered choices made by independent actors not before the courts and whose exercise of broad

[6] Standing is a "threshold question in every federal case, determining the power of the court to entertain the suit." *Warth v. Seldin*, 422 U.S. 490, 498 (1975). Standing "pertain[s] to a federal court's subject-matter jurisdiction under Article III, . . . [and therefore is] properly raised in a motion to dismiss under Federal Rule of Civil Procedure 12(b)(1)." *White v. Lee*, 227 F.3d 1214, 1242 (9th Cir. 2000).

and legitimate discretion the courts cannot presume either to control or to predict," it "becomes the burden of the plaintiff to adduce facts showing that those choices have been or will be made in such manner as to produce causation and permit redressability of injury." *Lujan*, 504 U.S. at 562 (citations omitted). "[U]nadorned speculation will not suffice to invoke the federal judicial power." *Simon v. E. Ky. Welfare Rights Org.*, 426 U.S. 26, 44 (1976). Plaintiffs' bald assertions that the guidance contained in the Functional Standard and Privacy Impact Assessment, as well as unspecified training provided to law enforcement by Defendants, caused local police and private security guards to undertake actions against Plaintiffs, *see* Compl. ¶¶ 90, 94, 112–13, 121–22, 133, 147–48, are insufficient to meet this standard.

As the Ninth Circuit recently recognized, where, as here, a party alleges that "government action caused injury by influencing the conduct of third parties, . . . 'more particular facts are needed to show standing' . . . because the third parties may well have engaged in their [allegedly] injury-inflicting actions even in the absence of the government's challenged conduct." *Mendia v. Garcia*, --- F.3d ----, 12-16220, 2014 WL 4800087, at *3 (9th Cir. Sept. 29, 2014) (quoting *Nat'l Audubon Soc'y v. Davis*, 307 F.3d 835, 849 (9th Cir. 2002)). Facts must be presented showing that the actions challenged were a "substantial factor motivating the third parties' actions." *Id*. (quotation marks and citations omitted). The bulk of Plaintiffs' claims, however, are based upon a speculative connection between the actions undertaken by local police and private security companies and the guidance and training provided under the NSI. Because such "'speculation'" and "'guesswork'" are insufficient to carry that burden, Plaintiffs fail to establish standing. *Id*. (quoting *Clapper v. Amnesty Int'l, USA*, 133 S. Ct. 1138, 1150 (2013)).

In addition, where Plaintiffs do attempt to offer more than mere conclusory allegations in support of their assertion that the actions of local police and private security guards were the result of Defendants' guidance and training, those allegations are contradicted by the facts available even at this stage through the pleadings. Plaintiffs

assert, for example, that an agent from a Joint Terrorism Task Force, "which . . . is a partnership between the FBI and other law enforcement agencies," spoke to Prigoff in 2004 because of a "SAR or SAR precursor report" about him. Compl. ¶¶ 109–10. But the Functional Standard being challenged in this case was not promulgated until 2008 – well after the alleged SAR. Indeed, as explained above, *see supra* Background Part I.B, the concept of the NSI was not proposed by the President until 2007. Accordingly, the questioning of Prigoff alleged in the Complaint could not have been the result of the NSI, let alone the standard for collecting and reporting SARs described by Defendants in the Functional Standard and Privacy Impact Assessment and now challenged in this lawsuit.[7] Plaintiffs also allege that Razak became the subject of a SAR "because of Defendants' training on their SAR reporting standards to state and local law enforcement and the private sector." Compl. ¶ 129. But the SAR attached to the Complaint makes clear that a private security guard reported the incident based on training the guard had received from "a local police agency," and not from the federal government. *See* Compl., Ex. C at 50.

Second, to the extent Plaintiffs are asserting that the actions of federal, state, and local law enforcement are a result of these agencies having access to information about suspicious incidents through federally maintained national databases, they do not allege any "legally cognizable injury" resulting from that information being made available. *Schmier*, 279 F.3d at 821. At most, only two of the Plaintiffs (Gill and Prigoff) arguably allege having been questioned by law enforcement as a result of information being made available in a national database. *See* Compl. ¶¶ 90–92, 109–10. But neither of these Plaintiffs claims that such questioning has led to any "legally cognizable injury" that could provide a basis for standing. "The federal courts do not have the constitutional authority to adjudicate the metaphysical injuries that [Plaintiffs have] allegedly suffered."

[7] And even if Prigoff could carry his burden of establishing standing based upon such assertions, his claims are time-barred. The six year statute of limitations in 28 U.S.C. § 2401(a) applies to APA claims. *Sierra Club v. Penfold*, 857 F.2d 1307, 1315 (9th Cir. 1988). Because Prigoff's claims first accrued ten years before the filing of the Complaint (in 2004), his claims are time barred and should additionally be dismissed for that reason.

Schmier, 279 F.3d at 822. Moreover, these Plaintiffs do not allege having been questioned since July 2012. *See* Compl. ¶¶ 91–92 (Gill last questioned in July 2012); *id.* ¶ 109–110 (Prigoff last questioned in August 2004). Their allegations, as explained next, are therefore plainly insufficient to sustain standing for the prospective relief sought in this case.

Third, while Plaintiffs seek prospective relief, their allegations of *future* law enforcement scrutiny are too vague and indeterminate to establish a cognizable injury-in-fact. Plaintiffs allege that they "fear[]" further investigative action as a result of the SAR about them, Compl. ¶ 98, that "may" include being visited by the FBI, *id*. ¶ 114, and "may" include "scrutiny or interviews" by law enforcement personnel, *id*. ¶¶ 123, 134, 149. To satisfy standing requirements, however, an injury must be "'concrete, particularized, and actual or imminent." *Clapper*, 133 S. Ct. at 1147. Plaintiffs may not rely on allegations that are "conjectural or hypothetical," *Lujan*, 504 U.S. at 560–61; *see also Nelsen v. King Cnty*., 895 F.2d 1248, 1252 (9th Cir. 1990) (holding that Article III standing cannot be based upon "chain of speculative contingencies").

This is particularly so with respect to claims for prospective relief, such as Plaintiffs' request for an order directing Defendants to require the use of the "reasonable suspicion" standard in 28 C.F.R. Part 23 when collecting, maintaining, and disseminating information in connection with the NSI. The Supreme Court has "repeatedly reiterated that 'threatened injury must be *certainly impending* to constitute injury in fact,' and that '[a]llegations of *possible* future injury' are not sufficient." *Clapper*, 133 S. Ct. at 1147 (quoting *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990)) (alterations and emphasis by the Court); *see also DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 345 (2006); *see also Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2341 (2014) ("An allegation of future injury may suffice if the threatened injury is 'certainly impending,' or there is a 'substantial risk' that the harm will occur."); *City of Los Angeles v. Lyons*, 461 U.S. 95, 101–02 (1983) (when pursuing a claim for prospective injunctive relief, a plaintiff must

establish standing based on an "injury or threat of injury" that is "both real and immediate, not conjectural or hypothetical" (quotation marks and citations omitted)).

Fourth, and finally, Plaintiffs' suggestions of constitutional injury are unavailing. Plaintiffs allege that Defendants' conduct has "chilled" their pursuit of photography and other activity. *See e.g.*, Compl. ¶ 115.[8] This allegation of "chilling" is precisely the sort of vague allegations of future harm that the Supreme Court has rejected. *See Clapper*, 133 S. Ct. at 1151 (explaining that plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending"); *Laird v. Tatum*, 408 U.S. 1 (1972) (rejecting standing based on the alleged chilling effect of certain Army investigations). While acknowledging that some cases have held that constitutional violations may arise from the chilling effect of "regulations that fall short of a direct prohibition against the exercise of First Amendment rights," the Court has made clear that none of those cases involved a "chilling effect aris[ing] merely from the individual's knowledge that a governmental agency was engaged in certain activities or from the individual's concomitant fear that, armed with the fruits of those activities, the agency might in the future take some other and additional action detrimental to that individual." *Clapper*, 133 S.Ct. at 1152 (citing *Laird*, 408 U.S. at 11). This is precisely what Plaintiffs have alleged, and it is not sufficient to establish standing.

[8] Plaintiffs also allege that Defendants' guidance has resulted in other alleged violations, such as racial profiling. *See, e.g.*, *id.* ¶¶ 95, 124. Plaintiffs have not presented any constitutional counts in the Complaint or any factual basis for them. To establish redressability, Plaintiffs must show that the "injury"—the unconstitutional racial profiling and other alleged constitutional violations—occurred and "will be redressed by a favorable decision." *Friends of the Earth v. Laidlaw Envtl. Servs.*, 528 U.S. 167, 181 (2000). Plaintiffs cannot make that showing, as they have failed to even present a constitutional count, let alone the grounds for it. Plaintiffs apparently decided not to do so because their "naked assertion[s] devoid of 'further factual enhancement'" cannot withstand dismissal under Rule 12(b)(6). *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atlantic Corp. v. Twombly*, 500 U.S. 544, 557 (2007)).

II. PLAINTIFFS HAVE AN ADEQUATE ALTERNATIVE REMEDY THAT PRECLUDES APA JURISDICTION

Assuming, *arguendo*, that Plaintiffs could establish standing, the Court still would lack subject-matter jurisdiction to hear their APA claims. Under the APA, only agency action for which there is "no other adequate remedy" is subject to judicial review. 5 U.S.C. § 704. Because Plaintiffs have an adequate remedy against the non-party police and private security companies that are alleged to have engaged in the conduct that Plaintiffs allege was improper, there is no proper basis for judicial review by a federal court.

The APA premises jurisdiction on the absence of an adequate alternative remedy. *See* 5 U.S.C. §§ 702, 704. "[F]or a cause of action to provide an adequate remedy in the § 704 context, a court need only be able to provide 'relief of the same genre' to the party seeking redress, but not necessarily 'relief identical to relief under the APA.'" *Rimmer v. Holder*, 700 F.3d 246, 262 (6th Cir. 2012) (quoting *Garcia v. Vilsack*, 563 F.3d 519, 522 (D.C. Cir. 2009). An alternative remedy is adequate if it would remedy the injury about which the plaintiff complains. *See, e.g., Coker v. Sullivan*, 902 F.2d 84, 90 n.5 (D.C. Cir. 1990). The remedy need not "have [an] effect upon the challenged agency action" to be adequate. *Id.*

Plaintiffs claim that they were improperly investigated by local police and private entities, and that those officials have engaged in other activity that violates the law. *See, e.g.*, Compl. ¶¶ 83–93, 102–09, 119–21, 128–31, 138–46. The appropriate vehicle to remedy those alleged grievances would be a lawsuit against those local and private entities under state or federal law, including the Constitution. Courts of Appeals have repeatedly held that lawsuits directly against non-federal entities provide an adequate alternative to APA review, therefore precluding suit under the APA. *See, e.g., Turner v. Sec'y of HUD*, 449 F.3d 536, 539–41 (3d Cir. 2006); *Jersey Heights Neighborhood Ass'n v. Glendening*, 174 F.3d 180, 191–92 (4th Cir. 1999); *Wash. Legal Found. v. Alexander*, 984 F.2d 483, 486 (D.C. Cir. 1993); *Coker*, 902 F.2d at 90 ("Actions directly against the

states are not merely adequate; they are also more suitable avenues for plaintiffs to pursue the relief they seek."); *cf. Brem-Air Disposal v. Cohen*, 156 F.3d 1002, 1004–05 (9th Cir. 1998) (holding that citizen suit provision of Resource Conservation and Recovery Act provided an adequate, alternative remedy precluding APA jurisdiction). Courts in this district have taken the same approach. *See, e.g.*, *Garcia v. McCarthy*, No. 13-cv-03939, 2014 WL 187386, at *11–15 (N.D. Cal. Jan. 16, 2014) (recognizing that state law action against state officials is an alternative adequate remedy that precludes judicial review of action against EPA under APA).

III. PLAINTIFFS' FAILURE TO ALLEGE A FINAL AGENCY ACTION ALSO PRECLUDES APA JURISDICTION

Plaintiffs have likewise failed to allege a final agency action reviewable under the APA. Plaintiffs rely on the Program Manager's issuance of the Functional Standard and FBI's issuance of the Privacy Impact Assessment as the final agency actions for which they seek judicial review. Compl. ¶¶ 51, 154, 160. The guidance provided in these documents, however, does not establish the type of binding legal norm that is reviewable under the APA. For this reason as well, Plaintiffs' claims should be dismissed for lack of subject-matter jurisdiction. *See Wild Fish Conservancy v. Jewell*, 730 F.3d 791, 794 (9th Cir. 2013) (affirming dismissal for lack of subject-matter jurisdiction where plaintiff did not challenge final agency action).

Unless an agency action is made specifically reviewable by statute, it is only reviewable by a federal court under the APA if it is a "final agency action." 5 U.S.C. 704. In *Bennett v. Spear*, 520 U.S. 154 (1997), the Supreme Court held that two conditions must be satisfied for an 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 action must be one by which "rights or obligations have been determined," or from which "legal consequences will flow."

Id. at 177–88 (citations omitted); *see also Mamigonian v. Biggs*, 710 F.3d 936, 942 (9th Cir. 2013).

Plaintiffs cannot satisfy the second condition. Under this prong of the finality test, "[t]he general rule is that administrative orders are not final and reviewable unless and until they impose an obligation, deny a right, or fix some legal relationship as a consummation of the administrative process." *Ukiah Valley Med. Ctr. v. F.T.C.*, 911 F.2d 261, 264 (9th Cir. 1990); *see also Oregon Natural Desert Ass'n v. U.S. Forest Serv.*, 465 F.3d 977, 986 (9th Cir. 2006). Relevant factors in determining whether an action is final include "whether the order [or rule] has the status of law or comparable legal force," "whether immediate compliance with its terms is expected," and whether the agency action has a "direct and immediate effect on the day-to-day business of the subject party." *Ukiah*, 911 F.2d at 264 (quotation marks and citations omitted); *see also Oregon Natural*, 465 F.3d at 986. Because the Functional Standard and Privacy Impact Assessment only provide functional guidance for the operation of the NSI, and do not create any legal rights or obligations, they do not constitute reviewable actions.

On their face, neither the Functional Standard nor the Privacy Impact Assessment requires NSI participants to apply the definition of suspicious activity (*i.e.*, "behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity") or the "Criteria Guidance" (*i.e.*, the categories of behavior that may be indicative of pre-operational planning related to terrorism) they provide. The Functional Standard, as explained, is descriptive in nature. It explains the NSI process, standardizes terminology, and discusses the type of incident reports that NSI participants should consider sharing. In fact, it expressly provides that analysts and law enforcement officers should exercise their professional judgment in deciding whether to share information in connection with the NSI. And the Privacy Impact Assessment simply repeats the guidance provided in a prior version the Functional Standard. These documents do not impose any legal obligation on NSI participants to share, or refrain from sharing, information relating to suspicious incidents or behaviors.

Moreover, there is no allegation or indication that the Program Manager, the FBI, or any other federal agency, has ever taken any legal action to compel NSI participants to follow the guidance provided in the Functional Standard or the Privacy Impact Assessment. Plaintiffs instead rely on their allegations that Defendants train NSI participants in the guidance they provide and that NSI participants follow this guidance when collecting and disseminating SARs. *See, e.g.*, Compl. ¶¶ 48–49, 59–60. But the fact that NSI participants may for practical reasons decide to follow agency guidance does not make that decision a legal consequence of agency action. *See Cntrs. for Auto Safety v. Nat'l Highway Traffic*, 452 F.3d 798, 809, 811 (D.C. Cir. 2006) (holding that regulated parties following agency guidance did not mean that the agency action had a "legal consequence" even when the agency had encouraged the parties to follow that guidance); *cf. Oregon Natural*, 465 F.3d at 986 (holding that the issuance of a grazing license was a final agency action where agency issued notices of enforcement action based on alleged violations of that license).

The NSI is a cooperative initiative between federal, state, local, tribal, and territorial agencies. The guidance provided in the Functional Standard and Privacy Impact Assessment was developed to help these agencies share information with one another in an effective manner that is consistent with privacy and civil liberty protections. It does not fix legal rights or obligations, and thus, is not reviewable by the Court under the APA.

IV. PLAINTIFFS' APA CLAIMS ARE LEGALLY DEFICIENT

In addition to the threshold deficiencies discussed above, Plaintiffs have failed to adequately state any basis for their legal challenges under the APA. Specifically, Plaintiffs assert that (1) Defendants were required to go through notice-and-comment rulemaking before releasing the Functional Standard and the Privacy Impact Assessment and (2) Defendants' guidance in those documents is contrary to law because it permits the collection of criminal intelligence in the absence of reasonable suspicion of criminal conduct. Both of these claims are deficient as a matter of law.

A. Notice-and-Comment Rulemaking Is Not Required

The APA only requires agencies to go through notice-and-comment rulemaking when they act pursuant to legislative power delegated to them by Congress. *See Stoddard Lumber Co. v. Marshall*, 627 F.2d 984, 987 (9th Cir. 1980). This type of rule is commonly referred to as a legislative rule and is as binding on courts as a statutory enactment. *See Prod. Tool Corp. v. Emp't & Training Admin., U.S. Dep't of Labor*, 688 F.2d 1161, 1165 (7th Cir. 1982) ("Legislative rules are said to have the 'force and effect of law'—i.e., they are as binding on the courts as any statute enacted by Congress."). "Legislative rules," in other words, "create rights, impose obligations, or effect a change in existing law pursuant to authority delegated by Congress." *Hemp Indus. Ass'n v. Drug Enforcement Admin.*, 333 F.3d 1082, 1087 (9th Cir. 2003).

For the same reasons that the release of the Functional Standard and the Privacy Impact Assessment do not constitute final agency actions, they are also not legislative rules. *See, e.g.*, *Broadgate Inc. v. U.S. Citizenship & Immigration Servs.*, 730 F. Supp. 2d 240, 244 (D.D.C. 2010) (explaining that the question of whether agency guidance constitutes an agency action is similar to the question of whether agency guidance constitutes a legislative rule). These documents do not purport on their face to impose mandatory obligations, let alone to have the force and effect of law. And there is no indication that they have ever been, or could ever be, enforced in that manner.

The Program Manager issued the Functional Standard to provide guidance for the effective operation of a cooperative initiative between federal, state, and local law enforcement. The Functional Standard, as noted, provides a definition of suspicious activity and "Criteria Guidance" to aid NSI participants in identifying the type of incident reports that they should consider sharing in connection with the NSI. The Program Manager was not acting pursuant to any congressionally delegated authority to issue legislative rules when it released the Functional Standard, and Plaintiffs do not allege that the Program Manager has ever brought any sort of enforcement action to require compliance with the guidance contained in that document.

Nor was the FBI acting pursuant to any rulemaking authority when it included portions of the Program Manager's guidance in the Privacy Impact Assessment. Federal agencies, as noted, are statutorily required to conduct assessments regarding the privacy implications of collecting information or implementing new technology. These assessments, contrary to Plaintiffs' suggestion, are not vehicles used to establish binding rules or standards of any kind. Indeed, Defendants have been unable to locate a single judicial opinion requiring the use of APA notice-and-comment procedures in connection with the release of a privacy impact assessment.

B. Defendants Are Acting in Accordance with Law

The APA permits a reviewing court to set aside agency actions that are "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." 5 U.S.C. § 706(2)(A). The scope of judicial review of agency action under the arbitrary-and-capricious standard is narrow; it is limited to "ensuring that agencies have engaged in reasoned decisionmaking." *Judulang v. Holder*, 132 S. Ct. 476, 484 (2011). As the Ninth Circuit has explained, this means that an agency action may only be set aside under this provision in the following circumstances:

> [1] if the agency fails to consider an important aspect of a problem, [2] if the agency offers an explanation for the decision that is contrary to the evidence, [3] if the agency's decision is so implausible that it could not be ascribed to a difference in view or be the product of agency expertise, or [4] if the agency's decision is contrary to the governing law.

Lands Council v. Powell, 395 F.3d 1019, 1026 (9th Cir. 2005).

Plaintiffs' assertion that Defendants have acted arbitrarily or capriciously is meritless. Plaintiffs' claims are based solely on the fourth prong of this standard—that Defendants' guidance is allegedly contrary to governing law. Plaintiffs do not assert that this agency guidance runs afoul of any constitutional or statutory rule. Instead, they assert that Defendants' guidance is contrary to law because it fails to impose one of the operating principles of 28 C.F.R. Part 23 on the information-sharing systems (ISE Shared

Spaces and eGuardian) that are used to share incident reports in connection with the NSI. But there is no basis for the contention that these information-sharing systems should be subject to that regulation.

First, these two guidelines—the Functional Standard and 28 C.F.R. Part 23—were issued pursuant to distinct statutory authorities for application to distinct information-gathering programs. *Compare* 42 U.S.C. § 3789g(c) (authorizing OJP to issue policy standards for criminal intelligence systems funded under the Omnibus Act) *with* 6 U.S.C. § 485(f)(2)(A)(iii) (authorizing the Program Manager to issue functional standards for the ISE). The operating principles of 28 C.F.R. Part 23 are expressly linked to federal funding of criminal intelligence systems under the Omnibus Act. *See* 42 U.S.C. § 3789g(c); 28 C.F.R. § 23.1; 28 C.F.R. § 23.3; 28 C.F.R. § 23.30; 28 C.F.R. § 23.40. And Plaintiffs should not be permitted to require Defendants to impose identical (or even similar) funding conditions on participants in a distinct information-sharing program.

Second, the information-sharing systems used to share incident reports in connection with the NSI are not criminal intelligence systems under the terms of 28 C.F.R Part 23. As noted, that regulation only applies to "criminal intelligence systems" that are used for receiving, storing, disseminating, and analyzing "data which has been evaluated to determine that it . . . [i]s 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). In other words, 28 C.F.R. Part 23 only applies where "the purpose of the system is to collect and share information with other law enforcement agencies on individuals reasonably suspected of involvement in criminal activity." Final Revision to the Office of Justice Programs, Criminal Intelligence Systems Operating Policies, 58 FR 48448–01 (Sept. 16, 1993).

The systems challenged by Plaintiffs are not used for that purpose. The purpose of the NSI is not to create dossiers about individuals and organizations—such as John Gotti or the Gambino crime family—that are already "reasonably suspected" of criminal activity. 28 C.F.R. § 23.3(b)(3)(i). It is to share tips and leads about suspicious incidents

and behaviors among federal, state, local, tribal, and territorial agencies so that these agencies can identify patterns and trends across jurisdictional lines. *See* Compl., Ex. D at 58–62. Indeed, it is often only by connecting the dots between these reported incidents that the relevant agencies are able to identify potential threats and allocate resources to investigating potential terror threats.[9]

Finally, Plaintiffs have not alleged that any information-sharing system actively used in connection with the NSI receives support through the Omnibus Act. As noted, there were previously two information-sharing systems—ISE Shared Spaces and eGuardian—used in to share incident reports in connection with the NSI, but use of the ISE Shared Spaces has been discontinued. *See supra* Background Part I.C. *See generally* Compl., Ex. E. The only active system is eGuardian, a national database maintained by the FBI. And Plaintiffs do not allege that this federal information-sharing system receives any Omnibus Act funding.[10] Indeed, the FBI would not be an eligible recipient for an Omnibus Act grant for the maintenance and operation of an information-sharing system, as these grants are exclusively provided to state, local, tribal, and private entities. *See, e.g.*, 42 U.S.C. § 3714a (authorizing grants to states for the establishment

[9] Courts generally defer to an agency's interpretation of its own regulation to the extent the meaning of that regulation is ambiguous. *See Christopher v. SmithKline Beecham Corp.*, 132 S. Ct. 2156, 2166–67 (2012); *Chase Bank USA, N.A v. McCoy*, 131 S. Ct. 871, 880 (2011). The interpretation of 28 C.F.R. Part 23 provided in this brief is supported by the clear language of 28 C.F.R. Part 23 and is consistent with DOJ's prior interpretations of that regulation. *See, e.g.*, 2013 Privacy Impact Assessment (2013) (noting that eGuardian is not subject to 28 C.F.R Part 23); Final Revision to the Office of Justice Programs, Criminal Intelligence Systems Operating Policies, 58 FR 48448–01 (Sept. 16, 1993) (explaining that 28 C.F.R. Part 23 only applies where the purpose of the funded system is to collect and share information about individuals reasonably suspected of criminal activity). However, to the extent the Court determines there is any ambiguity in the meaning of this regulation, it should defer to agency expertise in this matter.

[10] Instead, Plaintiffs allege that state, local, and tribal law enforcement agencies, as well as fusion centers, have received funding from OJP for the operation of certain information-sharing systems. Compl. ¶¶ 12, 23, 25, 73, 155, 161. Plaintiffs, however, do not allege that this OJP funding was provided through the Omnibus Act. Moreover, even if Plaintiffs had alleged that this funding was provided through the Omnibus Act, eGuardian is operated and maintained by the FBI, not by state, local, and tribal law enforcement at fusion centers.

and maintenance of threat-assessment databases); 42 U.S.C. § 3796(h) (authorizing grants to state, tribal, and local criminal justice agencies, and nonprofit organizations for maintenance and operation of certain information-sharing systems).

Defendants have provided guidance to state and local entities indicating that they should consider sharing incident and behavior reports with other NSI participants when those reports are reasonably indicative or pre-operational planning related to terrorism. There is no governing law requiring use of the reasonable suspicion standard instead of this reasonably indicative standard, and Plaintiffs should not be permitted to import a regulation created in the context of a distinct statutory scheme in order to impose that requirement.

V. PLAINTIFFS' CLAIMS SHOULD BE SEVERED AND ALL BUT IBRAHIM'S CLAIMS DISMISSED FOR LACK OF VENUE

This action can and should be dismissed in its entirety for the foregoing reasons. But even if Plaintiffs could overcome the grounds for dismissal set forth above, the Court should sever Plaintiffs' claims pursuant to Federal Rule of Civil Procedure 21, and dismiss the claims of Plaintiffs Gill, Prigoff, Razak, and Conklin because venue does not lie in this district to hear their claims under the terms of 28 U.S.C. § 1391(e).

A. Plaintiffs Do Not Satisfy the Requirements of Rule 20(a)

The five Plaintiffs may not be joined in this action because they do not satisfy the requirements of Federal Rule of Civil Procedure 20(a). That Rule provides:

> Persons may join in one action as plaintiffs if: (A) they assert any right to relief jointly, severally, or in the alternative with respect to or arising out of the same transaction, occurrence, or series of transactions or occurrences; and (B) any question of law or fact common to all plaintiffs will arise in the action.

Fed. R. Civ. P. 20(a)(1). "If the test for permissive joinder is not satisfied, a court, in its discretion, may sever the misjoined parties, so long as no substantial right will be prejudiced by the severance." *Coughlin v. Rogers*, 130 F.3d 1348, 1350 (9th Cir.1997).

Plaintiffs' claims do not meet the first prong of Rule 20 because the rights to relief asserted do not arise out of the same transaction or occurrence. In determining whether claims arise out of the same transaction or occurrence, courts use the logical relationship test. *See Pochiro v. Prudential Ins. Co. of Am.*, 827 F.2d 1246, 1249 (9th Cir. 1987). The logical relationship test considers "'whether the essential facts of the various claims are so logically connected that considerations of judicial economy and fairness dictate that all the issues be resolved in one lawsuit.'" *Id.* (quoting *Harris v. Steinem*, 571 F.2d 119, 123 (2d Cir. 1978)). Claims arise out of the same transaction or occurrence if they share similar factual backgrounds. *Couglin*, 130 F.3d at 1350. And claims possess sufficient factual similarity if they "'arise out of a systematic pattern of events.'" *Bautista v. Los Angeles Cnty.*, 216 F.3d 837, 842–43 (9th Cir. 2000) (quoting *Coughlin*, 130 F.3d at 1350). In this case, Plaintiffs' claims arose at different times, by different actions, by different parties, and from different circumstances. The fact that this disparate conduct was allegedly caused by the guidance and training challenged is not enough to support joinder. *Coughlin*, 130 F.3d at 1350 ("[A] common allegation . . . does not suffice to create a common transaction or occurrence.").

No substantive right of Plaintiffs will be prejudiced, moreover, by severance. Requiring Plaintiffs to file separate lawsuits will not cause any prejudice to their claims or result in unfairness.

Because the claims of the five Plaintiffs cannot proceed in a single action, their claims should be severed pursuant to Federal Rule of Civil Procedure 21. Fed. R. Civ. P. 21 (providing that severance, rather than dismissal, is the appropriate remedy for misjoinder).

B. The Claims of Plaintiffs Gill, Prigoff, Razak, and Conklin Should Be Dismissed Pursuant to 28 U.S.C. § 1391(e)

Once severed from the claims of Plaintiff Ibrahim, the claims of Plaintiffs Gill, Prigoff, Razak, and Conklin would be unable to proceed in this Court because venue does not lie in this district to adjudicate those claims.

Under 28 U.S.C. § 1391(e)(1), venue for civil actions brought against the agencies of the United States and their employees in their official capacities is proper in any judicial district in which: "(A) a defendant in the action resides, (B) a substantial part of the events or omissions giving rise to the claim occurred, or a substantial part of property that is the subject of the action is situated, or (C) the plaintiff resides if no real property is involved in the action." The Supreme Court has stated, "[t]he requirement of venue is specific and unambiguous; it is not one of those vague principles which, in the interest of some overriding policy, is to be given a 'liberal' construction." *Olberding v. Ill. Cent. R.R. Co.*, 346 U.S. 338, 340 (1953). Under 28 U.S.C. § 1406(a), therefore, a court "shall dismiss" a case that has been filed in the wrong district unless "the interest of justice" warrants transfer to a district where the case could have been brought. The burden of demonstrating that venue is satisfied resides with Plaintiffs, *see AJZN, Inc. v. Yu*, No. 12-CV-03348-LHK, 2013 WL 97916, at *1 (N.D. Cal. Jan. 7, 2013), and they have failed to meet that burden.

Plaintiffs first argue that "[d]efendants are agencies of the United States and officers of the United States sued in their official capacities[.]" Compl. ¶ 20. But this does not make the Defendants, all of which operate in Washington, D.C., subject to suit in every judicial judicial district where a plaintiff does not reside. *See Reuben H. Donnelley Corp. v. F.T.C.*, 580 F.2d 264, 267 (7th Cir. 1978); *Kings Cnty. Econ. Cmty. Dev. Ass'n v. Hardin*, 333 F. Supp. 1302, 1304 (N.D. Cal. 1971). Rather, Federal agencies and officials reside, for purposes of 28 U.S.C. § 1391(e), where they perform their official duties. 14D Charles Alan Wright, Arthur R. Miller & Edward H. Cooper, *Federal Practice and Procedure* § 3815 (2007).[11] Courts thus recognize that agencies headquartered in Washington, D.C., such as Defendants, are residents of the District of Columbia. *See, e.g., Wilson v. Dep't of Army*, No. 3:13-CV-643-H (WVG), 2013 WL

[11] *See also Reuben H. Donnelly Corp. v. FTC*, 580 F.2d 264, 266–67 (7th Cir. 1978); *Davies Precision Machining, Inc. v. Def. Logistics Agency*, 825 F. Supp. 105, 107 (E.D. Pa. 1993); *Lamont v. Haig*, 590 F.2d 1124, 1128 n.19 (D.D.C. 1978).

6730281, slip op. at *1 (S.D. Cal. Dec. 19, 2013); *Exxon Corp. v. DOE*, No. Civil CA-3-78-0420-W (Consolidated), 1979 WL 1001 at *2 (N.D. Tex. June 1, 1979) (unreported).

Plaintiffs next assert that venue is proper because "a substantial part of the events or omissions giving rise to this action occur or occurred in this district, including Alameda and Contra Costa Counties." Compl. ¶ 20. That contention is meritless as well. Plaintiffs are challenging the promulgation of guidance and training that they do not allege occurred in this district. In addition, to the extent relevant to the venue question, the particular events of which the Plaintiffs complain also do not support venue in this district. The events of which plaintiff Gill complains of occurred in Chico, California, Compl. ¶¶ 80–100, which is outside this judicial district, in Butte County. *See* http://www.cand.uscourts.gov/jurisdictionmap. The events Prigoff complains of occurred in Boston, Massachusetts and in Sacramento, California *id*. ¶¶ 101–117, which is in Sacramento County, and also outside this judicial district. The events Razak complains of occurred in Placentia, California, and Santa Ana, California, *id*. ¶ 126–136, both of which are in Orange County, and far outside this judicial district. Although one of the two events Conklin complains of occurred in this district, *see* Compl. ¶¶ 138, 141 (identifying incidents in Benicia, California and Martinez, California), this event cannot be said to constitute a "substantial part" of the events giving rise to his claims. To the contrary, Conklin (like the other Plaintiffs) challenges Defendants issuance of guidance and their provision of training, events which did not occur in this district.

Plaintiffs finally assert that "one or more ***plaintiffs*** reside in this district." Compl. ¶ 20 (emphasis added). But that is only true of Ibrahim, who resides in San Jose, California. *Id*. ¶ 118. The rest reside outside of this district. *See* Compl. ¶¶ 80, 101, 126, 137. And, as explained, to the extent the other Plaintiffs seek to be joined pursuant to 28 U.S.C. § 1391(e)(1), there is no basis to do so under the Federal Rules.

The claims of Gill, Prigoff, Razak, and Conklin should accordingly be dismissed. *See King v. Russell*, 963 F.2d 1301, 1304 (9th Cir. 1992) (recognizing that dismissal is appropriate where none of the statutory bases for venue exist under Section 1391(e)).

CONCLUSION

For the foregoing reasons, Plaintiffs' claim should be dismissed in their entirety under Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6), or in the alternative, Plaintiffs' claims should be severed and the claims of Plaintiffs Gill, Prigoff, Razak, and Conklin should be dismissed under Federal Rule of Civil Procedure 12(b)(3).

October 16, 2014

Respectfully submitted,

JOYCE R. BRANDA
Acting Assistant Attorney General

MELINDA L. HAAG
United States Attorney

ANTHONY J. COPPOLINO
Deputy Branch Director

PAUL G. FREEBORNE
Senior Trial Counsel
Va. Bar No. 33024

/s/ *Kieran G. Gostin*
KIERAN G. GOSTIN
Trial Attorney
D.C. Bar. No. 1019779

Attorneys for the Defendants

CERTIFICATE OF SERVICE

I hereby certify that on October 16, 2014, I electronically filed Defendants' Motion to Dismiss on the Clerk of the Court using the CM/ECF system, which will send notice of this filing to all parties.

/s/ *Kieran G. Gostin*
KIERAN G. GOSTIN